НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

24 листопада 2023 року

З НАГОДИ 5-Ї РІЧНИЦІ ЗАСНУВАННЯ ФАКУЛЬТЕТУ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КІБЕРПРОСТІР
В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: ТЕОРІЯ ТА ПРАКТИКА

МАТЕРІАЛИ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРПРОСТІР В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: ТЕОРІЯ ТА ПРАКТИКА

МАТЕРІАЛИ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

24 листопада 2023 року, м. Одеса

Одеса, 2023

УДК 340.12:316.3

ББК 67.0

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій,
кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу
несуть учасники конференції, їхні наукові керівники,
які рекомендували ці матеріали до друку.

Друкується згідно з наказом ректора
Національного університету «Одеська юридична академія»
(№ 3449-62 від 19.10.2023 р.)

Матеріали Міжнародної науково-практичної конференції «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика» (м. Одеса, 24 листопада 2023 р.). Одеса, 2023. 301 с.

Міжнародна науково-практична конференція «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика» присвячена 5-ї річниці заснування факультету кібербезпеки та інформаційних технологій.

До участі у конференції запрошені студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

© НУ «Одеська юридична академія», 2023

Шановні учасники міжнародної науково-практичної конференції «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика»!

В епоху стрімких змін та викликів кіберпростір став невід'ємною частиною людського життя, але разом з тим він приносить нові загрози та виклики, особливо в умовах війни та глобальних криз. Він вражає своєю багатогранністю та охоплює не тільки технологічні питання, а й соціально-психологічні, нормативно-правові, управлінські та інші аспекти.

Кожен з напрямів досліджень кіберсередовища є багатовекторним і всі вони є взаємопов'язаними. Кібербезпека та захист інформації є основою сучасного суспільства, адже кібератаки завдають значних збитків, як приватним компаніям, так і державним установам. Тому фахівці у галузі кібербезпеки повинні мати глибокі знання та навички не тільки в сфері технічного захисту інформації, але й в інших областях, таких як: законодавство у сфері кібербезпеки; економіка кібербезпеки; психологія кібербезпеки; організаційні аспекти кібербезпеки.

На рівні суспільства зміни в кіберсередовищі приносять, як користь, виявлену в забезпеченні прав людей на інформацію та задоволенні їхніх інформаційних потреб, так і потенційні ризики, пов’язані з неправомірним використанням інформації та шкодою інформаційним правам та інтересам осіб. У період воєнних дій особливо актуальними стають проблеми вибору достовірної інформації та запобігання неконтрольованому розповсюдженню інформації.

В умовах війни інформаційно-комунікаційні системи також переживають значні трансформації. Особливої уваги заслуговує сегмент Military Technologies, що зосереджується на підсиленні оборонних можливостей нашої держави.

Не менш важливою є роль правових принципів у регулюванні кібернетичного простору, тому актуальним є питання вдосконалення законодавчої бази, що викликає зростаючий інтерес серед юридичної наукової спільноти. Окрім того, кібертехнології мають значний вплив на управлінські процеси, соціальну взаємодію та психологічний стан людей у сучасному світі.

В цілому, більшість сучасних питань прямо чи опосередковано пов’язані з інформаційними технологіями та кіберпростіром. Одеса входить до числа лідерів у цій галузі, маючи всі необхідні умови для розвитку: матеріально-технічну базу, високий науковий потенціал, значний кадровий ресурс та розвинену IT спільноту.

Ми сподіваємося на подальшу плідну роботу, продуктивний обмін знаннями, ідеями та досвідом щодо подальшого розвитку кіберпростору в умовах війни та глобальних викликів сьогодення.

Президент Національного університету
“Одеська юридична академія”,
академік НАПрН України, академік НАПН України
доктор юридичних наук, професор,
Заслужений юрист України *Сергій КІВАЛОВ*

Секція 1. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ ЯК ОСНОВА СУЧАСНОГО СУСПІЛЬСТВА

ТЕНДЕНЦІЇ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ: СУЧАСНІ ВИКЛИКИ

Дикий Олег

декан факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», кандидат юридичних наук, доцент

Сучасна українська освіта стикнулася проблемами та ризиками, які не мали аналогів у світовій історії, що обумовлено, як швидкоплинністю змін в сфері інформаційних технологій, так і повномасштабним вторгненням росії. Інформаційні та кібератаки вже стали буденними для українського суспільства, що детермінує пошук нових методів та форм їх протидії. До того ж така діяльність не може бути ефективною без підготовки висококваліфікованих фахівців у вказаних напрямках. Усвідомлення цього стимулювало запровадження атестації здобувачів ступеня вищої освіти на першому (бакалаврському) рівні у формі єдиного державного кваліфікаційного іспиту за спеціальністю 125 «Кібербезпека»[1], а вже 16 травня 2023 року, відбулося апробаційне проведення єдиного державного кваліфікаційного іспиту (ЄДКІ) за спеціальністю 125 Кібербезпека на першому (бакалаврському) рівні вищої освіти.

В подальшому відбулося переосмислення самої назви спеціальності 125 «Кібербезпека», яка в подальшому отримала назву 125 «Кібербезпека та захист інформації»[2], що було частиною адаптації українського законодавства в сфері освіти до європейського освітнього простору. Також ця еволюція визначена кількома факторами, які відображають сучасні реалії і вимоги індустрії.

Зміна назви спеціальності безумовно не є самоцілю, вже зараз відбувається адаптація стандарту вищої освіти за вказаною спеціальністю, що обумовлено викликами сучасності. Так, фахівець з кібербезпеки повинен володіти не лише технічними навичками в області виявлення та усунення кіберзагроз, але й розуміти принципи захисту конфіденційної інформації. Відкриття нових напрямків у сфері кібербезпеки обумовлено необхідністю адаптації до сучасних реалій та розширення спектру компетенцій.

У сучасному світі кібербезпека є однією з найважливіших проблем. Кібератаки завдають значних збитків як приватним компаніям, так і державним установам. Тому фахівці у галузі кібербезпеки повинні мати глибокі знання та навички не тільки в сфері технічного захисту інформації, але й в

інших областях, таких як: законодавство у сфері кібербезпеки; економіка кібербезпеки; психологія кібербезпеки; організаційні аспекти кібербезпеки.

Безумовно захист інформації став невід'ємною частиною кібербезпеки. У світі, де цифрові дані стають все більш цінними та піддаються атакам, важливо, щоб фахівець із кібербезпеки розумів не лише аспекти захисту систем, а й методи та стратегії захисту конфіденційної інформації. Зміна назви спеціальності відображає розвиток комплексного підходу, спрямованого на забезпечення безпеки не лише технічних систем, але й самої інформації, що обробляється цими системами.

Кіберзагрози та кібератаки стають більш складними та вдосконаленими з кожним роком. Сучасні фахівці з кібербезпеки повинні бути готові до вирішення проблем, пов'язаних не лише з технічними аспектами, але й з питаннями захисту конфіденційної інформації. Особливо гостро це питання постало під час повномасштабного вторгнення росії, так як крім класичних форм війни зараз з'явилися нові, що ведуться в кібер- та інформаційному просторах і направленні, як на заволодіння, знищення або пошкодження даних в інформаційних системах, так і проведенню інформаційно-психологічних операціях, в тому числі з використанням ботоферм в ЗМІ.

Зміна назви та змісту спеціальності також є відповіддю на зростаючий попит на фахівців, які можуть забезпечити повноцінний захист інформації в умовах сучасного цифрового середовища. Підприємства та організації все більше усвідомлюють важливість захисту конфіденційної інформації, і тому вони шукають фахівців, які не лише володіють технічними навичками, але й мають глибоке розуміння стратегій захисту інформації.

Варто також звернути увагу, що у міжнародній практиці більш поширена назва «Кібербезпека та захист інформації». Так, у країнах Європейського Союзу існує спеціальність «Cybersecurity and Information Security». Перейменування спеціальності також відбувається в контексті гармонізації з міжнародними стандартами у галузі кібербезпеки. Європейські країни розуміють важливість співпраці та обміну знаннями на міжнародному рівні у сфері кібербезпеки. Нова назва відображає бажання створити уніфіковані підходи та методи навчання, які відповідають сучасним міжнародним вимогам у галузі кібербезпеки та захисту інформації. Використання цієї назви в Україні відповідає міжнародним стандартам і сприятиме кращій інтеграції українських фахівців у світову спільноту.

Загалом зміна назви спеціальності 125 на «Кібербезпека та захист інформації» відображає важливі зрушення в сфері кібербезпеки. Це визнання того, що сучасний фахівець повинен бути готовий до вирішення не лише технічних викликів, але й забезпечення повноцінного захисту конфіденційної інформації. Це також відповідь на ринкові потреби та вимоги сучасного циф-

рового середовища, де інформація стає ключовим ресурсом, а кіберзагрози стають все більш вибагливими та різноманітними.

Список використаних джерел:

1. Постанова КМУ «Про атестацію здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційного іспиту» від 19 травня 2021 р. № 497. Режим доступу: https://zakon.rada.gov.ua/laws/show/497-2021-%D0%BF#Text
2. Постанова КМУ «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від від 16 грудня 2022 р. № 1392. Режим доступу: https://zakon.rada.gov.ua/laws/show/1392-2022-%D0%BF#Text

Ключові слова: штучний інтелект, веброзробка, персоналізація користувача, досвід користувача.
Keywords: artificial intelligence, web development, user personalization, user experience.

РОЛЬ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ В СЬОГОДЕННІ: ПРОБЛЕМАТИКА, ВИКЛИКИ ТА ЗАХОДИ ЗАХИСТУ

Ісмайлов Карен

Департамент кіберполіції Національної поліції України,
кандидат юридичних наук, доцент, підполковник поліції

Інформаційно-психологічна операція (далі ІПСО) є складовою частиною інформаційної війни і спрямована на вплив суспільних настроїв, уявлень та переконань. У сучасному світі, де доступ до інформації стає все більш широким та впливовим, ІПСО відіграють дедалі важливішу роль. Вони використовуються в різних сферах, включаючи політику, соціальні медіа, онлайн-середовища, а також особлива увага приділяється умовах правового режиму воєнного стану.

Для визначення ролі інформаційно-психологічних операцій наведемо його поняття, отже ІПСО – це різновид інформаційних операцій, проведення яких передбачає використання на практиці складної сукупності узгоджених, скоординованих і взаємопов'язаних форм, методів і прийомів психологічного впливу. Воно складається з політичних, військових, економічних, дипломатичних і власне інформаційно-психологічних заходів, спрямованих на конкретну людину чи групи людей з метою впровадження в їх середовище чужих ідеологічних і соціальних установок, формування помилкових стереоти-

пів поведінки, трансформації в потрібному напрямку їх настроїв, почуттів, волі [1].

Основними цілями ІПСО є: зміна психологічного ставлення та переконань цільової аудиторії, формування бажаних уявлень, стереотипів та маніпулювання емоціями та поведінкою людей. Засоби та методи які використовуються ІПСО тісно пов'язанні із буденним життям людей, а саме: інформаційні засоби (медіа, соціальні мережі, веб-ресурси, реклами) та психологічні техніки (дезінформація, маніпулювання емоціями, формування стереотипів, апеляція до психологічних слабкостей). Ці операції здатні впливати на думки, ставлення та переконання людей, що може мати значний вплив на їхні рішення, допомагають створювати образи та враження про певні ситуації, лідерів чи країни.

Застосування ІПСО у політиці, соціальних медіа та онлайн середовищах стає дедалі важливішим фактором формування громадської думки, ставлення до політичних подій та впливу на вибори, суспільні процеси та поведінку користувачів мережі. В політичних процесах ІПСО можуть використовуватися для зміни громадської думки про політичні події та кандидатів. Це може призвести до перемоги/програшу певної політичної сили або кандидата на виборах [2].

Так, найбільшого поширення та охоплення ІПСО отримує через просування в соціальних мережах, оскільки люди зазвичай використовують їх під час відпочинку і на підсвідомому рівні не готові критично аналізувати інформацію отриману з даних джерел. Тим більше, що зараз стає дорослим перше покоління, яке зросло на гаджетах і соцмережах. Вони більш агресивні та схильні до ризику, більш радикальні й схильні до депресій. Їх менше цікавлять романтичні стосунки.

ІПСО використовують психологію та емоції людей для впливу на їхню поведінку та переконання. Вони можуть формувати образи політичних лідерів, партій або груп, щоб викликати у людей бажані емоції, такі як страх, гнів або співчуття. Це може призвести до того, що люди будуть сприймати їх певним чином і ідентифікуватися з ними.

Основні загрози, які несуть інформаційно-психологічні операції в умовах воєнного конфлікту: розпалення конфлікту та поглиблення напруження, маніпуляція суспільною думкою, розповсюдження дезінформації, підрив моралі та деморалізація військових та населення, психологічний тиск та зміна стратегій ведення війни, посилення стереотипів та ворожнечі, порушення міжнародного співтовариства. Ці загрози можуть мати серйозні наслідки для всієї громадськості, зокрема: загострення конфлікту та погіршення ситуації на місцях, формування бажаних переконань та ставлення до конфлікту, спотворення реальності та поширення дезінформації, підрив бойового духу та

зниження ефективності військових, зміна стратегій та тактики ведення війни, загострення міжнаціональних відносин та підвищення ризику нових конфліктів [3].

Для запобігання впливу ІПСО на суспільство та політичні процеси важливо: захищати інформаційну безпеку, підвищувати інформаційну грамотність та критичне мислення населення, розробити та запровадити програми, які спрямовані на виявлення та боротьбу з дезінформацією через активне виявлення та відповідну реакцію на маніпуляції, захистити критичні інфраструктури через зміцнення кібербезпеки та захисту інформаційних систем від зловживань, вірусів, хакерських атак та інших кіберзагроз, розвивати внутрішньодержавні та міжнародні політичні стратегії, розбудовувати міжнародні співпраці, виявляти та контролювати соціальні мережі від поширення фейкової, дезінформуючої та маніпулятивної інформації.

Таким чином, нами булі розглянуті основна роль інформаційно-психологічних операцій та зроблено висновок, що ІПСО є серйозною загрозою для суспільства та політичних процесів. Вони можуть використовуватися для досягнення різноманітних цілей, включаючи вплив на громадську думку, формування бажаних переконань, розповсюдження дезінформації та маніпулювання емоціями. А також надано рекомендації для запобігання впливу ІПСО, а саме важливо захищати інформаційну безпеку, підвищувати інформаційну грамотність та критичне мислення населення, а також розробляти та запроваджувати програми, спрямовані на виявлення та боротьбу з дезінформацією. Ці заходи є важливими для забезпечення інформаційної безпеки та захисту суспільства від негативного впливу ІПСО.

Список використаних джерел:

1. Підручник Інформаційна безпека (соціально-правові аспекти) / Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. ; за заг. ред. Є.Д.Скулиша. К. : КНТ, 2010;
2. Що таке ІПСО та як росія використовує їх у війні проти України. URL: https://chas.news/current/scho-take-ipso-ta-yak-rosiya-vikoristovue-ih-u-viini-proti-ukraini
3. Інформаційно-психологічні операції росії. Як вони працюють і чи можна їм протидіяти. URL: https://nashkiev.ua/life/informatsiino-psihologichni-operatsii-rosii-yak-voni-pratsyuyut-i-chi-mozhna-im-protidiyati

Ключові слова: кібербезпека, кіберзлочинність, іпсо, соціальні мережи, інформаційна безпека.
Keywords: cybersecurity, cybercrime, ipso, social networks, information security.

АНАЛІЗ СУЧАСНИХ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Самойлов Станіслав

начальник 3-го управління інформаційних технологій та програмування Департаменту кіберполіції НПУ, кандидат юридичних наук

У зв'язку з швидким та невпинним зростанням використання штучного інтелекту, збільшення передачі потоків інформації з кожним днем, використанням соціальних мереж не тільки для особистого користування, актуальність вдосконалення стеганографічних методів захисту інформації росте швидко та стає все більш актуальною.

Збереження конфіденційності та цілісності інформаційних потоків під час їх передачі по різним каналами зв'язку займає провідну позицію у процесі забезпечення як особистої інформаційної безпеки так і в безпеці на рівні держави та суспільства [1].

Метою роботи є аналіз сучасних стеганографічних методів захисту інформації. Для якісного аналізу стенографічних методів захисту інформації необхідно дати визначення самого поняття стеганографії. Стеганографія – спосіб збереження, чи передачі інформації, при якому приховується сам факт існування інформації. На відміну від криптографії, де факт передачі інформації є відомий, а його зміст є зашифрованим, стеганографія покликана приховати саме існування інформації.

В умовах війни, приховування важливої інформації стає дуже важливим елементом безпеки. Саме для цього потрібна стеганографія. Сховати важливу інформацію в середині абсолютно стороннього файлу, який не викликає ніяких підозр. Наприклад, можна приховати текстовий файл в середині картинки. Ця картинка буде відкриватись як картинка, завантажуватись і розпізнаватись як картинка іншими програмами й 99% людей не здогадаються, що в середині є якийсь файл [4].

Основою цього аналізу являється моделювання та дослідження стеганографічних систем що допоможе виявити надійність та визначити вразливі місця.

Сучасні методи стеганографії часто базуються на використанні різних технік та алгоритмів, серед яких:

1. Метод LSB (Least Significant Bit). Цей метод використовується для зберігання інформації в менш важливих бітах зображення, звуку чи тексту, таким чином, що зміни не помітні для людського спостереження.

2. Частотність зміни пікселів/звукових семплів. Цей метод заснований на зміні частоти пікселів у зображених або змінених звукових семплів так, щоб приховати інформацію без втрати видимої чи аудіо якості.

3. Використання текстових форматів. Введення інформації в текстові файли шляхом зміни букв реєстру, додавання зайвих пробілів, використання спеціальних форматів тощо.

4. Використання криптографії. З'єднання методів стеганографії з криптографією для забезпечення безпеки отриманої інформації.

5. Адаптивні методи. Техніки, які автоматично пристосовуються до змінних умов для ефективного сприйняття інформації.

Важливо зауважити, що багато з цих методів вимагають збалансованості між об’ємом отриманої інформації та збереження якості основних даних. Також використання стеганографії може бути піддано ризикам з боку кібербезпеки та може використовуватися як знаряддя для незаконних дій.

Якщо провести аналіз джерел літератури, то можна виділити чотири напрями сучасної стеганографії: класична, цифрова, лінгвістична та квантова.

Кожний із цих напрямів вартий уваги та використовується для певних цілей. Кожний із цих напрямів має свої ефективні методи для приховування інформації.

Велика частина нашого дослідження присвячена саме розробці нових та вдосконаленню існуючих методів приховування даних. Незважаючи на велику кількість досліджень в цій галузі, та високий рівень досліджень, до недавнього часу була не визначена класифікація таких методів. Це ускладнювало аналіз та не давало, в повній мірі, здійснити оцінку методів. Складність визначення оцінки не давала прослідити ефективність та вдосконалень.

Існують основні методи цифрової стеганографії:

- засновані на використанні комп’ютерних форматів;
- цифрової обробки сигналів.

Проаналізував сучасні методи стеганографії їх можна розділити наступним образом [2]:

- вибір контейнера,
- наявність ключа,
- призначення,
- принцип приховування,
- стійкість.

На кожному етапі треба приділяти увагу перевагам та недолікам

На прикладі цифрорової стеганограії можно розглянути розподіл методів на групи, їх переваги та недоліки .

До недоліків стеганографічних методів захисту інформації можна віднести:

- малий обсяг переданої інформації,
- малу пропускну здатність
- низький ступінь скритності.

До переваг стеганографічних методів захисту інформації можна віднести:

- зниження ймовірності факту передачі повідомлення;
- додатковий рівень захисту;

Висновки таким чином, проведено аналіз стеганографічних методів захисту інформації на прикладі цифрової (комп'ютерної) стеганографії, виявлено, що найпопулярнішими та найефективнішими методами є вбудовування секретних повідомлень. Задяки особливості передачі, завантаження, зберігання файлів, вбудоване повідомлення часто може бути не виявлено отримувачем.

В подальшій роботі планується розглянути аналіз сучасних стеганографічних методів захисту інформації всіх напрямів стеганографії.

Список використаних джерел:

1. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. К. : Юниор, 2003. 464 с.
2. Юдін О.К., Конахович Г.Ф., Корченко О.Г. Захист інформації в мережах передачі даних: Підручник. К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009.
3. Карпінець В.В., Яремчук Ю.Є. Аналіз рівня спотворень векторних зображень внаслідок вбудовування цифрових водяних знаків. Сучасний захист інформації. 2011. №2. С. 94-99.
4. Стеганографія, або як сховати файл на видному місці. URL: https://sprotyv.mod.gov.ua/steganografiya-abo-yak-shovaty-fajl-na-vydnomu-mistsi/

Ключові слова: кібербезпека, стеганографія, захист інформації, інформаційна безпека.
Keywords: cybersecurity, steganography, protection of information, information security.

ДОСЛІДЖЕННЯ АЛГОРИТМУ ФОРМУВАННЯ СТЕГАНОГРАФІЧНОГО КЛЮЧА ДЛЯ ПОБУДОВИ ЗМІННИХ КРИПТОГРАФІЧНИХ S-БЛОКІВ

Ахаметьєва Ганна

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Сучасні глобальні тенденції, спрямовані на впровадження цифрового документообігу, електронних баз даних, реєстрів, аналізу ринку та прогнозування подальшої ситуації в будь-якій сфері людського життя, обробку вели-

чезної кількості цифрової конфіденційної інформації, тощо, потребують постійного удосконалення засобів її захисту, зокрема криптографічних і стеганографічних методів.

Традиційним засобом захисту є криптографічне закриття інформації шляхом виконання циклів послідовних перетворень над блоками вхідних даних. Надійність такого закриття і стійкість до зламу визначаються структурою циклів та їх кількістю. Особливу увагу розробники приділяють увагу S-блокам заміни, за допомогою яких реалізується нелінійний шар криптографічного перетворення, який в значній мірі запобігає можливості використання сучасних методів криптоаналізу, таких як диференціального, лінійного та інших. S-блоки заміни, як правило, є складовими криптографічних алгоритмів, в деяких з них передбачена можливість використання сторонніх таблиць заміни, зокрема таку можливість надає національний стандарт шифрування ДСТУ 7624:2014 [1, 2].

Стеганографічні методи захисту є більш специфічними і не мають поширення для захисту значних обсягів даних через обмеження пропускної спроможності прихованого каналу зв'язку, оскільки, по-перше, це вимагає надвеликих обсягів контейнерів для зберігання захищених даних, по-друге, збільшення даних на одиницю контейнера призведе до погіршення якості самого контейнера, що взагалі нівелює сенс захисту.

У стеганографії одним з параметрів ключа, зокрема для зображень і відео, може виступати матриця, яка задає порядок вибору елементів контейнеру для вбудовування інформації. Елементами цієї матриці (розміри якої залежать від розміру контейнера) є значення від 0 до MN–1, перемішані згідно заданого алгоритму. Якщо розглянути елементи S-блоків заміни у криптографічному перетворенні, то це також перестановка значень від 0 до 2N–1, записана в формі квадратної матриці. В роботі [3] був запропонований алгоритм для формування стеганографічного ключу, який можна адаптувати для задачі формування змінних S-блоків заміни криптографічного перетворення.

До основних досягнутих результатів алгоритму [3], які є корисними для S-блоків, можна віднести наступні.

1. Стеганографічний ключ (матриця ключа) розраховується на основі вхідних параметрів: розміру контейнеру; паролю, який подається на вхід обраної хеш-функції; числа перемішувань, яке задає кількість проходів кожного рядка і стовпця таблиці при перемішуванні. Ключову матрицю можна не зберігати в окремих захищених файлах, оскільки її легко відтворити за вхідними параметрами. У випадку S-блоків маємо їх фіксований розмір, тому можна прив'язати їх формування до ключа шифрування та числа перемішування, а через це S-блок також стає секретним структурним елементом криптографічного перетворення.

2. Процедура перемішування стеганографічного ключа задіює і рядки, і стовпці шляхом їх циклічного зсуву, причому величина зсуву для кожного рядку/стовпця на кожному кроці є змінною. Вибір рядків і стовпців для перемішування не є послідовним, а задається генератором псевдовипадкових чисел (ПВЧ), параметри якого формують окремі значення дайджесту паролю. Це дозволило отримати непередбачений характер самої процедури перемішування, оскільки всі її внутрішні параметри прив'язані до секретного елементу – в даному випадку хеш-значення ключа і числа перемішувань.

3. Запропонований алгоритм був протестований графічними статистичними тестами [4]. Для алгоритму експериментальним шляхом було визначено мінімальне число перемішувань P, яке забезпечує проходження графічних тестів та рівномірний розподіл вибраних елементів по всьому контейнеру (розташування перших 0,05-0,1% чисел з послідовності від 0 до MN–1). При P=7 і вище спостерігається проходження тестів автокореляційної функції, розподілу на площині, гістограми розподілу бітових слів від 0 до 255, гістограми розподілу цифр від 0 до 9, спектральний тест.

Дослідження графічних тестів достатньо лише для попереднього аналізу, слід мати на увазі, що результати таких тестів є суб'єктивними, оскільки спираються на візуальні графіки та трактовки експертів. Для подальшого вивчення і дослідження властивостей ключової матриці, а також можливості застосування в криптографічних перетвореннях S-блоків, сформованих на основі запропонованого алгоритму, слід проаналізувати проходження статистичних тестів, наприклад, NIST [5] та/або Diehard [6]. Попереднє дослідження обмеженої кількості ключових матриць розміром 256×256 показало проходження всіх тестів NIST та доцільність проведення подальшого чисельного експерименту.

S-блок представляє собою бієктивну матрицю заміни, в якій кожному вхідному елементу єдиним способом ставиться у відповідність вихідний елемент. Сучасні криптографічні алгоритми, такі як AES та ДСТУ 7624:2014, працюють з байтовими замінами, тобто S-блок має розмір 16×16 та працює з числами від 0 до 255. Для з'ясування можливості застосування алгоритму формування стеганографічного ключа, який по суті здійснює перемішування елементів, до генерування S-блоків слід провести оцінку параметрів нелінійності S-блоків.

Якщо проаналізувати саму структуру алгоритму (рис. 1), то вона є досить складною і містить забагато внутрішніх параметрів і складних обчислень:

- процедура «Формування додаткових ключів» містить задані параметри у виборі складових хешу та обчислення математичних виразів, обґрунту-

вання яких в [4] не наводиться, – в подальшому цю процедуру можна спростити;

- при генеруванні послідовності ПВЧ («Генерація ППВЧ») використовуються два лінійних конгруентних генератори за модулями PM та PN, для забезпечення максимального періоду яких використовуються ще дві константи – множник и модуль, а також стоїть задача факторизації складеного числа;

- специфічна операція порозрядного складання десяткових чисел при обчисленні величини зсуву – кожний розряд десяткового числа складається за модулем цифри, що є максимальною у ПВЧ (md – maximum digit), що відповідає номеру рядка/стовпця. З одного боку ця операція є нестандартною – через постійну зміну ПВЧ змінюється і цифра-модуль, що знов вносить непередбачуваність, з іншого вимагає багато обчислень в десятковій системі числення, що негативно впливає на швидкість.

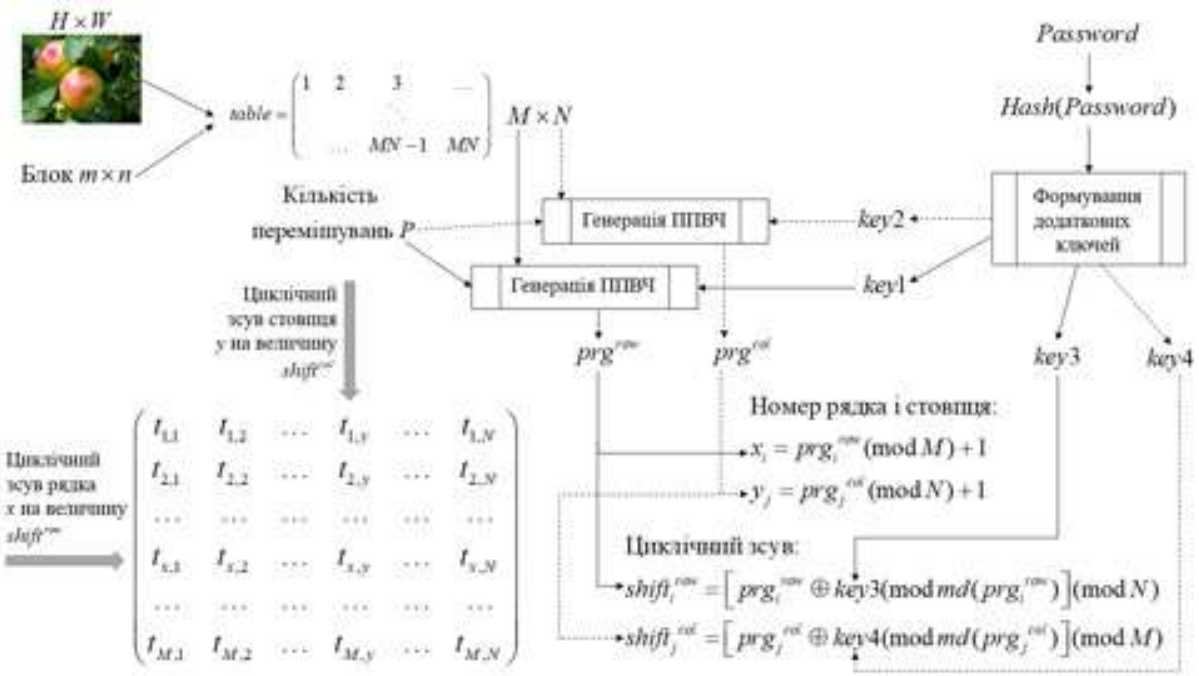


Рис.1. Структурна схема алгоритму формування стеганографічного ключа

Таким чином, за попередніми результатами досліджень можна зробити висновок про можливість використання алгоритму формування стеганографічного ключа до генерування змінних S-блоків, ймовірно з деякою його адаптацією під вхідний параметр – ключ шифрування. Це дозволить отримати змінні секретні S-блоки, як додатковий захищений параметр криптографічного алгоритму. Детальні результати проведених експериментальних досліджень будуть опубліковані в науковій статті.

Список використаних джерел:

1. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Текст]. – Введ. 01–07–2015. – К. : Мінекономрозвитку України, 2015.
2. Горбенко І. Д. Симетричний блоковий шифр «Калина» – новий національний стандарт України / І. Д. Горбенко, Р. В. Олійников, О. В. Казимиров, В. І. Руженцев, О. О. Кузнєцов, Ю. І. Горбенко, О. В. Дирда, В. І. Долгов, А. І. Пушкарьов, Р. І. Мордвінов // Радіотехніка. – 2015. – Вип. 181. – С. 5–22.
3. Ахмаметьєва Г.В., Бойко Н.В. Розробка алгоритму формування стеганографічного ключа для цифрових зображень. «Шляхи розвитку науки в сучасних кризових умовах»: матеріали І Міжнародної науково-практичної інтернет-конференції (Дніпро, 28-29 травня 2020 р.). / Дніпро, 2020. Т.1. 608 с. С.32-35.
4. Бойко Н.В. Удосконалення стеганографічного методу для цифрових зображень. Розробка алгоритму формування стеганографічного ключу: квал. роб. бак.: 122 Комп'ютерні науки. – Одеса 2020. – 67 с.
5. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. NIST Special Publication 800-22. May 15, 2001.
6. The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness// http://www.stat.fsu.edu/pub/diehard/

Ключові слова: стеганографія, стеганографічний ключ, криптографія, S-блоки заміни, перемішування, статистичні характеристики
Keywords: steganography, steganographic key, cryptography, S-boxes, permutation, statistical characteristics

ВПЛИВ КІБЕРЗАГРОЗ НА ЕФЕКТИВНІСТЬ УПРАВЛІННЯ ПІДПРИЄМСТВОМ

Пунченко Наталія

в.о. завідувача кафедри інформаційних технологій Одеського державного аграрного університету, кандидат технічних наук, доцент

Златова Марія

магістрант Одеського державного аграрного університету

У роботі розглядається важливий аспект у сучасному бізнес-середовищі. Аналізуючи зростання кіберзагроз і кібератак, у роботі досліджується, як ці інциденти впливають на загальну ефективність управління підприємством. Зокрема, розглядається втрата прибутку, вартість відновлення та зміни в стратегічному плануванні підприємства. Підкреслюється необхідність інтеграції ефективних стратегій кібербезпеки в систему управління підприєм-

ством і досліджується роль різних відділів, включаючи IT і вищого керівництва для забезпечення кіберстійкості. Крім того, робота рекомендує компаніям звернути увагу на інвестиції в кібербезпеку, враховуючи її важливість для довгострокового успіху та відновлення після потенційних кібератак [1].

У роботі дані посилання джерел, які пояснюють представлений матеріал.

The article considers an important aspect in the modern business environment. Analyzing the growth of cyber threats and cyber attacks, the article examines how these incidents affect the overall effectiveness of enterprise management. In particular, it considers the loss of profit, the cost of recovery and changes in the strategic planning of the enterprise.The article highlights the need to integrate effective cyber security strategies into the enterprise management system and examines the role of various departments, including IT and senior management, in ensuring cyber resilience.In addition, the article recommends that businesses pay attention to investments in cybersecurity, given its importance to long-term success and recovery from potential cyberattacks[1].

The work provides links to sources that explain the material presented.

Проблема впливу кіберзагроз на ефективність управління підприємством стає все більш актуальною в умовах цифрової трансформації бізнесу. Кібератаки можуть призвести до серйозних наслідків, таких як втрати конфіденційної інформації, переривання бізнес-процесів та пошкодження репутації підприємства.

Зростання кількості та складності кіберзагроз ставить під сумнів ефективність існуючих стратегій управління ризиками та кібербезпеки. Підприємства повинні усвідомити, що кіберзагрози не обмежуються лише технічними аспектами, але також мають важливий економічний вимір, впливаючи на фінансові показники та загальний відтік вартості бізнесу[2].

Поставлена проблема вимагає глибокого аналізу та розробки ефективних стратегій управління кіберризиками, які б враховували не лише технічні заходи забезпечення безпеки, а й економічні аспекти, такі як вартість відновлення, страхування та витрати на ефективні заходи кібербезпеки.

Аналіз останніх досліджень та публікацій показує, що за останні роки тема впливу кіберзагроз на управління підприємством привернула значну увагу в наукових дослідженнях. Її вивченням займались Арістова І.В., О. Криворучко, Ю.О. Черниш та багато інших науковців[4]. Їх дослідження акцентуються на розширенні кількості та складності кіберзагроз, оцінці економічних втрат від кібератак, а також розробці стратегій управління ризиками та кібербезпекою. Дослідники вивчали ефективність заходів кіберзахисту та їх вплив на бізнес-процеси та фінансові результати підприємства. Так, Шеломенцев В.П. особливу увагу приділив аспектам інтеграції кібербезпеки в за-

гальну стратегію управління підприємством, враховуючи зростання кількості та різноманітності кіберзагроз[4].

Виходячи з вищевикладеного можна визначити мету дослідження, яка полягає у аналізі комплексного впливу кіберзагроз на рівні аспекти функціонування підприємства та у визначенні стратегії, що спрямована на забезпечення стійкості та оптимальної ефективності у цифровому середовищі.

Сучасна дійсність свідчить про те, що кіберзагрози стрімко розвиваються: кіберзлочини стають більш вдосконаленими, краще координованими і мають транснаціональний характер. Це випливає з того, що Інтернет, цифрові послуги та інформаційно-комунікаційні технології (ІКТ) стали необхідною частиною світової економіки: від електронного обігу документів, інтернет-магазинів та онлайн-банкінгу до систем Інтернету речей та інтелектуальних систем управління підприємствами. За зростанням залежності від ІКТ у бізнесі та підприємництві також зростають кіберризики і кіберзагрози, що вимагає невідкладної реакції для їхнього уникнення або вирішення, а також збільшує необхідність обізнаності факторів ризику серед всіх зацікавлених сторін[3].

Система кібербезпеки має слугувати загальному інтересу як для постачальників послуг, так і для користувачів. Держава, яка виступає гарантом прав і свобод громадян, повинна взяти на себе відповідальність за забезпечення доступу до стабільного та безпечного цифрового простору, доступного для всіх громадян[2]. Відповідно, забезпечення належного рівня кібербезпеки стає необхідною умовою розвитку інформаційного суспільства.

Кібербезпека може не лише реагувати на інциденти, але й передбачати та запобігати атакам ще до їх виникнення. Для підвищення продуктивності підприємства, фахівці з кібербезпеки повинні акцентувати увагу не лише на технологіях, але й на тісній взаємодії з бізнес-командами. Співпраця повинна призвести до готовності відповідати на виклики кіберзловмисників і відбивати атаки з раніше невиданою ефективністю. Керівники підприємств все частіше звертаються до експертів з інформаційної безпеки для підвищення стійкості інформаційної системи та створення цінності захисту для бізнесу [3].

Однак за останні роки використання інформаційних технологій в гібридній війні породило нові вищого рівня кіберзагрози, спрямовані на національну та міжнародну безпеку. Збільшується кількість і потужність кібератак, мотивованих геополітичними інтересами окремих держав, груп та осіб, і вони вже не обмежуються поняттями фінансової ефективності чи рентабельності[1].

Нова епоха кібербезпеки вимагає повністю нових стратегій управління підприємством та його ресурсами, зокрема, інформаційними. Успішне впровадження таких змін в значній мірі залежить від гнучкості бізнес-процесів на підприємстві та ефективності інтеграції нових моделей та методів роботи.

Під час аналізу сучасного стану та тенденцій цифрових технологій, які визначають нову еру кібербезпеки, визначено ключові напрямки захисту підприємства від кіберзагроз.

Щодня стає все важливішим змінювати стереотипи в суспільстві щодо особистих даних, переконуючи, що вони є цінними. Відповідно, актуально проводити навчання фахівців з використання захищених протоколів передачі інформації та впровадження захищених інформаційних систем у роботу[2].

Ризик в сфері кібербезпеки для підприємства може бути пов'язаний із його партнерами та постачальниками. Захист IT-систем може бути посилений, але атаки хакерів можуть відбутися через отримання доступу до даних. Основною загрозою є те, що підприємства, намагаючись забезпечити сильний кіберзахист своїх інформаційних систем, мають труднощі у контролі дій всіх своїх партнерів та підрядників, яким надають доступ до своїх даних. Ці партнери та підрядники можуть виявитися менш кіберграмотними серед співробітників та мати менш ефективні рішення з кібербезпеки. І саме цими вразливостями користуються хакери, нападаючи на компанії-підрядники та отримуючи доступ до необхідних їм інформаційних систем[3].

Незалежно від причин виникнення, кіберінциденти завжди представляють загрозу для неперервної діяльності та сталого розвитку будь-якого підприємства. Основним інструментом для запобігання їм є система кіберзахисту, яка базується на наявних організаційних та технологічних ресурсах, фінансах, людських кадрах і нормативно-правовому базисі. Зазвичай системний адміністратор відповідає за створення цієї системи на локальному рівні. На великих підприємствах управління комплексом заходів протидії кіберзагрозам вже є управлінською задачею, для вирішення якої необхідно залучати кваліфікованих фахівців. Незалежно від конкретних інструментів, які планується використовувати, менеджмент безпеки виконується відповідно до таких принципів: локалізація людського фактору; розуміння критичних місць та джерел небезпеки; моніторинг ризиків; можливість оперативного реагування[4].

Висновки. Вплив кіберзагроз на ефективність управління підприємством вимагає комплексного підходу. Активне керівництво, розвиток культури безпеки та впровадження передових стратегій є важливими кроками у забезпеченні стійкості та успішної діяльності підприємства в умовах кіберзагроз.

Визначено, що для забезпечення кібербезпеки бізнесу є доцільним впровадження відповідних заходів, з основним акцентом на налагодженні потужного захисту інформаційних систем. Важливо враховувати, що загрози кібератак постійно еволюціонують, тому українському бізнесу важливо активно працювати над удосконаленням кіберзахисту. Це завдання зали-

шається стратегічно важливим як для державних установ, так і для приватного бізнесу.

Список використаних джерел:

1. Кібербезпека бізнесу в умовах нестабільності. URL: https://www.pwc.com/ua/uk/publications/2022/ cybersecurity-uncertainty-state.html. (дата звернення: 09.11.2023)
2. Майже половину кібератак СБУ виявляє у режимі «реального часу». URL: https://www.ukrinform.ua/ rubric-technology/3584942-majze-polovinu-kiberatak-sbu-viavlae-u-rezimi-realnogo-casu.html (дата звернення: 09.11.2023)
3. УПРАВЛІННЯ РИЗИКАМИ НА ПІДПРИЄМСТВІ. URL: http://dees.iei.od.ua/index.php/journal/article/view/218/204 (дата звернення: 10.11.2023)
4. КІБЕРБЕЗПЕКА УКРАЇНИ: АНАЛІЗ СУЧАСНОГО СТАНУ. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y (дата звернення: 10.11.2023)

Ключові слова: кібератака, кібербезпека, кіберзагроза, кіберінцидент.
Keywords: cyber attack, cyber security, cyber threats, cyber insident.

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

Кухаренко Сергій

доцент кафедри кібербезпеки факультету кібербезпеки і інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Кількість кіберзагроз з кожним роком швидко зростає. Розвиток кібератак, їх масштаби і можливі впливи на діяльність будь-яких організації спонукають останніх знаходити та приймати важливі рішення про те, як економічно ефективно управляти операціями щодо забезпечення безпеки.

Великі корпорації та організації всього світу такі, як JPMorgan Chase, IBM, Cisco, Amazon Web Services (AWS), Microsoft вже протягом багатьох років активно використовують Security Incident Event Management (SIEM) та Security Operations Center (SOC) у своїх стратегіях забезпечення інформаційної безпеки.

SOC – це спеціалізований центр (фізичний об'єкт всередині організації), що поєднує фахівці з інформаційної безпеки (команда аналітиків), які за допомогою спеціальних систем, процесів та технологій, призначених для безперервного моніторингу та реагування на події вирішують завдання з безпеки. Таких як контроль питань кібербезпеки, виявлення загроз, порушень та їх

аналіз, оперативне реагування на них, запобігання їх виникненню та складання звітності, а також координація дій щодо забезпечення безпеки.

SIEM представляє собою комплексну систему для збору, аналізу та управління журналами подій та даними безпеки організації. Він призначений для виявлення та реагування на потенційні загрози та є центральним інструментом для обробки інформації про безпеку, надаючи можливість агрегувати та аналізувати дані з різних джерел, а також створювати оповіщення про потенційні інциденти.

Важливо розуміти, що SIEM та SOC працюють спільно. SIEM відповідає за збирання та аналіз даних про безпеку, а також за створення сповіщень на основі виявлених подій. Згенеровані оповіщення передаються в SOC, де аналітики проводять детальніший аналіз, вирішуючи, які події вимагають додаткових дій.

Ця взаємодія дозволяє забезпечувати оперативне реагування на небезпеку.

У разі підозрілої активності, команда SOC-центру отримує повідомлення, аналізує їх, вивчає контекст і приймає рішення про подальші дії. Якщо рівень підозрілості події дуже високий, SIEM може самостійно ізолювати процес, а потім вже сповістити аналітиків.

SOC відіграє ключову роль у використанні SIEM. Аналітики SOC відповідають за:

1. Моніторинг оповіщень, створюваних SIEM, та проведення додаткових перевірок для встановлення їхньої справжності та серйозності.

2. Реагування на підтверджені інциденти безпеки та вжиття заходів щодо їх усунення.

3. Координацію дій у разі кібератак та інцидентів.

4. Забезпечення безпеки організації у реальному часі.

SOC є інтерфейсом між SIEM та реальним світом, гарантуючи, що дії вживаються відповідно до виявлених загроз.

В загалі SOC – це комплексне безперервне управління ризиками, вразливостями, загрозами та інцидентами безпеки у тому числі пов’язаними з розвиненими стійкими погрозами і прихованими тривалими інцидентами.

До основних напрямків SOC можна віднести наступні попереджувальні і реагуючі практичні цілі: запобігання інцидентам безпеки; моніторинг, виявлення та аналіз потенційних вторгнень; реагування на підтверджені інциденти; ситуаційна обізнаність і звітність про статус безпеки; проектування та експлуатація захисту комп’ютерних мереж.

В свою чергу SIEM підтримує процеси, які можна описати наступним чином.

1. Збирає та об’єднує дані з джерел подій у системі, систематизує їх та надає співробітникам SOC.

2. Аналізує та формує подій за допомогою правил загроз на основі пріоритетів.

3. Запобігає фішингу.

4. Аналізує поведінку користувачів і об'єктів, щоб виявити незвичну, ненормальну поведінку, котра може вказувати на загрозу.

5. Проводить оптимізацію робочих процесів у відповідність стандартам безпеки, нормативним вимогам та законам. Таким як, наприклад, PCI DSS, HIPAA, SOX, GDPR та багатьом іншим.

Можна сказати, що SIEM-система – це своєрідний скелет, на який нарощується пул з інших технологій, компонентів та масивів даних. Правильне проектування, побудова та налаштування всієї цієї конструкції дозволяє сформувати гармонійну систему захисту, яка управляється однією командою з SOC-центру.

SIEM-система є найнеобхіднішим сучасним інструментом кібербезпеки для державних установ та бізнесу, як в мирний, так особливо і в воєнний час. Адже в обставинах безперервних, як ракетних, так і кібератак, оперативне реагування є ключовою складовою убезпечення життя, як людського, так і життя оборонного сектору держави, а отже і держави в цілому. Наявність великої кількості інструментів у складі SIEM-системи, дозволяє експлуатувати її у відповідності до особливостей діяльності організації та задач інформаційної безпеки, що перед ним стоять.

Виходячи з вищеописаного, для своєчасної реакції на вторгнення, коли периметр захисту вже подоланий зловмисниками, крім наявності стандартних засобів безпеки (антивірусів, міжмережевих екранів, систем безпеки електронної пошти та доступу до WEB, систем управлінням доступом до мережі тощо) для ефективного відображення сучасних атак необхідні збір та централізований аналіз подій усередині IT-інфраструктури.

З урахуванням того, що в середній мережі обсяг записів про події за добу може досягати десятків гігабайт, перегляд цих подій та їх аналіз є трудомістким процесом, що посилюється різною структурою повідомлень, різними рівнями критичності тощо. Саме для цих цілей використовуються системи Security Information and Event Management (SIEM), завданням яких і є збір логів із систем, їх нормалізація, знаходження підозрілих дій і залежностей для повідомлення про них фахівця з безпеки, як про невдалу подію, що вдалася або злом, що триває.

Розуміння SIEM та SOC дозволить нам краще зрозуміти, як ці два компоненти взаємодіють для забезпечення безпеки організації. Перевагами сучасних SIEM-рішень є аналіз поведінки, застосування машинного навчання та штучного інтелекту, а також автоматизація SOC.

Компоненти SIEM-рішень, такі як збір даних, аналіз загроз, кореляція подій, просунута аналітика та інші, відіграють ключову роль у забезпеченні безпеки та дозволяють оперативно реагувати на інциденти.

Отже, SIEM і SOC спільно забезпечують безпеку організації у сфері кібербезпеки. Їхнє правильне впровадження та інтеграція можуть суттєво покращити захист від кіберзагроз та сприяти забезпеченню безпеки інформації та активів організації.

Список використаних джерел:

1. The essential guide to SIEM (Learn Security Information and Event Management) [Електронний ресурс] – Режим доступу до ресурсу: https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2020/12/The-Essential-Guide-to-SIEM.pdf.
2. SIEM vs SOC: Do You Know the Difference? [Електронний ресурс] – Режим доступу до ресурсу: https://cybersecuritykings.com/what-is-the-difference-between-siem-and-soc/.
3. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures [Електронний ресурс] – Режим доступу до ресурсу: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8309804/.
4. Сучасний SOC: чому SIEM-системи є необхідними? Електронний ресурс] – Режим доступу до ресурсу: https://eska.global/blog/suchasnij-soc-chomu-siem-sistemi-ye-neobhidnimi.
5. 4 Reasons Why Companies Need SIEM-Based SOC [Електронний ресурс] – Режим доступу до ресурсу: https://www.linkedin.com/pulse/4-reasons-why-companies-need-siem-based-soc-esecuritytogo/

Ключові слова: Кібербезпека, управління кібербезпекою, аудит, операційний центр безпеки, SEIM-системи
Keywords: Cyber security, cyber security management, audit, security operations center, SEIM systems

ДОСЛІДЖЕННЯ КІБЕРЗАГРОЗ ТА ОЦІНКА РИЗИКІВ КІБЕРБЕЗПЕКИ ЗАСОБАМИ IPYTHON / JUPYTERLAB

Бойко Віктор

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат технічних наук

Аналіз та оцінка ризиків кібербезпеки є значною частиною роботи фахівців та експертів з інформаційної безпеки. При цьому характер роботи, особливо аналіз та дослідження даних про вторгнення до системи, передбачає роботу з великими обсягами різнорідних даних. Окрім звичайного тексту,

це можуть бути табличні дані, ілюстрації, графіки, креслення, схеми, мультимедійні формати, математичні формули.

Окремой проблемой є обробка та аналіз різнорідних первинних даних. Як приклад таких даних можна навести бази даних, логи та системні журнали, дампи мережевих пакетів, перехоплених програмами-аналізаторами трафіку (сніферами - sniffer). Робота з такими даними серйозно ускладнюється через великі обсяги даних. Це особливо стосується дампів мережевих пакетів: дамп кількох хвилин роботи в мережі без спеціально встановлених фільтрів може займати десятки гігабайт. Існують різноманітні способи стиснення дампу, що зберігається шляхом усунення надмірності, проте такі способи допомагають слабо, оскільки аналіз даних може проводитися тільки на несжатому, "чистому" дампі.

При цьому в роботі аналітика інтерес представляє не тільки результат, але і процес отримання даних і хід міркувань аналітика, яки часто потрібно відтворювати для даних різного типу та характеру[1].

Зазвичай організація робочого процесу такого типу, якщо розглядати його з точки зору інструментів, що використовуються, організована нераціонально та виконується з великими витратами на ручну роботу, яку існуючими засобами складно автоматизувати[2].

Як правило для аналізу та написання звітів використовуються офісні пакети (пакети сімейства Microsoft Office, або Microsoft 365, або Libre Office Document Foundation) – при цьому для аналізу використовується табличний процесор, а для написання звіту – текстовий процесор та іноді редактор формул.

Якщо офісний пакет міститься у центр робочого процесу, то "сирі" (raw) дані доводиться опрацьовувати окремо, оскільки сучасні офісні пакети не розраховані на обробку таких обсягів інформації. Результати обробки (графіки, таблиці, формули у разі CAS) також доводиться генерувати окремо, а потім вручну додавати до протоколів та звітів аналізу. При цьому для нових даних весь процес потрібно повторювати вручну (обробка даних - генерація результатів аналізу - додавання їх до протоколу та звіту).

У деяких робочих колективах робляться спроби автоматизації цього процесу. Існує кілька конвертерів із різних форматів (pandoc[3], rtf2latex2e[4]), проте у випадку Microsoft Office проблема додатково ускладнюється пропрієтарним форматом файлів Microsoft, внаслідок проблеми автоматизації та вбудовування результатів роботи в документи доводиться вирішувати методами реверс інжинірингу.

Альтернативний варіант - використання в робочому процесі засобів середовища jupyter lab[5], що розвинулася в процесі еволюції оболонки ipython.

На початку ipython просто передбачала розширені засоби роботи з історією команд REPL-консолі: збереження, різного роду маніпуляції та відновлення історії роботи консолі.

Поряд з розвитком оболонки ipython з'явився і розвивався формат зберігання історії сесій "ipynb" (скорочення від ipython notebook), який у загальному вигляді є json-файлом у кодуванні UTF-8, при цьому бінарна інформація (наприклад, файли формату png) зберігається в вигляді base64-рядків. Формат виявився зручним, оскільки дозволяв поширювати та обмінюватися необхідними даними в "атомарному режимі", коли вся необхідна інформація доставлялася в одному файлі.

Подальший розвиток формату та оболонки призвело до того, що на платформі ipython виникла система з веб-інтерфейсом, яка дозволяла виконувати всі необхідні дії, не виходячи з браузера. Надалі проект із веб-інтерфейсом виділився в окремий проект jupyter, який отримав можливість працювати з ядрами інших мов. При цьому загальним робочим форматом залишається ipynb.

Jupyter lab має розвинені можливості експорту, крім того, він сам по собі набув широкого поширення серед дослідників та аналітиків, перетворившись де-факто на стандарт відкритої науки та аналізу великих даних.

Використання для аналізу ризиків та загроз кібербезпеці інструментарію середовища ipython/jupyterlab та формату даних ipython notebooks дозволяє отримати наступні переваги:

· єдиний формат для зберігання різноманітних даних - ipynb-формат дозволяє зберігати та відтворювати дані практично всіх необхідних для аналізу категорій: код, табличні значення, ілюстрації, графіки, математичні формули, мультимедійні дані;

· автоматизація процесу аналізу та генерації звітів для різних вхідних даних;

· при використанні jupyter lab, є мовонезалежним (lang agnostic) та допускає використання "ядер" (kernel за термінологією jupyter lab) від інших мов програмування та програмних середовищ (наприклад, CAS Maxima у поєднанні з clist kernel та можливістю виведення результатів роботи перетворень у TeX -форматі);

· є машинно-читаним, що відкриває додаткові можливості;

· завдяки механізму virtual environment (venv) дозволяє легко відтворювати робоче середовище та бібліотеки у тій частині, яка стосується python та його бібліотек;

· дозволяє виробляти експорт у більшість поширених відкритих форматів (html, tex, markdown); - що робить його ще більш універсальним інструментом;

· універсальний формат зберігання даних, що поєднує в собі універсальність і зручність роботи з даними, при цьому дані можуть як вбудовуються (embedding) в документ, так і підключатися до нього засобами скрипта, що запускається всередині jupyter lab / python.

Таким чином, використання в робочому процесі дослідження кіберзагроз та оцінки ризиків кібербезпеки засобів ipython/jupyterlab дозволить значно спростити процес, зробить його універсальним, розвантажить аналітиків та експертів з кібербезпеки від частини ручної роботи та покращить взаємодію між ними.

Список використаних джерел:

1. Security Big Data Analytics: Past, Present and Future [Електронний ресурс]. – Режим доступу : https://www.exabeam.com/explainers/siem/siem-analytics/ – Назва з екрана.
2. Happy collaboration with Rmd to docx [Електронний ресурс]. – Режим доступу : https://rmarkdown.rstudio.com/articles_docx.html – Назва з екрана.
3. Pandoc [Електронний ресурс]. – Режим доступу : https://pandoc.org/ – Назва з екрана.
4. rtf2latex2e: [Електронний ресурс]. – Режим доступу : https://latex2rtf.sourceforge.net/ (дата звернення: 2023-11-22). – Назва з екрана.
5. Project Jupyter [Електронний ресурс]. – Режим доступу : https://jupyter.org/ – Назва з екрана.

Ключові слова: кібербезпека, кіберзагроза, python, ipython, cas maxima, пошуковий аналіз, bigdata, data explore
Keywords: cybersecurity, cyberthreat, python, ipython, cas maxima, exploratory analysis, bigdata, data explore

ОГЛЯД МЕТОДІВ ВБУДОВУВАННЯ ІНФОРМАЦІЇ В ЗВУКОВІ ФАЙЛИ

Овчинников Микола

асистент кафедри кібербезпеки Національного університету «Одеська юридична академія»

На сьогоднішній день методи стеганографії актуальни як ніколи. Крім основного їх призначення – збереження інформації від несанкціонованого доступу, вони допомагають захистити інтелектуальну власність, коли справа стосується мультимедійних даних, зокрема аудіофайлів.

Відомо, що звукові файли мають своїх законних власників – авторів з моменту їх створення. Законодавство не вимагає додаткових дій від автора. Але було б логічно, щоб при створенні (виробництві) аудіо контенту, прихована інформація про автора вбудовувалася б усередину файлу відразу в мо-

мент створення. Знайти місце для зберігання такої інформації нам допоможе надмірність файлів, які містять мультимедійні дані.

Розглянемо, які методи занурення захищеної інформації за допомогою стеганографії існують на сьогоднішній день, з'ясуємо, що лежить в основі їхньої роботи, виділимо їх переваги і звернемо увагу на слабкі сторони.

Одним з найбільш відомих та популярних методів вбудовування секретної інформації, що зачіпають область аудіоданих, є метод зміни найменших значущих бітів (LSB - Least Significant Bit). Цей метод найчастіше використовується для приховування даних в аудіофайлах формату WAV завдяки простоті здійснення вставки [1].

Метод полягає у використанні похибки дискретизації, яка завжди існує в оцифрованих аудіофайлах. Ця похибка дорівнює найменшому значущому двійковому розряду числа, що визначає величину елемента файлу [2]. Використовуючи звуковий сигнал шляхом заміни найменших значущих біт кожної точки здійснення вибірки, представленої двійковою послідовністю, можна зашифрувати значний обсяг інформації. Сам процес вбудовування інформації полягає в тому, що у кожному значенні амплітуди найменший значний біт замінюється на біт повідомлення.

Популярність даного методу обумовлена його простотою і тим, що дозволяє приховувати в відносно невеликих файлах значні обсяги інформації. Метод часто працює з растровими зображеннями, представленими у форматі без компресії, наприклад, GIF та BMP.

Метод LSB має низьку стеганографічну стійкість до атак пасивного та активного порушників. Основний його недолік - висока чутливість до найменших спотворень контейнера. Для ослаблення цієї чутливості часто додатково застосовують завадостійке кодування [3]. Для підвищення стійкості методу, а також ефективнішого приховування інформації можливе використання даного методу спільно з криптографією [4].

Метод фазового кодування полягає у розбитті сигналу на сегменти та заміщенні фази початкового сегмента аудіо сигналу на фазу, яка характеризує дані (секретне повідомлення). Фази наступних сегментів регулюються з метою збереження різниці фаз між сегментами. Метод фазового кодування є одним із методів, який стійкий до стиснення та впливу шумів. Коли відношення фаз між частотами змінюється, відбувається помітна фазова дисперсія. Проте “нечутне” кодування у своїй однаково досягається, оскільки зміна фази досить мало.

Методи, що ґрунтуються на зміні фазової області, як правило, змінюють абсолютне значення фази деяких гармонік. Існують варіації, у яких відновлюються значення різниці фаз суміжних фреймів. Робиться це виходячи з припущення, що людське сприйняття звуку чутливе не до абсолютного зна-

чення фази сигналу, а до різниці фаз суміжних фрагментів. У найпростіших випадках ці методи є нестійкими до модифікацій даних.

З переваг цього методу - висока стійким до атак. З недоліків - він певною мірою знижує суб'єктивну якість звуку.

Не менш популярними методами вкладання цифрових водяних знаків (ЦВЗ) в аудіосигнал є метод модуляції миттєвої фази [5] та додавання ехосигналів [6, 7]. Перший використовує слабку чутливість людського вуха фазовому спектру аудіосигналу. Однак подальші дослідження показали, що для виділення ЦВЗ потрібно забезпечити дуже точну синхронізацію на приймальній стороні, що фактично неможливо у реальних умовах.

Явище реверберації полягає у суперпозиції різних ехосигналів, отриманих від джерела звуку. Ефект реверберації можна спостерігати у закритих приміщеннях після вимкнення джерела звуку [5]. Реверберація присутня спочатку у будь-якому звукозаписі, іноді її додають штучно з метою надання музичним творам певних відтінків звучання.

Для штучного додавання реверберації необхідно зробити згортку вихідного сигналу з «кімнатним імпульсом». Кімнатний імпульс - це реакція приміщення, що моделюється, на одиничний звуковий імпульс [8].

Найважливішою вимогою до системи ЦВЗ є її стійкість до різних природних та навмисних перетворень аудіофайлів з вкладенням, при яких зберігається висока якість основного аудіосигналу (наприклад, музичного файлу).

До природних перетворень відносять, перш за все, стиск із використанням стандартних методів. Тестуючи метод на файлах формату mp3, можна побачити, що хоча кількість бітових помилок зросте, це не призведе до повного «обриву» каналу ЦВЗ, як можна було б очікувати при такого методу вкладення, як, наприклад, LSB.

Таким чином, розглянувши кілька методів занурення секретної інформації в звуковий файл, можна дійти висновку, що кожен з розглянутих методів має як сильні сторони, так і ряд недоліків, які заважають зробити кожен з цих методів універсальним, стійким до змін, спотворень, а також різного роду атак. Однак у ряді випадків застосування кожного з цих методів допустиме та виправдане.

Вважаю, що подальше вивчення результатів роботи цих методів дає можливість врахувати переваги кожного з них, а також уникнути помилок розробки більш надійного методу занурення інформації в звукові файли.

Список використаних джерел:

1. Pranati Rakshit, Souvik Pal, Sreeparna Ganguly, Dac-Nhuong Le. Securing Technique Using Pattern-Based LSB Audio Steganography and Intensity-Based Visual Cryptography. Computers Materials & Continua · January 2021

2. Hariom Dudhwal, Jayshree Boaddh, Jashwant Samar. A Review of an Extensive Survey on Audio Steganography Based on LSB Method. International Journal of Scientific Research & Engineering Trends. Volume 7, Issue 1, Jan-Feb-2021
3. Tavoli R. Bakhsi Maryam Salehian F. A new method for text hiding in the image by using LSB. (IJACSA) Internation Journal of Advanced Computer Sceince and Apllications, vol.7, No4, 2016, p.126-132.
4. Joshi K. Yadav R. A new LSB-S image steganography method blend with cryptography for secret communication. Third International Conference on Image Information Processing (ICIIP), 2015, p. 86-90.
5. Nishimura, R. Audio watermark based on periodical phase shift [Text] / R. Nishimura, Y. Suzuki // J. Acoust. Soc. Japan. –2004. –Vol. 60. –No 5. –P. 268–272.
6. Bender W., Gruhl D., Morimoto N. Techniques for Data Hiding. Proc. SPIE. — 1995. — Vol. 2420. — P.40.
7. Tavoli R. Bakhsi Maryam Salehian F. A new method for text hiding in the image by using LSB. (IJACSA) Internation Journal of Advanced Computer Sceince and Apllications, vol.7, No4, 2016, p.126-132.
8. Kim, H.J. A novel echo-hiding scheme with backward and forward kernels [Text] / H.J. Kim, Y.H. Choi // IEEE Transactions on Circuits and Systems for Video Technology. – 2003. –No 13 (8). –P. 885–889.

Ключові слова: стеганографія, аудіофайли, метод заміни найменших значущих бітів, метод фазового кодування, метод на основі реверберації
Keywords: steganography, audio files, least significant bit method, phase coding method, reverberation based method

Науковий керівник: к.т.н., доцент Ахмаметьєва Г.В.

УРАЗЛИВОСТІ СТЕКА XAMPP

Стаднік Денис

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

XAMPP - це кросплатформна збірка локального веб-сервера, що містить Apache, MariaDB, інтерпретатор скриптів PHP, мову програмування Perl і велику кількість додаткових бібліотек, які дають змогу запустити повноцінний веб-сервер. XAMPP працює з усіма 32-х і 64-х розрядними ОС Microsoft (98/2000/XP/2003/Vista/7/8/10/11), а також з Linux, Mac OS X і Solaris. Програма вільно поширюється згідно з ліцензією GNU General Public License і є безкоштовним, зручним у роботі web-сервером, здатним обслуговувати динамічні сторінки [1].

XAMPP дає змогу швидко і легко створити локальне середовище розробки для веб-проектів. Це корисно для тестування нових проєктів, налагодження помилок і навчання веб-розробці.

Основні компоненти XAMPP [2]:

1) Apache - веб-сервер, який відповідає за обслуговування HTTP-запитів.

2) MariaDB - вільний репозиторій MySQL, який надає СУБД для зберігання даних.

3) PHP - інтерпретатор скриптів, який дає змогу створювати динамічні веб-сторінки.

4) Perl - мова програмування загального призначення, яка часто використовується для створення веб-додатків.

XAMPP також має низку проблем, які можуть вплинути на його безпеку, продуктивність або надійність. XAMPP має низку вразливостей, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до системи.

Ось деякі з найпоширеніших вразливостей XAMPP:

1. Система комплексна - розібратися складніше, ніж під час звичайного встановлення. Крім того, постачальник може довільно змінювати конфігурацію.

2. Уразливості безпеки Apache: Apache є одним із найпопулярніших веб-серверів у світі, і він має низку відомих вразливостей безпеки. Ці вразливості можуть бути використані зловмисниками для отримання несанкціонованого доступу до веб-сервера або для виконання шкідливого коду.

3. Уразливості безпеки PHP: PHP є однією з найпопулярніших мов програмування для веб-розробки, і вона має низку відомих вразливостей безпеки. Ці вразливості можуть бути використані зловмисниками для виконання шкідливого коду або для отримання доступу до даних користувача.

4. Уразливості безпеки MariaDB: MariaDB є вільною і відкритою реалізацією MySQL. Вона має низку відомих вразливостей безпеки. Ці вразливості можуть бути використані зловмисниками для отримання доступу до даних користувача або для виконання шкідливого коду.

XAMPP має низку налаштувань, які можуть вплинути на його безпеку, продуктивність або надійність. Налаштування системи за замовчуванням можуть містити проблеми та вразливості [3]. До таких налаштувань належать:

1) Непотрібні служби, які мають уразливості

2) Відсутність парольного захисту веб-сервера та бази даних

3) Функцію автентифікації спочатку вимкнено

4) Брандмауер від початку не налаштований для захисту веб-сервера

5) Відкриваються непотрібні порти, які дають зловмиснику більше можливостей

6) можливість отримати доступ за замовчуванням до веб-сервера і бази даних.

Усе це потенційно несе ризики для недосвідченого адміністратора і відкриває нові шляхи для зловмисників. Щоб зробити свій веб-сервер безпечнішим, необхідно усувати можливі проблеми заздалегідь, поки зловмисник не встиг ними скористатися.

Ось кілька порад щодо усунення вразливостей XAMPP:

1. Оновіть програмне забезпечення: регулярно оновлюйте Apache, PHP і MariaDB до останньої версії.

2. Використовуйте брандмауер: використовуйте брандмауер для захисту свого сервера від зовнішніх атак.

3. Увімкніть аутентифікацію: Увімкніть аутентифікацію для доступу до веб-сервера і бази даних.

4. Використовуйте надійні паролі: Використовуйте надійні паролі для доступу до веб-сервера та бази даних.

5. Вимкніть непотрібні служби: Вимкніть непотрібні служби, такі як FTP і SSH.

Під час встановлення XAMPP необхідно відразу проводити повне налаштування для підвищення безпеки. У XAMPP є безліч непотрібних налаштувань, які необхідно вимкнути, і присутні потрібні функції, які необхідно увімкнути.

Стандартні налаштування XAMPP, яких слід позбутися з метою безпеки:

1) Відключити доступ за замовчуванням до веб-сервера і бази даних: За замовчуванням XAMPP доступний за адресою http://localhost і localhost:3306 відповідно. Це означає, що будь-хто, хто має доступ до вашого комп'ютера, може отримати доступ до вашого веб-сайту і бази даних. Щоб підвищити безпеку, необхідно відключити доступ за замовчуванням до веб-сервера і бази даних. Це можна зробити змінивши налаштування Apache і MariaDB.

2) Увімкнути аутентифікацію: Аутентифікація допомагає захистити ваш веб-сайт і базу даних від несанкціонованого доступу. За замовчуванням XAMPP не використовує аутентифікацію. Щоб увімкнути автентифікацію, необхідно змінити налаштування Apache і MariaDB.

3) Використовувати надійні паролі: Ненадійні паролі легко зламати. Необхідно використовувати надійні паролі для доступу до веб-сервера, бази даних та інших захищених ресурсів.

4) Вимкнути непотрібні служби: XAMPP містить низку служб, які не завжди необхідні. Вимкнення непотрібних служб може допомогти підвищити безпеку вашого сервера.

5) Налаштувати брандмауер: Брандмауер може допомогти захистити ваш сервер від зовнішніх атак. Налаштування брандмауер необхідне, щоб дозволити тільки необхідний доступ до вашого сервера.

6) Регулярно оновлювати програмне забезпечення: Розробники програмного забезпечення часто випускають виправлення безпеки для усунення відомих вразливостей. Регулярне оновлення програмного забезпечення XAMPP допоможе захистити свій сервер від нових вразливостей.

XAMPP - це потужний і універсальний інструмент, який може використовуватися для різних цілей. Він є чудовим вибором для веб-розробників, які хочуть створити локальне середовище розробки для своїх проектів. Однак XAMPP має низку проблем із безпекою та налаштуванням, що робить його складним у використанні для комерційних додатків і недосвідчених користувачів. Для того, щоб розпочинати роботу з XAMPP, необхідно провести повне налаштування програми і прибрати всі відомі вразливості. Якщо розібратися з кожним компонентом, що входить до складу XAMPP, його використання стає більш функціональним і зрозумілим.

Список використаних джерел:

1. What is XAMPP? [Електронний ресурс] – Режим доступу до ресурсу: https://www.apachefriends.org/index.html.
2. What is XAMPP, and how do you install it on Windows? [Електронний ресурс] – Режим доступу до ресурсу: https://www.quora.com/What-is-XAMPP-and-how-do-you-install-it-on-Windows.
3. Reasons Why You Should Never Use XAMPP on Your Production Server [Електронний ресурс] – Режим доступу до ресурсу: https://www.makeuseof.com/reasons-why-you-should-never-use-xampp-on-production-server/.

Ключові слова: налаштування, програмне забезпечення, вразливості, користувач, безпека.
Keywords: customize, software, vulnerabilities, user, security.

Науковий керівник: к.т.н., доцент Бойко В.Д.

ТЕХНОЛОГІЇ ПРИХОВУВАННЯ ПРИСУТНОСТІ В СИСТЕМІ

Соловйов Артем

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасному світі кібербезпека відіграє ключову роль у захисті конфіденційної інформації, як для приватних осіб, так і для організацій. Однією з проблем кібербезпеки є тренд шкідливого програмного забезпечення (ШПО)

на приховування своєї присутності в системі після вторгнення і отримання необхідних прав. Чим далі, тим більш потайними стають ШПО. Згідно "Mandiant Security Effectiveness Report 2020" 53% кібератак закінчується невиявленим впровадженням в організаційні структури та 91% усіх інцидентів не викликають спрацювання систем безпеки [1]. Згідно з звітами IBM за 2020 рік, тільки на ідентифікацію витоків йде до 280 днів, оцінки інших експертів варіюються в межах від сотень до року [2].

Приховування слідів активності зловмисників і пентестерів стає дедалі складнішим завданням, оскільки зловмисники постійно розробляють нові техніки і технології, щоб ускладнити їх виявлення.

Зловмисники використовують широкий спектр технік приховування присутності, включаючи:

· Маскування активності: зміна характеристик мережевої активності, щоб зробити її менш помітною від звичайного трафіку.

· Очищення логів: видалення або зміна записів у журналах, щоб приховати сліди активності.

· Шифрування логів: захист логів з використанням шифрування, щоб запобігти їхньому читанню або аналізу.

· Зміна часових міток: маніпуляція часовими позначками в логах, щоб ускладнити визначення послідовності подій.

· Маскування активності: створення фальшивих подій або зменшення інформативності логів.

· Розподілений запис логів: логи зберігаються на різних пристроях або серверах, щоб ускладнити їх збирання та аналіз.

· Маскування IP-адрес: зміна і переадресація IP-адрес для ускладнення визначення джерела активності.

· Керування доступом до логів: обмеження доступу до журналів тільки для авторизованих користувачів.

· Використання прихованих каналів: передання інформації через нестандартні канали, не пов'язані зі звичайними мережевими протоколами.

Найважчою ситуація є для веб-серверів із сегмента середнього рівня — у разі ресурсів для організації окремої служби недостатньо і всі завдання безпеки виконує системний адміністратор[3]. Чиїх зусиль і знань зазвичай недостатньо.

З появою нових методів та інструментів для виявлення вторгнень, а також удосконаленням методів аналізу логів, необхідність в інноваціях на полі кібербезпеки стає очевидною. Просунуті зловмисники обходять стандартні методи виявлення і активно використовують нові технології для маскування своєї присутності.

З перерахованого випливає необхідність з одного боку підвищення кваліфікації системних адміністраторів, з другого - розробки та вдосконалення нових інструментів виявлення присутності у системі ШПО.

Список використаних джерел:

1. Mandiant Security Effectiveness Report 2020 Now Available I Business Wire [Електронний ресурс]. – Режим доступу : https://www.businesswire.com/news/home/20200505005192/en/Mandiant-Security-Effectiveness-Report-2020-Now-Available – Назва з екрана.
2. IBM: Cost of a Data Breach Report 2020 [Електронний ресурс]. – Режим доступу : https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf – Назва з екрана.
3. Top Skills Linux SysAdmins Should Ace in 2022 - Spiceworks [Електронний ресурс]. – Режим доступу : https://www.spiceworks.com/tech/it-careers-skills/articles/key-skills-for-linux-sysadmins/ – Назва з екрана.

Ключові слова: Тестування на проникнення, приховання присутності, проникнення, мережі, комп'ютерні мережі, скритя логів, шифрування, маскування, боротьба, сліди.
Keywords: Penetration testing, presence concealment, penetration, networks, computer networks, hiding logs, encryption, masking, fighting, traces.

Науковий керівник: к.т.н., доцент Бойко В.Д.

БЕЗПЕЧНЕ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ БОЙОВИХ ДІЙ

Спесівцев Микола

студент 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасному світі інформаційні технології (далі ІКТ) відіграють важливу роль в різних сферах життя, включаючи військовий сектор. Використання ІКТ в умовах бойових дій стає все більш розповсюдженим і дозволяє покращити ефективність військових операцій.

Використання ІКТ відкриває перед військовими нові можливості, такі як краща координація операцій, розвідка, контроль та забезпечення стабільного функціонування комунікацій. Проте, це також збільшує ризики стосовно кібератак і розголошення важливої інформації. Для забезпечення безпеки військових операцій важливо розглянути декілька аспектів.

Основні аспекти безпечного використання ІКТ в умовах бойових дій:

Захист від кібератак:

· Усунення слабкостей. Постійна оцінка та виправлення слабкостей в військових інформаційних системах є ключовим завданням. Це включає в себе постійні оновлення та аудит систем безпеки.

· Моніторинг та реагування. Системи моніторингу дозволяють виявляти незвичайну активність та спроби вторгнення, що дозволяє швидко реагувати на потенційні загрози.

Шифрування та безпека даних:

· Ключова інфраструктура/ Забезпечення захищеної інфраструктури для обміну ключами та шифрування даних є критичним. Використання сучасних криптографічних алгоритмів і стандартів є необхідним.

· Кібергігієна. Підтримка кібергігієни військового персоналу, включаючи навчання щодо безпеки паролів, фішингу та інших кіберзагроз.

Резервне керування:

· Системи автономного керування. Розробка систем, які можуть автономно функціонувати в умовах обмеженої або повної втрати доступу до централізованих комунікаційних мереж, наприклад, системи наземного керування безпілотними літальними апаратами.

· Використання супутників. Забезпечення можливості комунікації через супутникові мережі в разі недоступності звичайних засобів.

Спеціалізовані та безпечні програмні засоби

· Захищені операційні системи. Використання спеціалізованих операційних систем з підвищеним рівнем безпеки для критичних військових систем.

· Аудит та сертифікація. Проведення аудиту і сертифікації програмних засобів на відповідність стандартам безпеки.

Розвиток ІКТ в воєнній справі призвів до створення доктрини мережево-центричної війни.

Мережево-центрична війна — це концепція ведення бойових дій, що передбачає збільшення бойової потужності угруповання об'єднаних сил шляхом утворення інформаційно-комунікаційної мережі, що поєднує джерела інформації (розвідки), органи управління та засоби ураження (придушення), що забезпечує доведення до учасників операцій достовірної та повної інформації про обстановку практично в реальному масштабі часу [1].

У 2016 році в Україні була впроваджена національна система ситуаційної обізнаності “Дельта” для використання Силами безпеки і оборони України. Ця система розроблена відповідно до стандартів НАТО і призначена для забезпечення ведення МЦВ і контролю ситуації.

Система "Дельта" інтегрує інформацію щодо розташування сил і засобів ворога, надаючи можливість в реальному часі відслідковувати їхню позицію

та швидко визначати цілі для подальших атак. Вона об'єднує дані про ворога на цифровій мапі, які надходять з різних джерел, таких як супутникові знімки, радари, сенсори, GPS-трекери і радіоперехоплення. Користувачі можуть спостерігати за діями ворога на суходолі, в морі, в повітрі, в космосі.

Ця система використовується для планування військових операцій. За допомогою захищеного месенджера ELEMENT, який є частиною системи "Дельта", здійснюється координація між військовими підрозділами та безпечний обмін інформацією. Платформа і сервіси "Дельта" відповідають стандартам НАТО, підтримують специфікацію MIP (Multilateral Interoperability Programme) і дозволяють проводити мережево-центричні війни (МЦВ). Крім того, система є сумісною з аналогічними рішеннями, які використовують армії країн-членів НАТО. За словами співзасновника "Аеророзвідки" Ярослава Гончара, практично всі нові західні технології, які надають союзники України для відбиття російської агресії, автоматично інтегруються в систему "Дельта" [2].

Система побудована згідно з принципами "нульової довіри" (zero trust security), що забезпечує високий рівень безпеки. Вона також обладнана автоматизованим моніторингом для виявлення підозрілої активності і спроб несанкціонованого доступу. Перевірку користувачів системи "Дельта" проводиться відповідно до протоколу, визначеного Службою безпеки України.

З початку 2021 року кіберпідрозділи союзників України регулярно проводять тести системи "Дельта" для виявлення можливих вразливостей та ризиків витоку даних. Наприклад, у березні 2021 року було проведено захід "Hack Delta", під час якого кіберпідрозділ одного з союзників, відповідальний за кібербезпеку, проводив повне тестування системи для виявлення можливих вразливостей. У результаті цього тестування не було виявлено критичних або високоризикових загроз, і виявлені низькоризикові проблеми були відповідно виправлені розробниками.

Під час російського вторгнення в Україну, система "Дельта" активно використовувалася, зокрема під час оборони Києва, знищення крейсера "Москва", звільнення острова Зміїний і Слобожанського контрнаступу. До системи приєдналися Національна гвардія, прикордонники, Служба безпеки, Міністерство внутрішніх справ, територіальна оборона, оператори мобільного зв'язку і добровольці. За даними станом на травень 2022 року, кожного дня до системи приєднується 20-30 нових користувачів. Розробники стверджують, що кількість користувачів "росте з геометричною прогресією" [3].

12 березня 2022 року до цієї системи був доданий чат-бот "єВорог", розроблений Міністерством цифрової трансформації. Цей чат-бот дозволяв українцям надсилати фотографії та відео, що стосуються розташування російських військ і техніки, і після обробки цієї інформації вона подавалася до

системи "Дельта". За дев'ять місяців роботи цього чат-бота ним скористалися 433 тисячі українців, як повідомлялося Міністерством цифрової трансформації.

Пізніше до "Дельти" був інтегрований чат-бот "STOP Russian War", розроблений Службою безпеки України [4].

11 липня 2023 року Міністерство цифрової трансформації України повідомило, що систему "Дельта" успішно протестували з 15 системами з 10 країн, включаючи 3 системи, що розроблені безпосередньо НАТО. Також було протестовано 4 протоколи обміну даними, які використовуються для більшості сучасного озброєння, яке Україна отримує від західних партнерів. Основний протокол, який було протестовано, - це Link 16, що надає можливість отримувати дані в систему "Дельта" з винищувачів F-16.

Списки використаних джерел:

1. Аналіз мережоцентричної моделі застосування засобів ураження по даним повітряної розвідки / Б.М. Іващук, І.М. Зелінський, А.С. Небрат, О.О. Борщевський, О.М. Трисантович. Наука і техніка Повітряних Сил Збройних Сил України. — 2016. — № 3(24). С. 60-63.
2. Delta wiki. Delta. [Електронний ресурс]. URL: http://surl.li/muzgr.
3. Дельта (система ситуаційної обізнаності). Wikipedia. [Електронний ресурс]. URL: http://surl.li/muzhw.
4. Мельник Т. Військовий софт Delta тепер офіційно у ЗСУ. Forbes. [Електронний ресурс]. URL: http://surl.li/dzabg.

Ключові слова: інформаційно комунікаційні технології, захист комунікацій, мережево-центрична війна, Дельта.
Keywords: information and communication technologies, communications protection, network-centric warfare, Delta

Науковий керівник: к.т.н., доцент Задерейко О.В.

ВИДИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Орел Анастасія

студентка 1-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасному світі інформаційних технологій захист програмного забезпечення (ПЗ) стає все важливішим завданням у його розробці. З кожним роком технології все більше удосконалюються, відкриваючи все більше нових програмних рішень та можливостей. Разом з цим, зростає все більша загроза захисту ПЗ тому, що кіберзлочинці стають все винахідливішими. Через це

виникає потреба у розробці ефективних програмних рішень з ефективною та надійною системою захисту.

Одним із ключових методів захисту ПЗ є застосування технологій, які базуються на його прив'язці до параметрів комп'ютера. Цей підхід став необхідністю для забезпечення високого рівня безпеки та контролю над використанням програмних продуктів. Ця стратегія захисту дозволяє ПЗ взаємодіяти тільки з окремим користувачем, забезпечуючи таким чином його конфіденційність, неушкодженість та доступність.

Існують різні методи прив'язки ПЗ до параметрів комп'ютера. Ці методи включають в себе широкий спектр технічних, правових та організаційних відомостей, спрямованих на захист ПЗ від несанкціонованого доступу та зловмисних атак. Одним з них можна виділити метод, який для забезпечення захисту, використовує апаратні ключі або, так звані, токени, які зберігаються на комп'ютері користувача.

Цей метод забезпечує безпеку шляхом обмеження доступу до ПЗ при відсутності вірного ключа або токена. Апаратний ключ (інколи також називають електронним ключем) є спеціальним фізичним пристроєм, що за виглядом майже нічим не відрізняється від звичайної флешки, але на відміну від неї він може мати кілька застосувань:

· апаратний ключ може зберігати кваліфікований електронний підпис (КЕП), що гарантує цілісність даних та ідентифікацію користувача.

· він може використовуватись для ідентифікації користувача в різноманітних сервісах.

· може застосовуватися для двофакторної автентифікації, що надає додатковий рівень безпеки при вході в систему. Як приклад можна навести систему Google або Facebook [1].

Ще один метод захисту ПЗ полягає в можливості призначення ліцензії на основі IP-адреси або мережевих параметрів, що дозволяє обмежити доступ до нього з певних мереж або незареєстрованого обладнання. Завдяки такому підходу розробники ПЗ мають можливість надавати доступ до застосунку обмеженій кількості аудиторії, що має певну ліцензію [2].

Не дивлячись на те, що з першого погляду цей метод виглядає досить надійним у обмеженні доступу для несанкціонованих користувачів, він не є повністю непроникним. Навіть використовуючи доступ за IP-адресою, такий фільтр легко обійти за допомогою різних мережевих сервісів, що на деякий час здатні змінити IP користувача підробляючи її на необхідну.

Для підвищення надійності цього методу, рекомендується комбінувати його з іншими методами захисту, наприклад, з прив'язкою до апаратних ключів.

У випадку, коли потрібно обмежити доступ до ПЗ лише для окремих пристроїв, доступ можливо організувати за допомогою перевірки унікального ідентифікатора обладнання, такого як його серійний номер. Цей метод дозволяє забезпечити ліцензійне використання програми, запобігаючи її використанню на сторонніх пристроях [3].

Такий підхід не лише гарантує додатковий рівень захисту, а й те, що ПЗ використовується лише на легальних та зареєстрованих пристроях. Це особливо корисно для компаній та підприємств, які надають доступ до свого ПЗ обмеженій кількості пристроїв чи клієнтів.

Незважаючи на переваги захисту цього методу, в нього існує ряд недоліків. Однією з проблем є незручність у масовому користуванні ПЗ, оскільки кожен користувач повинен мати унікальний ключ. Це призводить до того, що ліцензійний ключ може потрапити до рук зловмисника, який може використати його для поширення піратських копій ПЗ.

Крім цього методу, ПЗ також може перевіряти апаратні характеристики комп'ютера, такі як тип процесора, обсяг оперативної пам'яті та інші параметри, для ідентифікації конкретної машини. Таким чином для кожного обладнання буде створено унікальний профіль, за допомогою якого буде можливим точно визначити на якому саме пристрої використовується ПЗ [4].

Порівнюючи з іншими методами захисту, обхід перевірки апаратних характеристик комп'ютера є найскладнішим завданням для нелегальних користувачів. Не дивлячись на це, цей метод може мати деякі незручності. Перш за все, при його використанні, користувач не матиме змогу користуватися застосунком на декількох пристроях, оскільки кожен з них матиме унікальні характеристики. Також можуть виникнути проблеми під час оновлення обладнання або його складових, оскільки при його зміні, ймовірно зміняться й апаратні характеристики, що може призвести до втрати доступу до ПЗ.

Усі зазначені методи здатні допомогти зберегти ПЗ від різноманітних небезпек та плагіату. Вони створюють додаткові шари захисту та унеможливлюють несанкціонований доступ або використання ПЗ. Не дивлячись на це жоден з цих методів не є вдосконалим та повністю непроникним для загроз.

Висновки. Для досягнення максимальної надійності та ефективності системи захисту, важливо їх комбінувати. Поєднання різних методів створює комплексний підхід до безпеки і створить надійніший рівень захисту від майбутніх загроз.

Список використаних джерел

1. Онацький О. В., Бірулін К.О. Протокол двофакторної автентифікації в системах управління доступом // Science, innovations and education: problems and

prospects”(January 13-15, 2022) CPN Publishing Group, Tokyo, Japan. 2022. In: The 6th International scientific and practical conference “ 705 p. 2022. p. 218.
2. González, Florencio J., et al. "Identification of Static and Dynamic Security Controls Using Machine Learning." Computación y Sistemas 27.2 (2023): 581-592. URL: https://cys.cic.ipn.mx/ojs/index.php/CyS/article/viewFile/4429/3550.
3. Han, Alex Heunhe, and Dong Hoon Lee. "Detecting Risky Authentication Using the OpenID Connect Token Exchange Time." Sensors 23.19 (2023): 8256. URL: https://www.mdpi.com/1424-8220/23/19/8256.
4. Пуздрановський І. В., Салієва О. В. Аналіз сучасних DRM-систем керування цифровими правами. Diss. ВНТУ, 2023. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/36889/122966.pdf.

Ключові слова: програмне забезпечення, програмні рішення, обмеження доступу, захист програмного забезпечення
Keywords: software, software solutions, access restrictions, software protection

Науковий керівник: к.т.н., доцент Задерейко О.В.

СПОСОБИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ЗА ДОПОМОГОЮ ЛОГ-ФАЙЛІВ

Раєв Олександр

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Аналіз і моніторинг лог-файлів є надійним і ефективним способом виявлення вторгнень в інформаційні системи, сприяючи підвищенню кібербезпеки та захисту важливих даних.

Способи виявлення вторгнень за допомогою лог-файлів, як-от аналіз змін у трафіку, виявлення аномалій і сигнатурний аналіз або евристичний аналіз, дають змогу ідентифікувати неавторизований доступ і атаки на інформаційні системи. Цей підхід допомагає забезпечити своєчасну реакцію на потенційні загрози, мінімізувати ризики та забезпечувати стабільну роботу мережі. Ефективне використання лог-файлів сприяє підвищенню загальної кібербезпеки та захисту конфіденційної інформації, надаючи змогу підприємствам і організаціям зберігати довіру користувачів та зберігати важливі дані недоступними для несанкціонованого доступу.

Виявлення вторгнень за допомогою лог-файлів поділяється на два основних методи:

1) Аналіз лог-файлів на основі сигнатур та евристики

2)Аналіз поведінки операційної системи

Аналіз лог-файлів на основі сигнатур та евристики

Аналіз лог-файлів на основі сигнатур є важливою складовою стратегії виявлення вторгнень, оскільки він дає змогу ідентифікувати конкретні шаб-

лони та відомі атаки з використанням уже наявних сигнатур атак. Цей метод, заснований на порівнянні активності в мережі з відомими атаками, допомагає виявити загрози, які раніше були відомі та вивчені, і надає можливість вчасно реагувати на них. Однак, важливо пам'ятати, що аналіз на основі сигнатур має свої обмеження, оскільки він не може виявити нові атаки або атаки, які модифікують свої сигнатури. Тому важливо комбінувати цей метод з іншими стратегіями виявлення вторгнень, такими як аналіз аномалій, для забезпечення комплексного захисту інформаційних систем.

Аналіз лог-файлів на основі евристики є потужним інструментом для виявлення вторгнень, оскільки він дає змогу виявити потенційно небезпечні зразки й аномалії, не обмежуючись конкретними сигнатурами атак. Цей метод дає змогу виявити навіть нові, раніше невідомі загрози, ґрунтуючись на виявленні нетипової або підозрілої активності в мережі або системі. Аналіз на основі евристики допомагає підвищити рівень кібербезпеки та зменшити ризик інцидентів, що стосуються безпеки інформаційних систем. Поєднуючи аналіз на основі евристики з іншими методами виявлення вторгнень, можна створити комплексну систему захисту, яка ефективно бореться з різними загрозами для безпеки даних і мереж[1].

Недоліки цього методу:

1) Потрібно тримати базу даних

2) Потрібно оновлювати базу даних

3)Погано справляється із атаками нульового дня (Zero day)

Аналіз системних журналів

Аналіз поведінки операційної системи є ключовим компонентом сучасних систем виявлення вторгнень, оскільки він дає змогу виявляти аномальну та підозрілу активність, що може бути пов'язана з потенційними вторгненнями або загрозами для безпеки даних і системи. Цей метод аналізу створює можливість виявити нові, раніше невідомі загрози, а також атаки, які можуть змінювати свою сигнатуру. Аналіз поведінки операційної системи базується на моніторингу та аналізі активності процесів, файлів, мережевого трафіку та інших системних подій, що дає змогу виявити аномалії та вчасно реагувати на них. Цей підхід відіграє важливу роль у забезпеченні кібербезпеки та захисту інформаційних систем від сучасних загроз.

Аналіз проводиться:

1) Характеристик систем
2) Вхідний та вихідний трафік
3) Системні журнали

Якщо є більше одного системного журналу то проводиться аналіз:

1) Операційної системи
2) Веб-сервера

3) Бази даних

4) Користувальницьких прогам

Перевагами такого аналізу є можливість зіставляти події та можливість знаходження Zero day активності.

Зіставлення подій в операційній системі є ефективним методом виявлення вторгнень і аналізу аномальних змін, сприяючи підвищенню кібербезпеки та безпеки даних. Цей підхід включає аналіз і порівняння послідовних подій, системних ресурсів, користувацької активності та мережевого трафіку, що дає змогу виявити навіть найсуб'єктивніші аномалії та сусідство подій, які можуть свідчити про інциденти безпеки. Зіставлення подій допомагає побудувати повну картину подій у системі, ідентифікувати потенційні загрози та діяти вчасно для запобігання негативним наслідкам для безпеки інформації та операційної системи.

Аналіз поведінки операційної системи та зіставлення подій у ній стали важливими складовими сучасних систем виявлення вторгнень і забезпечують вищий рівень кібербезпеки та захисту даних. Ці методи дають змогу виявити як відомі, так і нові загрози для безпеки інформації, а також аналізувати аномалії та сусідство подій, які можуть свідчити про атаки. Їхнє ефективне використання допомагає організаціям вчасно реагувати на потенційні інциденти безпеки, мінімізувати ризики та забезпечувати стабільну й безпечну роботу операційних систем та інформаційних систем загалом. Завдяки цим підходам, сучасні компанії та організації можуть зберігати довіру користувачів і надійно захищати свою інформацію від різних загроз кібербезпеки [2].

Аналіз лог-файлів є надійним і ефективним способом виявлення вторгнень в інформаційні системи. Комбінація аналізу лог-файлів на основі сигнатур, евристики та аналізу системних журналів забезпечує найбільший рівень захисту.

Список використаних джерел:

1. IBM [Електронний ресурс] – Режим доступу до ресурсу: https://www.ibm.com/topics/intrusion-detection-system
2. "Network behavior analysis of selected operating systems" [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/336578006_Network_behavior_analysis_of_selected_operating_systems.

Ключові слова: Лог-файли, веб-сервер, система, аналіз.
Keywords: Log-files, web server, system, analysis.

Науковий керівник: к.т.н., доцент Бойко В.Д.

АВТОМАТИЗАЦІЯ ПЕНТЕСТИНГУ ВЕБ-САЙТІВ ЗА ДОПОМОГОЮ МОВИ PYTHON

Жук Максим

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

На сьогоднішній день інформаційні технології є невід'ємною частиною життя нашого суспільства. Кожного дня через мережу Інтернет ми передаємо неймовірну кількість даних, які курсують по всьому світі. І у багатьох випадках ці дані є для нас важливими чи конфіденційними.

Системний адміністратор є важливою частиною схеми захисту даних, адже саме від нього залежить безпека конфіденційних даних тисяч людей. І на жаль, деколи, саме цей елемент схеми працює неправильно. Чи маючи недостатню компетентнійсть чи просто не розуміючись на захисті даних, системні адміністратори скоюють помилки, які можна було б запобігти простим пентестом.

Отже актуальною є потреба в простому, та дружному до користувача інструменті для пентесту веб-сайтів. Також бажаним є, щоб цей інструмент був кроссплатформеним, для можливості його експлуатації на різних системах. Такий інструмент буде орієнтуватися на зрозумілість для користувача та проводити тестування одних з найбільш поширених атак на веб-сайти та застосунки в світі. Вставляти в інструмент всі існуючі типи атак має мало сенсу, адже тоді інструмент буде занадто громіздким та користувач просто заплутається в типах атак. Тому ми виберемо найпоширеніші типи.

Якщо подивитися на статистику, можна визначити найчастіші типи та види атак. Наприклад, згідно зі статистикою Майкрософт по DDoS атакам за 2022 рік [1] на системи Microsoft здійснювалось в середньому 1 435 атак на день. Максимальна кількість атак за один день становила 2 215 атак 22 вересня 2022 року. Мінімальна кількість атак за день була 680 22 серпня 2022 року. Всього було виявлено понад 520 000 унікальних атак на глобальну інфраструктуру Microsoft протягом 2022 року [2].

Статистика 2022 року показує наступний розподіл уразливостей сайтів: SQL-ін’єкція є основним джерелом критичних вразливостей в веб-застосунках, знайдених у всьому світі в 2022 році (33 відсотка), за якими слідує 26,7 відсотків критичних вразливостей, пов'язаних із збереженими атаками межсайтового скрипта (cross site scripting). Та разом вони перекривають майже дві третини загального обсягу атак. Таким чином, найкращим варіантом буде

додавання до інструменту перевірку на захищеність від DDoS атак, SQL-ін'єкцій та XSS.

Пропонований інструмент планується, як рішення для системних адміністраторів, які не розуміються в побудовах систем безпеки для веб-сайтів та ніколи не мали справи з інструментами для тестування на проникнення. Через свою простоту та дружність до користувача він може стати гарним першим кроком для людини, яка нічого не розуміє в пентестах, у неї немає грошей на спеціаліста чи на інструмент та їй потрібно просто зараз провести просту перевірку свого веб-сайту на захист від найпоширеніших атак.

Хорошим варіантом для вирішення цього завдання буде використання мови Python та її вбудованих та зовнішніх бібліотек[3], які спростять написання утиліти. Зокрема, можна виділити такі бібліотеки: Scapy для аналізу та роботи з вмістом пакетів мережевого трафіку, Requests, що дозволяє генерувати http-запити, Beautiful Soup 4 – html/xml парсер, Socket – модуль, який забезпечує доступ до інтерфейсу сокетів BSD, а також пакети pwntools, IMpacket, Pexpect, Paramiko.

Робота такої утиліти має забезпечувати можливість двох режимів сканування:

· внутрішній, коли програма запускається безпосередньо на сервері, що забезпечує роботу веб-сайту та сканує його "зсередини";

· зовнішній, коли програма запускається поза сервером, що забезпечує роботу веб-сайту, отримує від користувача ціль для сканування та сканує сервер "зовні";

Розроблений інструмент повинен являти собою скрипт, що потенційно розширюється плагінами. Для цього також зручно використовувати функціонал мови Python, який дозволяє гнучко працювати з розширеннями або включаючи їх безпосередньо до дистрибутиву інструменту, або додаючи їх через функціонал штатних інструментів роботи із зовнішніми пакетами та бібліотеками (pip/venv).

Таким чином, запропонована утиліта має спростити та покращити процес пентестування для сайтів середнього рівня, що у свою чергу має позитивно позначитися на спільній безпеці веб-простору.

Список використаних джерел

1. 2022 in review: DDoS attack trends and insights URL: https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/#:~:text=The%20maximum%20number%20of%20attacks,our%20global%20infrastructure%20during%202022.
2. Distribution of web application critical vulnerabilities worldwide as of 2022 URL: https://www.statista.com/statistics/806081/worldwide-application-vulnerability-taxonomy/#statisticContainer

3. Python for pentesting: Programming, exploits and attacks | Infosec [Електронний ресурс]. – Режим доступу : https://resources.infosecinstitute.com/topics/general-security/python-for-pentesting-programming-exploits-and-attacks/ – Назва з екрана.

Ключові слова: пентест, ризики, кібербезпека.
Keywords: pentest, risks, cybersecurity.

Науковий керівник: к.т.н., доцент Бойко В.Д.

КІБЕРБЕЗПЕКА ЯК ФАКТОР ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Тишко Ілонна

студентка 3-го курсу факультету прокуратури та слідства Національного університету «Одеська юридична академія»

У сучасних умовах цифрової трансформації українського суспільства, важливим стає питання фінансової стійкості підприємств та їхньої кібербезпеки. Кілька років тому кібербезпека як елемент захисту від кіберзагроз підприємства не мала належного врегулювання на законодавчому рівні. Тільки після серії масштабних кібератак на державні установи, в тому числі на фінансові органи управління України, почалася активна робота у цьому напрямку. В економічному середовищі підприємства стикаються з різноманітними внутрішніми та зовнішніми кіберзагрозами, які мають негативний вплив на їхню фінансову стійкість та інвестиційну привабливість.

У сучасних умовах побудови бізнесу необхідно враховувати не лише конкурентні ризики, нововведення та боротьбу зі "шахраями бізнесу", що надають подібні послуги, але й внутрішню безпеку підприємства. Це означає, що внутрішня безпека підприємства пов'язана не лише з організаційними аспектами його діяльності, а й з ризиками, які створюють конкуренти, включаючи кібератаки та шахрайство.

О.І. Судакова визначає фінансову безпеку як важливу складову економічної безпеки підприємства. Ця безпека базується на незалежності, ефективності й конкурентоспроможності фінансів підприємства. Вона відображається через систему критеріїв і показників його стану, яка характеризує збалансованість фінансів, достатню ліквідність активів і наявність необхідних грошових резервів, фінансову стабільність, ступінь захищеності фінансових інтересів на всіх рівнях фінансових відносин [1].

У широкому розумінні, згідно із Законом України від 5 жовтня 2017 р. №2163-VIII "Про основні засади забезпечення кібербезпеки України", "кіберзагроза" означає наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кібер-

просторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів [2]. У вузькому розумінні, кіберзагроза у фінансовій діяльності підприємства - це втручання у операційну діяльність підприємства, що веде до втрат фінансових ресурсів, і відповідно впливає на інтереси як власників, так і інвесторів. Таким чином, одним із проявів порушення фінансової безпеки підприємства є кіберзагрози.

Сфера кібербезпеки, як частина інформаційної безпеки будь-якого суб'єкта господарювання, є одним із головних пріоритетів майбутнього розвитку підприємств. Важливо зазначити, що довгий час причиною вразливості бізнесу була недооцінка можливих загроз.

Згідно з дослідженням "EY Global Information Security Survey 2018-19" (GISS), проведеним компанією EY (Ernst & Young) та опублікованим на офіційному сайті, встановлено, що 77% респондентів мають базовий набір інструментів для забезпечення кібербезпеки. У більшості компаній не відомо, де саме зберігаються найбільш критичні інформаційні активи, й вони не мають гарантій щодо їхньої безпеки. Згідно з дослідженням GISS, 77% організацій планують не тільки встановити основні засоби кібербезпеки, а й налаштувати їх відповідно до можливостей та умов бізнесу. Такі компанії не лише впроваджують базові засоби кібербезпеки, а й переглядають принципи та архітектуру кібербезпеки, щоб ефективніше підтримувати діяльність бізнесу [3].

Основні втрати для діяльності підприємства, спричинені кібератаками, включають: втрату інтелектуальної власності; втрату бізнес-інформації; порушення безперебійності роботи IT-систем; шкоду репутації в результаті атак; втрату персональних даних, що зберігаються в комп'ютерних системах. Кожна з цих втрат негативно відображається на діловій активності підприємства, яка, в свою чергу, є елементом фінансових показників інвестиційної привабливості підприємства. Важливо зазначити, що поняття фінансової безпеки, як кількісного і якісного обумовлення фінансового стану, нерозривно пов'язане з рівнем інвестиційної привабливості підприємства, оскільки інвестори, вкладаючи кошти, мають на меті їх примноження з урахуванням безпечності їх залучення.

Серед найбільш поширених кібератак слід виділити такі:

- Фішинг: Ця атака переважно використовує електронну пошту як вектор і шляхом обману змушує людей завантажувати шкідливі програми на свої пристрої. У 2021 році близько 60% підприємств стали жертвами фішингу.

- Витік даних: Цей вид атаки відбувається, коли конфіденційна інформація користувача стає доступною зловмисникам. У 2021 році багато компаній повідомили про витоки даних, і очікується, що ця тенденція буде триматися й надалі.

Кібератаки набувають більшої сили і стають частішими у сфері малого та середнього бізнесу, оскільки такі компанії помилково вважають себе "нецікавими" у плані інформаційних ресурсів, якими володіють. Тільки протягом 2021 року правоохоронними органами було зареєстровано 11,3 тис. кримінальних проваджень щодо порушення кібербезпеки, виявлено 6 тис. правопорушень у сфері використання інформаційних технологій, розкрито діяльність 11 організаційних груп та 8 транснаціональних хакерських угрупувань.

Важним заходом для запобігання цьому є проведення профілактичних заходів. Необхідно постійно підвищувати обізнаність персоналу підприємства, відповідального за безпеку від таких атак, а також проводити тести. Варто також впроваджувати антифішингове програмне забезпечення та підвищувати рівень аутентифікації електронної пошти. Як тільки відбувається витік даних, компаніям необхідно негайно вживати заходів, щоб захистити свій репутацію і уникнути серйозних штрафів. Зазвичай про порушення стає відомо через внутрішні записи, повідомлення від банків, правоохоронних органів або сповіщення клієнтів. [4]

Досить відомим став випадок атаки в США, коли хакери отримали номери кредитних карт 40 мільйонів клієнтів з бази даних магазину Target, зламавши облікові дані постачальника послуг для Target - HVAC. Цей інцидент не лише був одним із найбільших в історії роздрібної торгівлі США, але й нагадав світові, як зловмисники можуть використовувати недостатньо захищені малий та середній бізнес як точку входу до великих корпорацій.

Отже, кібербезпека суттєво впливає на фінансову безпеку підприємства. Встановлено, що існує прямий зв'язок між достатнім рівнем фінансової стійкості підприємства і необхідним рівнем його кіберстійкості, який відображається у фінансових показниках підприємства та його привабливості для потенційних інвесторів. Забезпечення необхідного рівня кібербезпеки, захисту інформаційних ресурсів підприємств та запобігання несанкціонованому втручанню в операційну діяльність позитивно впливає на інвестиційну привабливість, яка відіграє вагому роль у підвищенні конкурентоспроможності підприємства, приваблені інвестицій, а також у зміцненні загалом економічної системи країни та гарантуванні захищеності економічних інтересів України. Таким чином, інформація є надзвичайно важливим ресурсом, який, як правило, може зацікавити зловмисників. Вони можуть отримати доступ до цієї інформації за допомогою кібератак, від яких ні бізнес, ні державний сектор не є повністю захищеними.

Список використаних джерел:

1. Судакова О.І. Стратегічне управління фінансовою безпекою підприємства. Економічний простір. 2008. № 9. С. 140-148.

2. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 р. №2163-VIII. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Маковець О.П. та Дрозд І.К.. «КІБЕРБЕЗПЕКА ЯК ФАКТОР ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА». ECONOMICS. FINANCES. LAW. 2020. № 5/3. Ст.31-35. [Електронний ресурс]. URL: http://efp.in.ua/uk/journal-article/442
4. Бутіна М. Юрист АО «Uniminds». «Кібербезпека підприємства: що врахувати?». [Електронний ресурс]. URL: https://jurliga.ligazakon.net/news/209245_kberbezpeka-pdprimstva-shcho-vrakhuvati

Ключові слова: кібербезпека, кібербезпека підприємства, фінансова безпека підприємства.
Keywords: cyber security, cyber security of the enterprise, financial security of the enterprise.

Науковий керівник: к.ю.н., доцент Добровольська В.В.

ВИЯВЛЕННЯ ЗЛОВМИСНОЇ АКТИВНОСТІ В КОРПОРАТИВНИХ ЛОКАЛЬНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ АНАЛІЗУ DNS-ЗАПИТІВ

Гуренко Марк

студент 4 курсу факультету кібезбезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасному цифровому просторі корпоративні локальні мережі постійно піддаються незліченній кількості кіберзагроз. Від зараження шкідливим програмним забезпеченням до витоку даних; організації повинні застосовувати надійні заходи безпеки, щоб захистити свої активи.

Одним із таких заходів є аналіз DNS-запитів, який зарекомендував себе як ефективний метод виявлення зловмисних дій у корпоративних мережах[1]. Ефективний аналіз DNS-запитів починається з повного ведення DNS-журналу. Всі DNS-запити і відповіді в корпоративній мережі повинні реєструватися, включаючи IP-адреси джерела і призначення, типи запитів і часові мітки. Ці дані є основою для аналізу.

Моніторинг DNS-трафіку в режимі реального часу має вирішальне значення для виявлення загроз і швидкого реагування на них. Необхідно мати інструменти та системи для постійного моніторингу DNS-трафіку на предмет виявлення будь-яких аномалій або підозрілих патернів.

Необхідно проводити регулярний аналіз даних DNS. Це включає аналіз минулих даних для виявлення тенденцій і закономірностей, а також аналіз у режимі реального часу для виявлення безпосередніх загроз.

При виявленні зловмисної активності важливе значення має своєчасне звітування. Звіти слід створювати та передавати відповідним зацікавленим сторонам, включаючи IT-команди, групи реагування на кіберінциденти тощо.

Швидке звітування дозволяє швидко реагувати на інциденти та стримувати загрози.

Платформи SIEM мають вирішальне значення для централізації та кореляції даних, пов'язаних з безпекою, з різних джерел, включаючи DNS-журнали. Вони надають цілісне уявлення про мережеву безпеку, аналізуючи дані з різних сторін [2].

Інтеграція інструментів аналізу DNS з SIEM дозволяє співвідносити дані DNS з іншими подіями безпеки, такими як журнали брандмауера та сповіщення системи виявлення вторгнень (IDS). Ця кореляція може допомогти виявити складні патерни атак, які можуть бути неочевидними при ізольованому аналізі DNS-даних.

SIEM-системи можуть генерувати оповіщення на основі попередньо визначених правил і порогових значень. Наприклад, якщо виявлено незвичний сплеск DNS-трафіку в поєднанні з підозрілими подіями брандмауера, може бути запущено оповіщення для негайного розслідування [3].

У разі кіберінциденту дані DNS можуть бути безцінними для криміналістичного аналізу, допомагаючи відстежити походження та масштаби атаки.

Дотримуючись цих практик, організації можуть максимізувати ефективність аналізу DNS-запитів як критично важливого компонента своєї стратегії мережевої безпеки. Інтеграція з платформами SIEM, а також зосередженість на навчанні, дотриманні політик і регулярних оновленнях допомагають створити надійний захист від нових кіберзагроз у корпоративних локальних мережах.

Отже, аналіз DNS-запитів є потужним інструментом для виявлення та усунення зловмисної активності в корпоративних локальних мережах. Розуміння основ функціонування DNS, використання ефективних методів виявлення та дотримання кращих практик є важливими для посилення мережевої безпеки. Використовуючи аналіз DNS-запитів, організації можуть посилити свій захист від широкого спектру кіберзагроз, в кінцевому підсумку захистивши свої цінні активи і підтримуючи цілісність своїх мереж.

Список використаних джерел:

1. What is DNS Monitoring and Why is it Important? [Електронний ресурс]. – Режим доступу : https://www.pagerduty.com/resources/learn/dns-monitoring/ – Назва з екрана.
2. Adiwal S. et al. DNS Intrusion Detection (DID) A SNORT-based solution to detect DNS Amplification and DNS Tunneling attacks // Franklin Open. Elsevier BV, 2023. Vol. 2. P. 100010.
3. Basheer Al-Duwairi, Wafaa Al-Kahla, Mhd Ammar AlRefai, Yazid Abdelqader, Abdullah Rawash, Rana Fahmawi SIEM-based detection and mitigation of IoT-botnet

DDoS attacks. International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 2, Квітень 2020, С. 2182-2191

Ключові слова: DNS, CC, C2 сервери, DGA, DNS Sinkhole, ML, машинне навчання, IoT ботнети, мережева безпека, SIEM
Keywords: DNS, CC, C2 servers, DGA, DNS Sinkhole, ML, Machine Learning, IoT botnets, Network security, SIEM

Науковий керівник: к.т.н., доцент Бойко В.Д.

ДОСЛІДЖЕННЯ MALWARE З ВИКОРИСТАННЯМ МЕТОДІВ ВКЛАДЕНОЇ ВІРТУАЛІЗАЦІЇ

Величканич Юрій

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Для подальшого захисту інформаційних систем перед обличчям постійно зростаючих вірусних і шкідливих програмних загроз важливо мати інструменти, здатні виявляти і аналізувати нові загрози, а також розуміти їх поведінку. Ця проблема зазвичай вирішується за допомогою традиційних методів антивірусного захисту, сигнатурних сканерів та евристичних алгоритмів. Однак з появою більш витончених типів шкідливих програм традиційні методи стають менш ефективними.

Запропоноване рішення, полягає у використанні технології вкладеної віртуалізації (Encapsulated VM - EVM) для створення ізольованих середовищ для аналізу шкідливого програмного забезпечення (ШПЗ). Це дозволить точніше вивчати та аналізувати поведінку шкідливих програм, при цьому знижуючи ризики зараження критично важливих систем.

Можна виділити дві основні категорії методів дослідження шкідливих програм [1]:

· Статичні методи, які досліджують ШПЗ без його виконання. Це робиться шляхом аналізу коду, метаданих або інших статичних характеристик шкідливого програмного забезпечення.

· Динамічні методи, які досліджують ШПЗ, запускаючи його в контрольованому середовищі. Це дозволяє спостерігати за поведінкою ШПЗ і збирати інформацію про його поведінку.

До статичних методів дослідження шкідливих програм за допомогою EVM належать:

· Аналіз сигнатур - процес пошуку відомих ознак ШПЗ в програмі;

· Евристичний аналіз - процес виявлення malware, що спирається на підсумовування обґрунтованих гіпотез на основі поведінки ШПЗ, та може ви-

явити нові шкідливі об’єкти, для яких наразі немає записів у базі даних програми;

· Аналіз метаданих - пошук ознак ШПЗ в метаданих програми, таких як ім'я файлу, розмір файлу і дата створення.

Динамічні методи дослідження ШПЗ включають:

· Поведінковий аналіз - це спостереження за поведінкою запущеного ШПЗ, яке дозволяє виявити потенційні шкідливі дії;

· Аналіз пам'яті - це процес аналізу пам'яті (або дампу пам'яті) яку використовує ШПЗ під час виконання. Він дозволяє виявити приховані ознаки ШПЗ, які неможливо побачити під час статичного аналізу.

· Мережевий аналіз - це процес спостереження за мережевою активністю під час виконання ШПЗ, який дозволяє визначити поведінку та цілі використання ШПЗ.

З перерахованих вище методів мережевий аналіз є найбільш оперативним і найменш витратним - ШПЗ у будь-якому випадку потрібен інформаційний обмін, оскільки йому потрібно ділитися зібраною інформацією, здійснювати атаки та приймати команди ззовні. Тому аналіз мережевої активності ШПЗ - найбільш інформативний і майже завжди оптимальний за співвідношенням витрат ресурсів та часу аналіз.

Проте, практично такий аналіз стикається з наступними проблемами.

По-перше, це активний тип аналізу, отже ШПЗ потрібно запустити. Враховуючи потенційну шкідливість ШПЗ, вкрай небажано робити це на робочій машині. Отже, потрібно використовувати віртуальну машину.

По-друге, метод аналізу ШПЗ шляхом запуску серед віртуальної машини не є таємницею для авторів ШПЗ, тому ШПЗ може бути забезпечено спеціальними системами на цей випадок.

В [2] проведено аналіз та показано, що шкідливі програми, які знають про віртуальні машини, зазвичай намагаються зробити наступне:

· Визначити, чи працює воно на віртуальній машині.

· Вимкнути або змінити функції віртуальної машини, які можуть бути використані для аналізу.

· Захищають себе від аналізу.

Для вирішення проблеми дослідження шкідливих програм за допомогою вкладеної віртуалізації пропонується використання спеціальної віртуальної машини (EVM) яка може працювати всередині інших VM. Це забезпечує багаторівневу ізоляцію і дозволяє аналізувати шкідливе програмне забезпечення в контрольованому середовищі.

Це дозволить запускати ШПЗ забезпечення в контрольованому середовищі, знижуючи ризик зараження хостів і мереж. Також технологія EVM забезпечить гнучкість дозволяючи налаштовувати середовище аналізу ШПЗ

відповідно до власних потреб, та підвищити ефективність процесу аналізу, дозволяючи дослідникам запускати кілька ВМ одночасно.

Таким чином використання технології EVM дозволить покращити та підвищити ефективність та безпеку технологій аналізу ШПЗ.

Список використаних джерел:

1. Rami S., Khairuddin O., K. A. Z. Ariffin. Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid, and Memory Analysis https://www.researchgate.net/publication/328760930_A_Survey_on_Malware_Analysis_Techniques_Static_Dynamic_Hybrid_and_Memory_Analysis
2. A. Pektaş, T. Acarman. A dynamic malware analyzer against virtual machine aware malicious software https://www.researchgate.net/publication/259542937_A_dynamic_malware_analyzer_against_virtual_machine_aware_malicious_software

Ключові слова: відкрите програмне забезпечення, відкриті формати даних, відкриті протоколи взаємодії, загрози і ризики, освіта.
Keywords: open software, open data formats, open communication protocols, threats and risks, education.

Науковий керівник: к.т.н., доцент Бойко В.Д.

HOLOMORPHIC IMMERSIONS OF COMPLEX MANIFOLDS

Josef Mikeš Professor

Doctor Sciences in Physics Mathematics
Department of Algebra and Geometry
Faculty of Science of the Palacky University (Czechia)

Exploration of Complex submanifolds of locally conformal Kähler manifolds was began in [2]. We continue the study.

A Hermitian manifold M^n, is called a locally conformal Kähler manifold (LCK - manifold) if there is an open cover $\mathsf{U} = \{U_\alpha\}_{\alpha\in A}$ of the manifold M and a family of such functions $\Sigma = \{\sigma_\alpha : U_\alpha \to \mathsf{R}\}_{\alpha\in A}$ that $\{g|_{U_\alpha}, \hat{g}_\alpha = e^{-2\sigma_\alpha} g|_{U_\alpha}\}$ is a Kählerian structure for any $\alpha\in A$. Transition from a metric $g|_{U_\alpha}$ to a metric $e^{-2\sigma_\alpha} g|_{U_\alpha}$ is reffered to as local transformation of the structure. The function σ is called defining function of the conformal transformation [2]. It is known, that on LCK-manifold Lee form, whose components are defined as [2]:

$$\omega = \frac{1}{m-1}\delta\Omega \quad \textit{або} \quad \omega_i = -\frac{2}{n-2} J^\alpha_{\beta,\alpha} J^\beta_i, \tag{1}$$

Have to be closed:

$$d\omega = 0.$$

A covariant derivative of the almost Complex structure with respect to a Levi-Civita connection of the LCK-manifold might be found by the formula:

$$J^k_{i,j} = \frac{1}{2}(\delta^k_j J^\alpha_i \omega_\alpha - \omega^k J_{ij} - J^k_j \omega_i + J^k_\alpha \omega^\alpha g_{ij}). \tag{2}$$

Let (M^{2m}, J, g) be a complex m-dimensional Hermitian manifold, g is it's Hermitian metric, J is it's comlex structure. Consider an immersion of a m-dimensional manifold

$$\Psi : \overline{M}^k \to M^{2m}$$

Let ∇ and $\overline{\nabla}$ be operators of covariant differentiations on the vector bundle $T(M^{2n})$ and $T(\overline{M}^k)$, respectively. Then the Gauss and Weingarten [1,3,4] formulas are given by

$$\nabla_X Y = \overline{\nabla}_X Y + h(X,Y), \tag{3}$$

$$\nabla_X \xi = -A_\xi X + \nabla^\perp_X \xi, \tag{4}$$

holds for any $X, Y \in T(\overline{M}^k), \xi \in E(\Psi)$. Here $T(\overline{M}^k)$ and $E(\Psi)$ are the tangent and normal bundles respectively on the immersed manifold $\overline{M}^k$. Also we denote by $h(X,Y)$ the second quadratic form and finely A_ξ denotes the Weingarten operator. The integrability conditions for the equations (3) and (4) are

$$g(R(X,Y)Z,W) = \overline{g}(\overline{R}(X,Y)Z,W) - g(h(X,W),h(Y,Z)) + g(h(Y,W),h(X,Z)), \tag{5}$$

$$nor\{R(X,Y)Z\} = (\overline{\nabla}_X h)(Y,Z) - (\overline{\nabla}_Y h)(X,Z), \tag{6}$$

$$g(R(X,Y)\xi,\eta) = g(R^\perp(X,Y)\xi,\eta) - g([A_\xi, A_\eta]X,Y) \tag{7}$$

For any $X, Y, Z \in T(M^k), \xi, \eta \in E(\Psi)$. Here R, $R^\perp$ and $\overline{R}$ are the curvature tensors for the connections ∇, $\nabla^\perp$ respectively $\overline{\nabla}$, $nor\{R(X,Y)Z\}$ is the vertical component of $R(X,Y)Z$. The equations (5), (6) and (7) are reffered to as the Gauss, Weingarten and Peterson-Codazzi formulas.

We call a manifold $\overline{M}^k$ $CR-$*submanifold of* a manifold (M^{2m}, J, g), if $\overline{M}^k$ carries C^∞- distribution D such that

1. D is holomorphic (i.e., for any $x \in \overline{M}^k$ $J_x(D_x) = D_x$)
2. The orthogonal component $D^\perp$ respect to the metric $\overline{g} = \Psi^* g$ to D y $T(\overline{M}^k)$ is anti-invariant (i.e. тобто, for any $x \in \overline{M}^k$ $J_x(D^\perp x) \subseteq E(\Psi)_x$)[3].

Let $(\overline{M}^k, D)$ is a $CR-$submanifold of a Hermitian manifold M_0^{2m}. Let us denote o $p = dim_{\mathbb{C}} D_x$ and $p = dim_{\mathbb{R}} D^\perp_x$ for any $x \in \overline{M}^k$ that so $2p + q = k$. If $q = 0$, then $\overline{M}^k$ is a complex submanifold and an immersion Ψ is holomorphic(analytic). If $p = 0$ then $\overline{M}^k$ is anti-invariant, i. e. for any $x \in \overline{M}^k$ $J_x(D^\perp_x) \subseteq E(\Psi)_x$. A $CR-$submanifold $(\overline{M}^k, D)$ is a proper one if $p \neq 0$ and $q \neq 0$. Also, $(\overline{M}^k, D)$ is generic, if $q = 2m - k$, i.e. for any $x \in \overline{M}^k$

$J_x(D_x^{\perp}) = E(\Psi)_x$.

A submanifold $\overline{M}^k$ of a manifold (M^{2m}, J) is totally real if, якщо

$$T_x(\overline{M}^k) \cap J_x(T_x(\overline{M}^k)) = \{0\}$$

For any point $x \in \overline{M}^k$. Note that any anti-invariant manifold is a totally real one. Any orientable surface in any point $x \in M^{2m-1}$ of (M^{2m}, J, g_0) is a generic $CR-$submanifold of (M^{2m}, J, g).

Let is immersed M^k into LCK-manifold M^{2m}

$$\Psi : \overline{M}^k \to M^{2m},$$

So that $k = 2p$ and for any $x \in \overline{M}^{2p}$

$$J_x(T_x(\overline{M}^{2p})) = T_x(\overline{M}^{2p}). \tag{8}$$

Then let the immersion is presented by functions

$$x^{\alpha} = x^{\alpha}(y^1, ..., y^{2p}), \tag{9}$$

where $\alpha = 1, ..., 2m$ are local coordinats on M^{2m}, and y^i, $i = 1, ..., 2p$ are local coordinats on $\overline{M}^{2p}$. Then the tangent space to the manifold $\overline{M}^{2p}$ in a point $x = x(y)$ is a linear combination of vectors

$$B_i^{\alpha} = \partial_i x^{\alpha}. \tag{10}$$

If $g_{\alpha\beta}$ is the metric tensor on M^{2m}, then because of (10), the induced metric $\overline{g}_{ij}$, induced on $\overline{M}^{2p}$ might written as

$$\overline{g}_{ij} = B_i^{\alpha} g_{\alpha\beta} B_j^{\beta}. \tag{11}$$

Also there are the next one useful mixed tensor

$$B_{\alpha}^i = B_j^{\beta} \overline{g}^{ij} g_{\alpha\beta}, \tag{12}$$

where $\overline{g}^{ij}$ is tensor whose matrix is inversed to the matrix of the induced metric tensor $\overline{g}_{ij}$. Then

$$B_{\alpha}^i B_j^{\alpha} = \delta_j^i, \tag{13}$$

and operator

$$P_{\alpha}^{\beta} = B_{\alpha}^i B_i^{\beta}, \tag{14}$$

defined on $T_x(M^{2m})$ is projector onto tangent space $T_x(\overline{M}^{2p})$. If

$$\overline{J}_i^j = J_{\beta}^{\alpha} B_{\alpha}^j B_i^{\beta}, \tag{15}$$

then because of (14) and (15) we get

$$\overline{J}_i^j \overline{J}_j^k = -\delta_j^k,$$

i.e. the affinor $\overline{J}_i^j$ defined on $T(\overline{M}^{2p})$ is the almost complex structure of the manifold $\overline{M}^{2p}$. From (11) and (15) it follows that

$$\overline{J}_k^j \overline{g}_{ij} \overline{J}_l^i = \overline{g}_{ij},$$

hence, the metric (11) is Hermitian. The Christoffel symbols for the connection $\overline{\nabla}$

respect to the metric $\overline{g}_{ij}$ we write as follows:

$$\overline{\Gamma}^h_{jk} = B^h_\alpha (B^\beta_j B^\gamma_k \Gamma^\alpha_{\beta\gamma} + \partial_j B^\alpha_k)$$

In local coordinats (9) the Gauss and Weingarten formulas (3), (4) might be written:

$$\overline{\nabla}_j B^\alpha_i = H_{ij(x)} C^\alpha_{(x)}; \tag{16}$$

$$\overline{\nabla}_j C^\alpha_{(x)} = -H^i_{j(x)} B^\alpha_i + L_{j(xy)} C^\alpha_{(y)}; \tag{17}$$

Here $H_{ij(x)}$ are the components of the second fundamental tensor of the manifold $\overline{M}^{2p}$, $C^\alpha_{(x)}$ are coordinats of normal vectors $x = \overline{2p+1,2m}$, and $L_{j(xy)} = (\overline{\nabla}_j C^\alpha_{(x)}) C^\beta_{(y)} g_{\alpha\beta}$.

Let us calculate the covariant derivative of the complex structure (15) respect to the conection $\overline{\nabla}$:

$$\overline{\nabla}_k \overline{J}^j_i = (\overline{\nabla}_k J^\alpha_\beta) B^j_\alpha B^\beta_i + J^\alpha_\beta (\overline{\nabla}_k B^j_\alpha) B^\beta_i + J^\alpha_\beta B^j_\alpha \overline{\nabla}_k B^\beta_i.$$

Taking into account (16) we get:

$$\overline{\nabla}_k \overline{J}^j_i = B^\gamma_k (\nabla_\gamma J^\alpha_\beta) B^j_\alpha B^\beta_i + J^\alpha_\beta H^j_{k(x)} C_{\alpha(x)} B^\beta_i + J^\alpha_\beta B^j_\alpha H_{ki(x)} C^\beta_{(x)}.$$

Since the immersion of a submanifold $\overline{M}^{2p}$ is complex, then (8) holds and hence the second and the third items in the right hand side are equal to zero. Hence, finelly we get:

$$\overline{\nabla}_k \overline{J}^j_i = B^\gamma_k B^j_\alpha B^\beta_i \nabla_\gamma J^\alpha_\beta. \tag{18}$$

Calculate the Nijenhuis tensor for the manifold $\overline{M}^{2p}$:

$$\overline{N}^h_{ij} = \overline{J}^t_i (\overline{\nabla}_t \overline{J}^h_j - \overline{\nabla}_j \overline{J}^h_t) - \overline{J}^t_j (\overline{\nabla}_t J^h_i - \overline{\nabla}_i \overline{J}^h_t)$$

Substitute (15) and (18)in the latter eqution. We obtain.

$$\overline{N}^h_{ij} = J^\alpha_\beta B^t_\alpha B^\beta_i (B^\gamma_t B^h_\delta B^\lambda_j \nabla_\gamma J^\delta_\lambda - B^\lambda_j B^h_\delta B^\gamma_t \nabla_\lambda J^\delta_\gamma) - J^\alpha_\lambda B^t_\alpha B^\lambda_j (B^\gamma_t B^h_\delta B^\beta_i \nabla_\gamma J^\delta_\beta - B^\beta_i B^h_\delta B^\gamma_t \nabla_\beta J^\delta_\gamma)$$
$$= B^\beta_i B^\lambda_j B^h_\delta B^t_\alpha B^\gamma_t (J^\alpha_\beta (\nabla_\gamma J^\delta_\lambda - \nabla_\lambda J^\delta_\gamma) - J^\alpha_\lambda (\nabla_\gamma J^\delta_\beta - \nabla_\beta J^\delta_\gamma))$$

One knows that the operator defined by (14) is projector onto the tangent space $T_x(\overline{M}^{2p})$. Hence

$$\overline{N}^h_{ij} = B^\beta_i B^\lambda_j B^h_\delta (J^\alpha_\beta (\nabla_\alpha J^\delta_\lambda - \nabla_\lambda J^\delta_\alpha) - J^\alpha_\lambda (\nabla_\alpha J^\delta_\beta - \nabla_\beta J^\delta_\alpha)),$$

i.e.

$$\overline{N}^h_{ij} = B^\beta_i B^\lambda_j B^h_\delta N^\delta_{\beta\lambda}, \tag{19}$$

where $N^\delta_{\beta\lambda}$ is the Nijenhuis tensor for the manifold M^{2m}. Since the latter is Hermitian, we have $N^\delta_{\beta\lambda} = 0$. Then $\overline{M}^{2p}$ is Hermitian too.

Let us take into account that M^{2m} is an LCK-manifold. Then, substitute from (2) in (18)

$$\overline{\nabla}_k \overline{J}^j_i = B^\gamma_k B^j_\alpha B^\beta_i \nabla_\gamma J^\alpha_\beta = B^\gamma_k B^j_\alpha B^\beta_i \frac{1}{2} (\delta^\alpha_\gamma J^\delta_\beta \omega_\delta - \omega^\alpha J_{\beta\gamma} - J^\alpha_\gamma \omega_\beta + J^\alpha_\delta \omega^\delta g_{\beta\gamma}). \tag{20}$$

Because of (10)-(15) from (20) it follows that

$$\overline{\nabla}_k \overline{J}_i^j = \frac{1}{2}(\delta_k^j \overline{J}_i^p \overline{\omega}_p - \overline{\omega}^j \overline{J}_{ik} - \overline{J}_k^j \overline{\omega}_i + \overline{J}_p^j \overline{\omega}^p \overline{g}_{ik}), \quad (21)$$

where $\overline{\omega}_i = B_i^\gamma \omega_\gamma$. Hence from (21) and also from the fact that for immersions the identity

$$d\Psi^* \omega = \Psi^* d\omega = 0,$$

holds, we obtain the theorem.

Theorem *If there exist a holomorphic immersion* $\Psi : \overline{M}^{2p} \to M^{2m}$*, where* $\overline{M}^{2p}$ *is a complex manifold and* $\overline{M}^{2p}$ *is an LCK-manifold, then the immersed manifold is also an LCK-manifold. In particular, if the Lee field is normal to* $\overline{M}^{2p}$*, then immersed manifold is* Kählerian*.*

The theory of immersions might be very useful if we apply it to statistical manifolds and informational geometry.

List of References:

1. Yano K. Differential geometry on complex and almost complex spaces /K. Yano--New York: Pergamon Press Book -- 1965, 326p.
2. I. Vaisman A geometric condition for an l.c.K. manifold to be Kähler// Geometriae Dedicata, 10 (1981), 129-134.
3. Yano K. Kon M. Structures on manifolds /K. Yano--Singapore : World Scientific Pub., -- 1984, 508p.
4. Mikeš J. at al. Differential geometry of special mappings. /J. Mikeš -- Olomouc: Palacky University, 2015, 566 p.
5. Cherevko Y., Chepurna O. Complex and Real Hypersurfaces of Locally Conformal Kähler Manifolds/Cherevko Y//Proceedings of the Eighteenth International Conference on Geometry, Integrability and Quantization, Ivanlo M. Mladenov, Guowu Meng and Akira Yoshioka, eds. (Sofia: Avangard Prima, 2017), p. 117 - 129. URL: http://projecteuclid.org/euclid.pgiq/1484362819

Keywords: almost Hermitian manifolds, Hermitian metric, submanifold, holomorphic immersion, LCK-manifold.

БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ В АРХІТЕКТУРІ СИСТЕМИ ОРКЕСТРАЦІЇ КЛАСТЕРІВ

Астахов Даниїл

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

В сьогоднішньому світі все більше і більше набувають популярність системи оркестрації, найвідомішою з них є система Kubernetes. Kubernetes, також відомі як K8s, є відкритим джерелом системи для автоматичного розгортання, шпильки, і управління контейнеризаційними застосунками. Але чи-

стий Kubernetes без належної конфігурації може бути дуже уразливим через деякі «проломи» в системі безпеці.

Проблемою в неправильно налаштованій системі безпеці Kubernetes є втручання в систему напряму через хмарний сервіс, де налаштований кластер та додатки, які підтримуються цією системою. Є безліч варіантів рішення цієї проблеми на різних етапах проекту: build phase security(фаза будування), deployment phase security(фаза розгортання), runtime phase security(фаза запуску). Розглянемо найпоширеніші:

1. Фаза будування

Рішення перше: збереження змінних середовища, які мають вразливу інформацію про дані користувачів, паролі, ключі тощо на віддаленому ресурсі на прикладі системи збереження змінних середовища Doppler чи на прикладі збереження.

Рішення друге: інтеграція безпеки в конвеєри CI/CD. Треба автоматизувати повторюваний аспект безпеки і генерувати сповіщення про серйозні уразливості, які можна виправити. Система CI допомагає зменшити ризик витоку інформації через фактор людини, тому що дії по будуванню проекту виконує певний скрипт, який повторює усі необхідні дії без втручання розробника, тому немає зайвого використання паролів, ключів тощо.

2. Фаза розгортання

Рішення перше: авторизація, по-перше, до хмарного ресурсу, де зберігається кластер системи оркестрації Kubernetes – додавання тільки потрібних користувачів в IAM (Identity and Access Management (IAM) — це веб-служба, яка допомагає безпечно контролювати доступ до ресурсів. За допомогою IAM ви можете централізовано керувати дозволами, які контролюють, до яких ресурсів мають доступ користувачі, хто пройшов автентифікацію (увійшов) і авторизований (має дозволи) на використання ресурсів). А, по-друге, авторизація всередині Kubernetes, а саме RBAC, в свою чергу, RBAC контролює авторизацію облікових записів користувачів і сервісів для доступу до сервера Kubernetes API кластера. Що

Рішення друге: використання мережевих політик. Kubernetes дозволяє кожному модулю зв’язуватися з кожним іншим подом за замовчуванням. Але треба використовувати політики та налаштування для того щоб фільтрувати вхідний та вихідний трафік та обмежувати комунікацію між контейнерами та сервісами, що підвищує безпеку.

3. Фаза запуску

Рішення перше: безпека застосунків. Безпека застосунків включає в себе використання контейнерних образів тільки з надійних репозиторіїв, регулярне оновлення додатків та тих самих образів, які були використані рані-

ше. Також існує такий інструмент, як Pod Security Admissio, який включає в собі політики безпеки для подів(мікросервісів), різні рівні логування тощо.

Рішення друге: відстежування мережевого трафіку. Треба спостерігати усі підключення на наявність «зайвих», а саме таких, які не підходять до політиці безпеки налаштованої системи оркестрації Kubernetes.

Конфіденційність та безпека даних системи оркестрації Kubernetes має бути вищим пріоритетом в її конфігурації. Тому що правильно налаштована система є гарантією безпеки як застосунку, який є впровадженим в цю систему, так і усіх сервісів, пов'язаних з ним, наприклад, база даних чи бекенд.

Список використаних джерел:

1. Kubernetes security best practices. URL: https://www.redhat.com/en/topics/containers/kubernetes-security-best-practices
2. Production-Grade Container Orchestration - https://kubernetes.io/
3. Kubernetes Security Best Practices: 10 Steps to Securing - https://www.aquasec.com/cloud-native-academy/kubernetes-in-production/kubernetes-security-best-practices-10-steps-to-securing-k8s/
4. What is IAM? URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

Ключові слова: ризики, кібербезпека, K8S, Kubernetes, кластери.
Keywords: risks, cybersecurity, K8S, Kubernetes, clusters.

Науковий керівник: к.т.н., доцент Бойко В.Д.

ШЛЯХИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ

Кіфа Константин

студент 3-го курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Задача захисту інформації комп'ютерних систем актуальна на сьогодні у зв'язку з широким розповсюдженням таких систем та розширенням комп'ютерних мереж, які передають великі обсяги інформації.

Забезпечення безпечної роботи комп'ютерних систем необхідне всім підприємствам і установам, від державних організацій до малих приватних компаній, незалежно від сфери їх діяльності. Різниця лише в засобах, методах та обсягах забезпечення безпеки. [1]

В умовах сьогодення потрібна реалізація системного підходу для забезпечення захисту інформації, що як правило включає комплекс взаємопов'язаних заходів (технічні і програмні, організаційні, нормативно – правові

акти, морально – етичні). заходи протидії тощо). Впровадження технології захисту інформації вимагає все більших витрат і зусиль в комп'ютерних інформаційних системах і мережах передачі даних. Все це, однак, дозволяє уникнути великих втрат і збитків під час реального впровадження ІБ та ІТ-загроз.

До основних загроз інформаційній безпеці та нормальному функціонуванню системи відносяться витік персональних даних, компрометація інформації, несанкціоноване та некоректне використання інформаційних ресурсів, переривання обслуговування та незаконне використання інформації тощо.

Витік конфіденційної інформації - це неконтрольований вихід конфіденційної інформації за межі ІБ або осіб, яким вона була доручена або стала відома в процесі роботи.

Розголошення власником або володільцем інформації - це умисне або необережне дію посадових осіб або користувачів (яким в порядку виконання службових обов'язків або роботи довірено відповідну інформацію), внаслідок чого особи, які не знають її, можуть отримати доступ до неї.

Несанкціонований доступ — це незаконне, навмисне володіння конфіденційною інформацією особою, яка не має прав доступу до інформації, що захищається.

Як правило, інформаційна компрометація (різновид інформаційного зараження) здійснюється шляхом несанкціонованих змін бази даних, в результаті чого споживач змушений або залишити її, або докласти додаткових зусиль для виявлення змін, або відновити реальну інформацію. Використовуючи скомпрометовану інформацію, споживач наражається на ризик прийняття неправильних рішень.

Зловживання санкціонованими джерелами інформації також може призвести до знищення, витоку або компрометації зазначених ресурсів.

Злам інформаційних служб – це загроза, яка походить із самих ІТ. Затримка надання інформаційних ресурсів абоненту може мати для нього серйозні наслідки. Відсутність актуальних даних, необхідних для прийняття рішень, призводить користувача до нераціональної поведінки. [2]

Отже, способи забезпечення безпеки комп’ютерних систем включають: ідентифікацію користувачів, персоналу та ресурсів системи; перевірка облікових даних; дозвіл і створення умов праці в межах установленого регламенту; реєстрація (логування) запитів на ресурси; реагування у разі несанкціонованої дії (тривога, відключення, затримка роботи, відхилення запиту тощо).

Регулювання — це створення умов для автоматизованої обробки, передачі та зберігання інформації, найбільшою мірою яких виконуються норми і стандарти цього захисту.

Примус – це метод захисту, при якому користувачі та IT-персонал дотримуються правил обробки, передачі та використання інформації, що загрожує фінансовою, адміністративною чи кримінальною відповідальністю.

Апаратні пристрої — це пристрої, вбудовані безпосередньо в обчислювальне обладнання, або ті, які обмінюються даними з ним через стандартний інтерфейс.

До фізичних засобів належать різноманітні технічні пристрої та споруди, які перешкоджають фізичному проникненню зловмисників на об'єкти охорони та захищають персонал (засоби індивідуальної безпеки), матеріальні цінності та фінанси, а також інформацію від протиправних дій.

Програмні засоби — це спеціальні програми та програмні комплекси, які використовуються для захисту інформації, що міститься в інформаційній системі. Багато з них інтегровані з самим програмним забезпеченням IS.

Організаційні засоби здійснюють своїм комплексам регламентацію виробничої діяльності в ІС та взаємовідносини виконавців на нормативно – правовій основі таким чином, що розголошення, витік і несанкціонований доступ до конфіденційної інформації стає неможливим або істотно ускладняється за рахунок проведення організаційних заходів. Комплекс цих заходів реалізується групою захисту інформації, але повинен бути під контролем першого керівника. [3]

Правові способи захисту визначаються законодавством даної країни, яке регламентує правила використання, обробки та передачі інформації з обмеженим доступом, а також визначає заходи відповідальності у разі порушення правил.

System Criteria (TCSC) — це стандарт інформаційної безпеки, розроблений Міністерством оборони Сполучених Штатів у 1983 році для визначення вимог безпеки до апаратного забезпечення, програмного забезпечення та спеціальної підтримки комп'ютерних систем, а також для розробки відповідної методології реалізації політики безпеки у військових для аналізів. комп'ютерні системи. Інша назва «Жовтогаряча книга». Критерії пропонують три категорії вимог безпеки - політика безпеки, аудит і коректність, в рамках яких сформульовано шість основних вимог безпеки: політика безпеки, мітки - в межах політики безпеки; ідентифікація та автентифікація, реєстрація та облік - у складі аудиту; перевірка правильності роботи захисних пристроїв, безперебійності захисту — в межах правильності.

[Information Technology Security Evaluation Criteria (ITSEC)] — стандарт інформаційної безпеки, розроблений у 1991 році в європейських країнах (Франція, Німеччина, Нідерланди та Велика Британія). «Європейські критерії» розглядають такі завдання засобів захисту інформації: захист інформації від несанкціонованого доступу для забезпечення конфіденційності; за-

безпечення цілісності інформації шляхом її захисту від несанкціонованої зміни або знищення; забезпечення працездатності систем шляхом боротьби із загрозами відмови в обслуговуванні.

Тому для вирішення проблеми визнання засобів захисту ефективними необхідно забезпечити гарантії, які включають два аспекти: ефективність, яка відображає відповідність засобів захисту вирішуваним завданням, і коректність, яка характеризує процес щодо їх розвитку і функціонування.

Висновок: комплексна оцінка рівня безпеки системи складається з функціональної міцності засобів захисту та гарантій їх виконання.

Список використаних джерел:

1. Гапак О. М. Підручник з курсу «Захист інформації в комп'ютерних системах». ДВНЗ «УжНУ» : Ужгород, 2021, 184 с.
2. А. С. Довбиш, В. К. Ободяк, І. В. Шелехов та ін. Сучасні інформаційні технології в кібербезпеці : монографія /; за ред. В. К. Ободяка, І. В. Шелехова. Суми : Сумський державний університет, 2021. 348 с.
3. О.Г. Корченко. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека", Ніжин : ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. 408 с.
4. Захист комп'ютера від вірусів. Мicрософт : веб-сайт. URL : https://support.microsoft.com/uk-ua/windows/захист-комп-ютера-від-вірусів-b2025ed1-02d5-1e87-ba5f-71999008e026 (Дата звернення 17.11.2022)

Ключові слова: безпека, кібербезпека, System Criteria (TCSC), Information Technology Security Evaluation Criteria (ITSEC), витік конфіденційної інформації, несанкціонований доступ, інформаційна компрометація, регулювання, примус, апаратні пристрої.
Keywords: security, cyber security, System Criteria (TCSC), Information Technology Security Evaluation Criteria (ITSEC), leak of confidential information, unauthorized access, information compromise, regulation, enforcement, hardware devices.

Науковий керівник: к.ф.-м.н., доцент Чепурна О.Є.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Вінник Мирослава

студентка 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасне суспільство є головним генератором і повноцінним споживачем інформаційного середовища. Виходячи з цього, можна впевнено стверджувати, що з розвитком цього явища формуються внутрішні безперервні зв'язки

та залежності між користувачами глобального або індивідуального інформаційного простору.

В період розвитку людства та починаючи з того часу, коли невеликі групи людей почали формувати племена, поселення, міста, імперії, а в наші дні з'явилися людино-машинні інфраструктури, почали існувати набори інформації, які з тих чи інших причин не можуть бути оприлюднені - простіше кажучи, всередині системи обміну інформацією з'явилися секрети.

З часів єгипетських фараонів людство намагалося замаскувати та краще приховати секрети чи таємну інформацію від ворогів. У цей період закладається основа процесу побудови комплексу технічних засобів і методів досягнення необхідного і достатнього рівня безпеки інформаційних мереж. Чим швидше розвивалося суспільство, тим досконалішими ставали методи контрольованого спотворення – шифрування – інформації. До 19 століття все шифрування було «ручним», тобто виконувалося повністю руками людини. З появою складних обчислювальних механізмів і обертових машин частина цього завдання лягла на механізми. Але коли в життя людства увірвалися потужні ЕОМ - комп'ютери, роль людини в цьому процесі була зведена до мінімуму і полягала в розробці нового покоління алгоритмів шифрування, які б дозволяли таким чином перетворювати інформацію. , використовуючи потужність обчислювальної техніки, щоб ворог не міг зламати шифрування. Складність методів і алгоритмів шифрування зростає прямо пропорційно швидкому розвитку самих комп'ютерів. На сьогоднішній день розроблено низку алгоритмів шифрування, які з урахуванням сучасних можливостей комп'ютерної техніки здатні зберігати цілісність і конфіденційність інформації. Найбільш популярними алгоритмами в сучасному інформаційному середовищі є симетричні алгоритми - DES, 3DES, AES, - і асиметричні алгоритми, такі як група RSA шифрування зі змінною довжиною ключа. [1]

Організація системи обробки даних та інформаційних технологій базується на загальних принципах визначення та вибору комплексної конфігурації технічних пристроїв, що забезпечують ефективне інформаційне обслуговування всіх рівнів та об'єктів управління, а також з урахуванням специфіки обробки даних. Функції та процедури управління в інформаційній системі, склад і кількість використовуваних технічних засобів визначаються обсягом і інтенсивністю інформаційного потоку, технологією реалізації функцій управління та їх часовими характеристиками. Зростаючі вимоги до економічної інформації та вдосконалення управління зумовлюють необхідність використання більш продуктивних і передових інструментів і технологій. [2]

Основою всіх КТС є комп'ютер. За розміром і функціональним призначенням комп'ютери можна поділити на: суперкомп'ютери, великі комп'ютери,

малі комп'ютери (мінікомп'ютери), мікрокомп'ютери (персональні комп'ютери), сервери, робочі станції.

Шифрування — це оборотне перетворення даних, яке має на меті приховати інформацію. Шифрування здійснюється за допомогою криптографічного ключа. Ключ — це певна кількість символів, які вільно утворюються із символів, доступних у системі шифрування. [3]

Концепція захисту даних за допомогою шифрування дуже важлива і актуальна сьогодні. Криптографія була розроблена для задоволення потреб аналізу загроз інформаційній безпеці та дозволяє ідентифікувати компоненти сучасних комп'ютерних загроз – їх джерела та драйвери, способи реалізації та наслідки. Аналіз надзвичайно важливий для отримання всієї необхідної інформації про інформаційні загрози, визначення розміру можливої матеріальної та нематеріальної шкоди та розробки відповідних заходів протидії. Однією з найпоширеніших загроз кібербезпеці є витік даних (близько 80% кіберінцидентів). [1]

Зазвичай існує два методи шифрування: симетричний і асиметричний [3]:

У симетричному шифруванні секретний ключ використовується як для шифрування, так і для дешифрування. Симетричні алгоритми шифрування можна розділити на потокові та блокові. Алгоритми потокового шифрування обробляють текстові повідомлення поетапно. Блокові алгоритми працюють з блоками фіксованого розміру. найчастіше розмір блоку становить 64 біта.

Асиметричне шифрування або метод відкритого ключа передбачає використання двох різних ключів у парах, а саме секретного ключа та відкритого ключа. Як випливає з назви, відкритий ключ безперешкодно розміщується в мережі, логічно закритий ключ завжди зберігається в секреті. При асиметричному шифруванні ключі працюють разом у парах, тобто коли інформація зашифрована відкритим ключем, її можна розшифрувати лише за допомогою відповідного закритого ключа, і навпаки. Неможливо використовувати відкритий ключ з однієї пари та закритий ключ з іншої пари. Усі асиметричні пари ключів пов'язані між собою математичними залежностями.

За словами експертів, останнім часом спостерігається все більше фішингових атак. Це широко поширена загроза кібербезпеці, яка створює величезні ризики для окремих осіб і організацій.

Фішингова атака – це техніка, яка використовується зловмисниками для викрадення конфіденційної інформації шляхом обману, змушуючи користувачів передати її. Більшість користувачів навіть не підозрюють про цю загрозу. Фішинг як той чи інший вид шахрайства використовується роками. Почалося з телефонних дзвінків. Але сьогодні кіберзлочинці вважають фішин-

гові атаки успішним і простим способом підготовки до більш складних кібератак.

Людина часто є першою слабкою ланкою в кібератаці. Після проведення розвідки та вивчення цілі виконавець такої атаки використовує отриману інформацію для входу в обліковий запис або іншу важливу інформацію, яка веде до захищених систем і ресурсів. Найчастіше зловмиснику щастить, і він може дізнатися облікові дані користувача з мінімальними зусиллями та ще меншим ризиком, просто здогадуючись, що можна зробити навіть в автоматичному режимі. Тему соціальної інженерії важко обговорювати, оскільки багато користувачів надмірно впевнені в захисті своїх облікових даних і не дотримуються належної «кібергігієни». [1]

Якщо говорити про технічне забезпечення інформаційної безпеки комп'ютерних мереж, то можна сміливо сказати, що такий процес був би неможливий без розробки навчальних систем криптографії та захисту інформації. У той же час існуючі системи безпеки розробляються безпосередньо тими, хто найбільш вразливий до кібератак.

Підсумовуючи, можна сказати, що технічне забезпечення інформаційної безпеки повинно мати цілісну структуру, яка включає як побудову стресостійких систем, так і відповідне навчання персоналу, який обслуговує ці системи.

Список використаних джерел

1. Виходець Ю. О. Технічне забезпечення безпеки функціонування комп'ютерних та інформаційних систем. Кібербезпека в сучасному світі : матеріали III Всеукраїнської науковопрактичної конференції (м. Одеса, 19 листопада 2021 р.) : Одеса, 2020 С. 4.
2. Конспект лекцій з дисципліни «Корпоративні інформаційні системи». 122 с. URL: https://learn.ztu.edu.ua/pluginfile.php/36808/mod_resource/content (Дата звернення 17.11.2022)
3. Види шифрування інформації. UA5.ORG. Методичні матеріали з інформатики : веб-сайт. URL : https://ua5.org/protect/395-vidi-shifruvannya-informaciyi.html (Дата звернення 17.11.2022)

Ключові слова: інформаційне середовище, інформаційні технології, шифрування, інформаційні та системи, безпека, фішингова атака, кібербезпека.
Keywords: nformation environment, information technologies, encryption, information and systems, security, phishing attack, cyber security.

Науковий керівник: к.ф.-м.наук, доцент Чепурна О.Є.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІННОВАЦІЙНИХ ПРОЕКТІВ В УМОВАХ СЬОГОДЕННЯ

Громов Ігор

студент 2-го курсу магістратури факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Протягом останніх десятиліть стає очевидним, що конкурентоспроможність і потенціал розвитку підприємств, успішність позиціонування продукції на внутрішньому та зовнішньому ринках значною мірою залежать від інновацій технологій, що застосовуються, матеріалів, готової продукції, сировини тощо.

Враховуючи ризикованість і високу вартість інноваційних проектів, постійно зростають потреби інвесторів та організаторів щодо реалізації інноваційних проектів в інформаційному забезпеченні процесу бізнес-планування інноваційних проектів.

Проблема полягає в тому, що описова, погано формалізована інформація щодо ключових параметрів бізнес-планування інноваційних проектів може бути трансформована в дані, придатні для автоматизованої обробки та прийняття сучасних та необхідних управлінських рішень. [1]

Проект є окремою, новоствореною системою, яка є унікальною за змістом і результатами діяльності, обмежена чітко визначеним часом від початку до кінця проекту, а зміни в середовищі викликають високий ступінь невизначеності. . середовище, небезпеки, небезпеки та ризики. Проект — це зобов'язання зі створення цінності, засноване на місії проекту, яке має бути виконано протягом визначеного часу, ресурсів і умов роботи. Проект має такі основні характеристики: унікальність проекту та його місії, часовий орієнтир, визначений датами початку та завершення, а також невизначеність, така як зміни в середовищі проекту та ризики [2].

У сучасних умовах джерела інформації є стратегічним ресурсом країни. Вони складають основу інформаційної системи, призначеної для розвитку інноваційної системи.

На кожному підприємстві, де створюються інноваційні проекти, забезпечується інноваційна діяльність, створюються інформаційні джерела, які спрямовані на встановлення та організацію інформаційних зв'язків між усіма учасниками інноваційної сфери на кожному етапі інноваційного процесу, створення інноваційної продукції, а це забезпечує зв'язок між попитом і пропозицією вітчизняної інноваційної продукції.

Розвиток інформаційної інфраструктури як елемента національної інноваційної системи впроваджує та створює нові інформаційно-комунікаційні

технології, мережи, формує нове інформаційне суспільство, будує розвиток інститутів системи науково-технічної інформації.

Аналіз інформаційного забезпечення інноваційної діяльності та управління проектами формує інформаційне суспільство та орієнтує його на використання сучасних інформаційно-комунікаційних технологій.

Інформаційні системи розвинених країн спрямовані на впровадження як новітніх технологій, так і нових форм організації діяльності в різних сферах економіки, метою яких є розвиток інноваційної діяльності.

Особливо в США, Японії та Канаді впроваджуються нові інформаційно-комунікаційні технології та децентралізоване управління інформаційною сферою. Велика Британія підтримує розвиток спеціальних установ, бібліотек, інформаційних організацій та інформаційних центрів з метою сприяння діяльності інноваційних структур. [3]

У 2021 році, із усіх кібератак у світі 19% були спрямовані проти України, згідно зі звітом Microsoft. Україна в рейтингу спрямованих кібератак посідає друге місце після США. Крім того, протягом минулого року оперативним центром реагування на кіберінциденти Державного центру кіберзахисту (ДЦКЗ) було зафіксовано 41 млн. підозрілих подій щодо інформаційної безпеки, було виявлено 160 тис. критичних подій та зареєстровано 147 кіберінцидентів. Більшість із яких пов'язані зі шкідливим програмним кодом (28%), збиранням інформації зловмисниками (18%) і шахрайством (6%). Зазвичай напади йшли з території російської федерації. Як зазначається у звітах з початком війни та напередодні російського вторгнення кількість атак зросла в рази.

З початку повномасштабного вторгнення росія здійснила 796 кібератак на Україну. Про це повідомляє Державна служба спеціального зв'язку та захисту інформації України. Порівняно з відповідним періодом минулого року їх кількість зросла втричі. Тому захистити свій інноваційний проект від таких ситуацій і ризиків вкрай необхідно.

Інформаційні технології відіграють важливу роль у багатьох аспектах ведення воєнних дій : координація військових дій, зв'язок між командуванням та з частинами, матеріально-технічне забезпечення військових, передача даних від лінії фронту до штабу, від фронту до командування, різного роду покриття, передньої позиції тощо. Використання зловмисної кіберактивності є частиною російської стратегії. Тому російські хакери посилили свою активність і систематично атакують українські банки та фінансові компанії, державні установи та приватні підприємства, які є частиною критичної інфраструктури, зокрема енергетичні, логістичні, телекомунікаційні та медіакомпанії. [4]

У цій ситуації можна проаналізувати власну систему безпеки, виявити слабкі місця та усунути їх; впровадження хоча б одного базового набору за-

собів захисту – йдеться про мережевий екран, антивірус, системи захисту WEB та MAIL, і паралельно – сприяння розвитку комп'ютерної грамотності, навчання основним правилам «цифрової гігієни»; оцінити всі ризики та побудувати систему СУІБ, контролювати та захистити працівників, створити нормативну базу та запровадити інформаційну безпеку процесів компанії.

Висновки: захист автоматизованих систем незалежно від його технічного рівня, інформаційного забезпечення інноваційних проектів потребує безпеки цих систем, яка значною мірою залежить від якісного та системного виконання усіх заходів, спрямованих на уникнення можливих ризиків пошкодження інформаційних систем, загрози хакерських атак на підприємстві; регулярні оновлення безпеки; відмова від використання застарілого програмного забезпечення; виконання перевірок уразливостей білих/сірих/чорних скриньок систем і додатків і виявлення слабких місць у захисті за допомогою кваліфікованих аудитів; повторна перевірка наявності вразливостей системи, можливості їх використання та переоцінка ризиків.

Список використаних джерел:

1. Богів Я.С., Мирощенко Н.Ю., Паук О.Є. Інформаційне забезпечення бізнес-планування інноваційних проектів підприємств : складові елементи та особливості їхньої взаємодії. Маркетинг і менеджмент інновацій, 2012, №4. С. 193-202.
2. Алькема В.Г., Літвін Н.М., Кириченко О.С. Економічна безпека інноваційного підприємства: навч. посібн. Київ : ВНЗ «Університет економіки та права «КРОК», 2015. 320 с.
3. Писаренко Т.В. Інформаційне забезпечення інноваційного розвитку : світовий та вітчизняний досвід : монографія, Київ : УкрІНТЕЇ, 2015. 239 с.
4. Як українському бізнесу захиститися від атак російських хакерів під час війни: поради IT-фахівців. URL : https://speka.media/kiberbezpeka-yak-ukrayinskomu-biznesu-zaxistitisya-vid-atak-rosiiskix-xakeriv-pid-cas-viini-poradi-vid-it-faxivciv-93766v (Дата звернення 17.11.2022)

Ключові слова: проект, інноваційний проект, інформаційні технології, цифрова гігієна, кібербезпека, організація безпеки інформаційних систем при веденні інноваційного проекту.
Keywords: project, innovation project, information technologies, digital hygiene, cyber security, organization of security of information systems during the implementation of an innovation project.

Науковий керівник: к.ф.-м.н., доцент Чепурна О.Є.

БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

Чеховський Андрій

студент 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

За умов повсюдної "інтернетизація" інфраструктур стрімко розвиваються публічні онлайн-сектори, де населення свідомо залишає свою персональну інформацію в рамках свого онлайн банкінгу і шопінгу, споживання онлайн-послуг (інформаційних, медичних, навчальних тощо), користування електронною поштою та хмарними сервісами тощо. Це відбувається через заповнення анкет, реєстрацію та автентифікацію, дописи та публікації у месенджерах та соціальних мережах тощо.

Зі зростанням обсягів інтернет-залежних сервісів та збільшенням кількості персональних даних, яку користувачі надають у мережі, збільшується ймовірність кіберзагроз та порушень конфіденційності [1]. Для забезпечення захисту від витоків персональних даних є різні методи, зокрема: двофакторна система автентифікації, антивіруси, біометрія, шифрування. Ці методи мають різні спектри дії і ступені безпеки, більшість з яких встановлюють обмеження на доступ до інформації, тим самим забезпечують їхню конфіденційність [2].

Двофакторна автентифікація (2FA) як метод захисту від несанкціонованого доступу використовує два різних елементи для підтвердження ідентифікації користувача. Для входу в систему користувач має ввести свій пароль, а також використати додатковий фактор у формі одноразового коду, який направляється на його мобільний пристрій. Цей метод забезпечує гарний рівень безпеки, оскільки навіть у разі витоку пароля, зловмисники не матимуть доступу без додаткового елемента ідентифікації. Такий підхід не лише ускладнює завдання потенційним зловмисникам, а й підвищує загальний рівень захисту конфіденційної інформації користувача.

Антивірусні системи є поширеним методом захисту від потенційних кіберзагроз, що можуть завдати шкоди пристрою та/або викрасти конфіденційну інформацію. Антивірусні програми працюють на основі різних алгоритмів та методів, які дозволяють виявляти та нейтралізувати шкідливі програми, забезпечуючи надійний захист для користувачів. Антивірусні бази такого програмного забезпечення постійно оновлюються, щоб виявляти найновіші загрози та ефективно боротися з ними. Розрізняють різні типи антивірусних програм: фільтри, вакцини, детектори, доктори, ревізори тощо [3]. Вибираючи антивірусне рішення для свого комп’ютера, потрібно багато чого враховувати. Більшість антивірусів мають подібні механізми захисту, включаючи

порівняння файлів із сигнатурами зловмисного програмного забезпечення, аналіз поведінки додатків і аналіз зразків зловмисного програмного забезпечення нульового дня, щоб кожен міг скористатися перевагами ефективнішого захисту [4].

Системи біометричного захисту використовують унікальні для кожної людини вимірювані фізіологічні характеристики для ідентифікації та автентифікації особи. Цей процес називається електронною автентифікацією. Біометрична автентифікація порівнює дані про характеристики людини з біометричним «шаблоном» цієї особи, який зберігається в базі даних, щоб визначити схожість. Мета ідентифікації полягає у перевірці того, чи відомий індивід системі, наприклад, за допомогою перевірки пароля, а авторизація полягає у наданні користувачеві доступу до певних ресурсів, залежно від його особи. Суттєвим недоліком цього способу захисту інформації є необхідність надання біометричній системі унікальних характеристик конкретної людини [5]. Здебільшого для біометричної автентифікації використовують: відбиток пальця, запис голосу, сканування райдужки або сітківки ока, розпізнавання обличчя.

Шифрування є надійним методом захисту конфіденційної інформації від несанкціонованого доступу. Використання шифрування гарантує, що навіть у випадку неправомірного доступу до інформації, зловмисникам буде надто складно або навіть неможливо зрозуміти чи використати дані без відповідного розшифрування. Шифрування створює бар'єр, який забезпечує безпеку конфіденційної інформації, запобігаючи її несанкціонованому використанню чи розголошенню. Це ефективний захисний механізм, який допомагає зменшити ризик втрати чи крадіжки цінних даних.

Сучасне програмне забезпечення на базі штучного інтелекту (ШІ) використовує багаторівневі технології, які допомагають запобігти зараженню зловмисним кодом. Наразі сфера безпеки в Інтернеті – це та сфера, яка потенційно може принести найбільшу користь від рішень ШІ, що зумовлює його впровадження [5].

Забезпечення безпеки персональної інформації є надзвичайно важливим завданням, яке потребує постійного вдосконалення та дотримання вимог законодавства. У сучасному цифровому світі зловмисники постійно шукають нові способи атаки та порушення конфіденційності даних. Тому важливо бути завжди на сторожі та забезпечувати безпеку конфіденційної інформації в інформаційному середовищі. Регулярні оновлення захисних програм, моніторинг та вдосконалення систем безпеки є обов'язковими завданнями для запобігання порушенням та втрати доступу до особистих даних. Ретельне виконання цих завдань є ключем до збереження приватності та надійності інформації в цифровому середовищі.

Список використаних джерел:

1. Задерейко О.В., Трофименко О.Г., Логінова Н.І. Захист персональних даних в ОС Windows 10. Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаціиних системах. VII міжнар. наук.-практ. конф. (8-10 листопада 2018 р.). Чернівці: ЧНУ ім. Юрія Федьковича. С. 304–307.
2. Zadereyko O., Trofymenko O., Loginova N. Algorithm of user's personal data protection against data leaks in Windows 10 OS. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. Lublin University of Technology. 2019. Vol. 9. No 1, pp. 41-44. DOI: 10.5604/01.3001.0013.0905.
3. Основи комп'ютерної техніки: навч.-метод. посібник / О. Г. Трофименко, О. В. Задерейко, Н.І. Логінова. Одеса: Фенікс, 2017. 148 с.
4. МакФарланд А. 10 «Найкращих» антивірусних програм для ПК. URL: https://www.unite.ai/uk/антивірус-пк/
5. Біометричний захист інформації. URL: https://vuzlit.com/963619/biometrichniy_zahist_informatsiyi/

Ключові слова: безпека інформації, конфіденційність, методи захисту інформації.
Keywords: information security, confidentiality, information protection methods.

Науковий керівник: доцент Трофименко О.Г.

THE STRESS-ENERGY TENSOR AND LCK-MANIFOLDS RESPECT TO CONFORMAL MAPPINGS

Patrik Peška

Doctor of Philosophy in Physical and Mathematical Sciences
Department of Algebra and Geometry
Faculty of Science of the Palacky University (Czechia)

Olena Chepurna

Doctor of Philosophy in Physical and Mathematical Sciences
Associate Professor of the Department of Department of Cybersecurity
Faculty of Cybersecurity and Information Technology

It is well known that the gravitation fields in a space (V_n, g) are described by the Einstein equations:

$$R_{ij} - \frac{Rg_{ij}}{2} = -\frac{8\pi k}{c^4} T_{ij}. \qquad (1)$$

The left-hand side contains such geometric objects of the space (V_n, g) as $R_{ij} = R^{\alpha}{}_{ij\alpha}$, reffered to as Ricci tenzor $R = R_{ij} g^{ij}$, pseudo-Riemannian metric g_{ij}, and the scalar curvature $R = R_{ij} g^{ij}$. The symbol T_{ij} denotes the stress-energy tensor. It is

covariant of order 2. Finely, c is the speed of light in vacuum and k is the gravitational constant.

We explore transformations of stress-energy tensor T_{ij} if a space is subjected by a conformal mapping $(V_n, g) \to (\overline{V}_n, \overline{g})$, i.e. their metrics satisfy the equation [4]

$$\overline{g}_{ij} = e^{2\varphi} g_{ij}, \tag{2}$$

Where $\varphi = \varphi(x^1, ..., x^n)$ is some scalar function. We consider the case when (V_n, g) is Hermitian and $(\overline{V}_n, \overline{g})$ is a locally conformally Kählerian one.

Let us recall some basic conceptions([1], [2], [4]). Obviously, spaces (V_n, g) and $(\overline{V}_n, \overline{g})$ are even-dimensional: $n = 2m$. Also, they carry an almost complex structure J.

Definition 1 The almost complex structure J *is called an affinor* J^i_j *that:*

$$J^i_\alpha J^\alpha_j = -\delta^i_j. \tag{3}$$

Here δ^i_j is the Kronecker delta.

Definition 2 *A space with an almost complex structure* J *is reffered to as an almost complex space.*

An almost complex space is denoted as $\{V_n, J, g\}$.

Definition 3 *An almost complex space* $\{V_n, J, g\}$ *is A Hermitian one if:*

1) The metric is Hermitian:

$$J^\alpha_i J^\beta_j g_{\alpha\beta} = g_{ij}; \tag{4}$$

2) The almost complex structure is integrable.

$$J^k_{i,j} = J^\alpha_i J^\beta_j J^k_{\alpha,\beta}; \tag{5}$$

We denote covariant derivative respect to the Rimanian metric g_{ij} by comma.

If in a Hermitian space $\{V_n, J, g\}$ the condition виконується умова:

$$J^k_{i,j} = 0, \tag{6}$$

holds, then it is reffered to as a Kählerian one.

Definition 4 A Hermitian space $\{V_n, J, g\}$, is called a locally conformal Kähler manifold (LCK- manifold) if there is an open cover $\mathsf{U} = \{U_\alpha\}_{\alpha \in A}$ of the manifold M and a family of such functions $\Sigma = \{\sigma_\alpha : U_\alpha \to \mathsf{R}\}_{\alpha \in A}$ that $\{J|_{U_\alpha}, \hat{g}_\alpha = e^{-2\varphi_\alpha} g|_{U_\alpha}\}$ is a Kählerian structure for any $\alpha \in A$. Transition from a metric $g|_{U_\alpha}$ to a metric $e^{-2\varphi_\alpha} g|_{U_\alpha}$ is reffered to as local transformation of the structure.

It means that (6) for $\{V_n, J, g\}$ does not hold, but locally for $\{\overline{V}_n, J, \overline{g} = e^{2\varphi} g\}$

$$J^k_{i|j} = 0 \tag{7}$$

is satisfied.

By the symbol “|” we denote covariant derivative respect to the Levi-Civita connection of the space $\{\overline{V}_n, J, \overline{g} = e^{2\varphi} g\}$.

These covariant derivatives wich respected to the different metrics satisfy the identity:

$$J^k_{i|j} = J^k_{i,j} + J^\alpha_i P^k_{\alpha j} - J^k_\alpha P^\alpha_{ij}, \tag{8}$$

where

$$P^k_{ij} = \delta^k_j \varphi_i + \delta^k_i \varphi_j - \varphi^k g_{ij} \tag{9}$$

is called a deformation tensor of the connections. Here we denote $\varphi_i = \partial_i \varphi$ and $\varphi^k = \varphi_i g^{ik}$. Substituting from (9) in (8) and taking into account (7), we get:

$$J^k_{i,j} + J^\alpha_i (\delta^k_j \varphi_\alpha + \delta^k_\alpha \varphi_j - \varphi^k g_{\alpha j}) - J^k_\alpha (\delta^\alpha_j \varphi_i + \delta^\alpha_i \varphi_j - \varphi^\alpha g_{ij}) = 0. \tag{10}$$

Simplifying (10) we get:

$$J^k_{i,j} = -\delta^k_j J^\alpha_i \varphi_\alpha + \varphi^k J_{ij} + J^k_j \varphi_i - J^k_\alpha \varphi^\alpha g_{ij}. \tag{11}$$

Contracting (11) for the indeces j and k:

$$J^{\alpha}_{i,\alpha} = -nJ^{\alpha}_{i}\varphi_{\alpha} + J_{i\alpha}\varphi^{\alpha} + J^{\alpha}_{\alpha}\varphi_{i} - J_{\alpha i}\varphi^{\alpha} = -nJ^{\alpha}_{i}\varphi_{\alpha} + J_{i\alpha}\varphi^{\alpha} + J_{i\alpha}\varphi^{\alpha} = -(n-2)J^{\alpha}_{i}\varphi_{\alpha}. \tag{12}$$

Note: in (12) we take accont of $J^{\alpha}_{\alpha} = 0$ and $J^{\alpha}_{i}g_{\alpha j} = J_{ij} = -J_{ji}$. Finally, from (12), because of (3), we get[3]:

$$\varphi_{i} = \frac{1}{n-2}J^{\alpha}_{\beta,\alpha}J^{\beta}_{i}. \tag{13}$$

The equation (13) give us coefficients of the differential form

$$\omega = \varphi_{i}dx^{i}; \tag{14}$$

which is reffered to as Lee form of the space $\{V_n, J, g\}$.

Then we get a system of PDE of the first order:

$$\frac{\partial\varphi}{\partial x^{i}} = \frac{1}{n-2}J^{\alpha}_{\beta,\alpha}J^{\beta}_{i}, \quad i = \overline{1,n}. \tag{15}$$

The system (15) has a solution if the conditions $\frac{\partial^2\varphi}{\partial x^{j}\partial x^{i}} = \frac{\partial^2\varphi}{\partial x^{i}\partial x^{j}}$ are satisfyed, or in terms of covariant derivatives:

$$\varphi_{i,j} = \varphi_{j,i}; \quad k,l = \overline{1,n}. \tag{16}$$

The requirement (16) is equivalent to the condition: the Lee form have to be closed one, i.e.: $d\omega = 0$. Differentiate (13) covariantly:

$$\varphi_{i,j} = \frac{1}{n-2}(J^{\alpha}_{\beta,\alpha j}J^{\beta}_{i} + J^{\alpha}_{\beta,\alpha}J^{\beta}_{i,j}). \tag{17}$$

Alternating (17) respect to indeces i and j, taking account of (16), we get:

$$\frac{1}{n-2}(J^{\alpha}_{\beta,\alpha j}J^{\beta}_{i} + J^{\alpha}_{\beta,\alpha}J^{\beta}_{i,j} - J^{\alpha}_{\beta,\alpha i}J^{\beta}_{j} - J^{\alpha}_{\beta,\alpha}J^{\beta}_{j,i}) = 0,$$

or:

$$J^{\alpha}_{\beta,\alpha j}J^{\beta}_{i} + J^{\alpha}_{\beta,\alpha}J^{\beta}_{i,j} - J^{\alpha}_{\beta,\alpha i}J^{\beta}_{j} - J^{\alpha}_{\beta,\alpha}J^{\beta}_{j,i} = 0. \tag{18}$$

Since the conditions of integrability (18) are independ of the function $\varphi = \varphi(x^1,...,x^n)$ and its derivatives, if an almost complex structure J satisfies (18), The system (15) is completely integrable. According to the differential eauation theory, (15) has the solution depending on single arbitrary parameter. The solution might be found by the formula [3]:

$$\varphi(x^1,...,x^n)=\sum_{i=1}^{n}\int_{x_0^i}^{x^i}\varphi_i(x_0^1,...,x_0^{i-1},x^i,...,x^n)dx^i+C,$$

or, sinse the arbitrary parameter C have a sense of initial value, finally we get:

$$\varphi(x^1,...,x^n)=\frac{1}{n-2}\sum_{i=1}^{n}\int_{x_0^i}^{x^i}J^{\alpha}_{\beta,\alpha}J^{\beta}_{i}(x_0^1,...,x_0^{i-1},x^i,...,x^n)dx^i++\varphi(x_0^1,...,x_0^n). \tag{19}$$

Hence, we have a theorem

Theorem 1 *A Hermitian space* $\{V_n,J,g\}$, $(n>2)$ *is a locally conformally Kählerian one, if and only if the almost complex structure satisfies the condition:*

$$J^{\alpha}_{\beta,\alpha j}J^{\beta}_{i}+J^{\alpha}_{\beta,\alpha}J^{\beta}_{i,j}-J^{\alpha}_{\beta,\alpha i}J^{\beta}_{j}-J^{\alpha}_{\beta,\alpha}J^{\beta}_{j,i}=0.$$

Also we prove the theorem [5].

Теорема 2 *If a Hermitian space* $\{V_n,J,g\}$ *locally mapped onto a Kählerian space* $\{\overline{V}_n,J,\overline{g}=e^{2\varphi}g\}$, $(n>2)$, *then the deformation of the stress-energy tensor depend only on the metric of the space* $\{V_n,J,g\}$ *and the complex structure. If in a Hermitian space* $\{V_n,J,g\}$ *satisfies the condition:*

$$\frac{1}{n-2}J^{\alpha}_{\beta,\alpha}J^{\beta}_{i}J^{\gamma}_{\delta,\gamma}J^{\delta}_{j}+J^{\alpha}_{\beta,\alpha\gamma}J^{\beta\gamma}g_{ij}-J^{\alpha}_{\beta,\alpha j}J^{\beta}_{i}-J^{\alpha}_{\beta,\alpha}J^{\beta}_{i,j}-\frac{n-1}{2(n-2)}J^{\alpha\beta}_{,\alpha}J^{\gamma}_{\beta,\gamma}g_{ij}=0,$$

then stress-energy tensor is is invariant respect to the conformal mapping onto Kählerian space $\{\overline{V}_n,J,\overline{g}=e^{2\varphi}g\}$.

The resuls might be applied for statistical manifolds and informational geometry as whole.

List of References:

1. S. Dragomir, L. Ornea Locally conformal Кдhler geometry// Boston ; Basel ; Berlin, cop. 1998.Series: Progress in mathematics, vol. 155.
2. I. Vaisman A geometric condition for an l.c.K. manifold to be Kähler// Geometriae Dedicata, 10 (1981), 129-134.
3. K. Yano Differential geometry on complex and almost complex spaces// Pure and Applied Math. vol. 49, Pergamon Press Book, New York (1965).
4. Mikeš J. at al. Differential geometry of special mappings. /J. Mikeš -- Olomouc: Palacky University, 2015, 566 p.
5. Cherevko Y. Geometry of special diffeomorphisms of conformal Kähler manifolds. Ph.D. Thesis, Odessa Nat. Econom. Univ., 2019. (supervisor V. Berezovskii)

Keywords: almost Hermitian manifolds, Hermitian metric, conformal mapping, LCK-manifold.

КРИТИЧНА ІНФРАСТРУКТУРА ЯК ОБ'ЄКТ КІБЕРЗАХИСТУ

Саврацький Олександр

аспірант кафедри кібербезпеки Національного університету «Одеська юридична академія»

В сучасних умовах критична інфраструктура є ключовим елементом для стабільності та безпеки будь-якої країни. Під критичною інфраструктурою розуміють «підприємства й установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології, телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки та безпеки держави, суспільства, населення, виведення з ладу або руйнування яких може позначитися на національній безпеці й обороні, природному середовищі, призвести до значних матеріальних і фінансових збитків, людських жертв» [1].

Об'єктами критичної інфраструктури можуть бути як державні, так і приватні установи і серед них обов'язково мають фігурувати: урядування та надання найважливіших адміністративних послуг, енергозабезпечення та водопостачання, продовольче забезпечення, охорона здоров'я, електронні комунікації, транспортні служби, фінансові послуги, сфера оборони та державної безпеки, система правосуддя, цивільний захист населення тощо.

Зростаюча глобалізація та поширення цифрових технологій, роблять критичну інфраструктуру вразливою до кібератак. Власне сам кіберпростір вже апріорі розглядається як середовище для потенційних злочинних дій, як у сфері несанкціонованого доступу до конфіденційної інформації, так і в контексті можливих збоїв у роботі програмного забезпечення, порушення режиму функціонування автоматизованих систем тощо. Одночасно відбувається й поступова зміна напряму загроз: з локального та галузевого на загальнонаціональний та наднаціональний [2, с. 184]. А в умовах повномасштабної війни кібератаки, які здійснювалися досі на критичну інфраструктуру будь-якої іншої країни у світі, за регулярністю, масовістю, глибиною та витонченістю не йдуть у жодне порівняння з кібератаками, які сьогодні відбуваються на об'єкти критичної інфраструктури України [3].

На рівні країни побудова ефективної системи кіберзахисту критичної інфраструктури передбачає розробку та інтеграцію комплексного підходу, який включає технічні, організаційні та правові аспекти і потребує відповідних управлінських рішень.

Насамперед, на об'єктах критичної інфраструктури необхідно впроваджувати передові технології захисту, які включають в себе фаєрволи, антивірусне програмне забезпечення, інструменти для виявлення та реагуван-

ня на інциденти, а також регулярне оновлення та патчінг систем. Окремим напрямом виділяють також мережеву безпеку, яка включає захист мережевого трафіку за допомогою інтрузивних систем виявлення та запобігання інтрузіям (IDS/IPS) та використання віртуальних приватних мереж (VPN) для захисту комунікацій. І, нарешті, захист даних, який включає шифрування чутливих даних в процесі зберігання та під час передачі, також забезпечення регулярних резервних копій та захист від втрати даних.

Серед організаційних заходів на об'єктах критичної інфраструктури провідне місце займає робота з персоналом. Конкретними інструментами при цьому виступають регулярне навчання працівників, проведення тренувань і симуляцій кібератак (пентест), а також розвиток корпоративної культури кібербезпеки. На рівні окремих працівників, особливо тих, хто має доступ до конфіденційної інформації, важливим аспектом є управління свідомістю та звітування про потенційні кіберзагрози та інциденти. Задля ефективного контролю потрібно також проведення регулярних аудитів безпеки для оцінки відповідності стандартам та виявлення слабких місць.

Нормативним підґрунтям кіберзахисту критичної інфраструктури є, зокрема, Закон України «Про критичну інфраструктуру» [4], а також інші закони, постанови кабінету міністрів, а також низка міжнародних договорів, що мають обов'язкову силу для України.

Щодо управлінського аспекту державним органом, який керує національною системою захисту критичної інфраструктури, координує міністерства та операторів інфраструктури, веде реєстр об'єктів критичної інфраструктури та готує оцінку ризиків системи на національному рівні – виступає Держспецзв'язку.

В той самий час в межах окремих об'єктів критичної інфраструктури побудова та інтеграція ефективної системи кіберзахисту ґрунтується на наявних організаційних та технологічних можливостях, фінансових та людських ресурсах, а також нормативно-правового базисі. Відповідальним за технічну складову вказаної системи виступає системний адміністратор, проте управлінські рішення стосовно боротьби з кіберзагрозами вже знаходяться в зоні відповідальності менеджменту [5, с. 137].

Відтак для найбільшої ефективності системи кіберзахисту критичної інфраструктури важливими є технічні, організаційні та нормативно-правові аспекти, а управлінська діяльність у вказаній сфері має спрямовуватися на запобігання ризикам, а не на ліквідацію негативного впливу.

Список використаних джерел:

1. Верголяс О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз. URL: https://

coolyanews.info/reformuvannyasistemi-zahistu-ta-piidvischennyastiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-v-rozriiziiaktual.html
2. Горбаченко С. А. Кібербезпека як складова економічної безпеки України. Галицький економічний вісник. 2020. Том 66. № 5. С. 180-186.
3. Пядишев В. Г. Кібербезпека критичних інфраструктур: закордонний досвід та українські реалії. URL: http://www.sulj.oduvs.od.ua/archive/2022/4/part_3/38.pdf
4. Закон України «Про критичну інфраструктуру». URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
5. Горбаченко С. А. Інтеграція менеджменту кібербезпеки в управлінські процеси вітчизняних суб'єктів підприємництва. Кібербезпека в сучасному світі: актуальні виклики: матеріали III Всеукраїнської науково-практичної конференції (м. Одеса, 25 листопада 2022 р.). 2022. С. 135-139.

Ключові слова: критична інфраструктура, організація, ризики, кіберзахист, менеджмент.
Keywords: critical infrastructure, organization, risks, cyber protection, management.

Науковий керівник: д.е.н., професор Горбаченко С.А.

СТАНДАРТ АВТЕНТИФІКАЦІЇ FIDO2

Даниловська Каріна

студентка 1-го курсу факультету цивільної та господарської юстиції Національного університету «Одеська юридична академія»

Після появи масових персональних комп'ютерів, смартфонів, глобальної мережі Інтернет і величезної кількості різноманітних ресурсів, що здійснюють свою діяльність за їхньою допомогою, виникла проблема з надійною автентифікацією користувачів. Для доступу до ресурсу під час автентифікації від самого початку використовувалася комбінація з імені користувача (логіна) і пароля. Звісно, проблеми зі збереженням у таємниці цих чинників автентифікації були й тоді (чимало користувачів записували свої паролі на папірці та приклеювали їх просто на монітор), але для несанкціонованого доступу до ресурсів здебільшого було необхідно мати фізичний доступ до комп'ютера.

З появою хмарних технологій ситуація різко змінилася в гірший бік, оскільки тепер як логін стали використовувати адреси електронної пошти, а вони не є «секретними». Пароль залишився єдиним секретом (фактором), необхідним для отримання доступу до ресурсу.

Крім того, тоді ж (приблизно 15 років тому) дослідження, що проводяться різними технологічними компаніями, показали, що офісний працівник під час роботи з різними сервісами в Інтернет змушений запам'ятовувати від 20 до 40 паролів [1].

Наслідком цього стала масова практика створення списків паролів і збереження їх в електронному вигляді на комп'ютерах і смартфонах. У разі втрати або крадіжки такого пристрою зловмисники зможуть отримати доступ не до одного, а до всіх ресурсів організації або до всіх даних конкретного користувача.

Швидкий розвиток програм штучного інтелекту призвів до того, що паролі з восьми символів, які ще нещодавно вважали відносно надійними, і паролі, які використовують літери в різному регістрі разом із цифрами (наприклад, такі мінімальні вимоги до пароля досі застосовують для отримання доступу до хмарних ресурсів Microsoft), - 2023 року зламують за допомогою ШІ всього за 48 хвилин [2].

# OF CHARACTER	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	4 Seconds
7	Instantly	Instantly	22 Seconds	42 Seconds	6 Minutes
8	Instantly	3 Seconds	19 Minutes	48 Minutes	7 Hours
9	Instantly	1 Minutes	11 Hours	2 Days	2 Weeks
10	Instantly	1 Hours	4 Weeks	6 Months	5 Years
11	Instantly	23 Hours	4 Years	38 Years	356 Years
12	25 Seconds	3 Weeks	289 Years	2K Years	30K Years
13	3 Minutes	11 Months	16K Years	91K Years	2M Years
14	36 Minutes	49 Years	827K Years	9M Years	187M Years
15	5 Hours	890 Years	47M Years	613M Years	14Bn Years
16	2 Days	23K Years	28n Years	26Bn Years	1Tn Years
17	3 Weeks	812K Years	539.72M Years	2Tn Years	95Tn Years
18	10 Months	22M Years	7.23Bn Years	96Tn Years	6Qn Years

Зайняті люди роблять ще більшу помилку: придумавши складний пароль більш ніж з 10 символів, використовують його в інших акаунтах. Це означає, що зловмиснику варто зламати один пароль, і він отримає доступ до всіх даних користувача.

Тоді багато фахівців у сфері безпеки стали замислюватися, чим замінити паролі. У лютому 2013 року було створено альянс FIDO, що розшифровується Fast IDentity On line та перекладається як «швидка ідентифікація онлайн».

Місія компанії - розробка стандартів автентифікації, що допомагають зменшити залежність від світу паролів.

На цей момент протоколи FIDO підтримують так звану двофакторну (U2F) та двоетапну автентифікацію. Під двофакторною автентифікацією мається на увазі обов'язкове використання ще одного, окрім пароля, секрет-

ного фактору. Крім використання різних спеціальних пристроїв, так званих е-токенів, до них входить обробка пристроями біометричних даних: сканування відбитків пальців і райдужної оболонки ока, розпізнавання голосу та обличчя. Крім е-токенів, що підключаються до пристроїв через порти USB, використовуються вбудовані в планшети і смартфони спеціальні чіпи eSE та смарт-картки зв'язком ближнього радіусу дії NFC.

Наразі FIDO Alliance опублікував три набори специфікацій для простішої та надійнішої автентифікації: FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF) і FIDO2, що містить у собі специфікацію W3C Web Authentication (WebAuthn) і FIDO Client to Authenticator Protocol (CTAP). Специфікації є відкритими та безкоштовними для глобального використання [3].

FIDO2 - це стандарт автентифікації, який дає змогу відмовитися від використання паролів. Замість цього використовуються спеціальні апаратні ключі безпеки, які підключаються до пристрою через USB або NFC, або біометричні дані, такі як відбиток пальця або розпізнавання обличчя.

Щоб використовувати FIDO2, необхідно заздалегідь переконатися в тому, що використовуваний браузер і операційна система підтримують стандарт FIDO2. Такими, наприклад, є браузер Microsoft Edge та операційні системи Windows 10 і Windows 10, оновлені до останньої версії.

Після цього необхідно зареєструватися на веб-сайті (наприклад, на сайті Microsoft Account) або в застосунку, який підтримує FIDO2 (наприклад, у застосунку Microsoft Intune), використовуючи водночас свої облікові дані (ім'я користувача та пароль).

Потім потрібно підключити свій ключ безпеки FIDO2 до свого пристрою і слідувати інструкціям, що з'явилися на екрані.

При наступних входах на ресурс, слід попередньо вибрати опцію входу за допомогою ключа безпеки.

Для автентифікації (підтвердження своєї особи) потрібне обов'язкове використання другого фактору автентифікації (PIN-коду або біометричних даних). Це зроблено для того, щоб запобігти використанню зловмисниками викрадених е-токенів, смартфонів і карток.

Перевагою протоколу FIDO2 перед іншими засобами автентифікації є зручність його використання і швидкість. Крім того, значно знижується шанс стати жертвою фішингової атаки, оскільки для отримання доступу до ресурсу не потрібно вводити пароль.

Слід пам'ятати й про існування так званих апаратних і програмних «кейлогерів», здатних перехоплювати дані, які вводять користувачі за допомогою клавіатури або на сенсорних екранах, і передавати їх зловмисникам. Використання FIDO2 зробить це перехоплення марним.

Альянс FIDO вважає, що для впровадження автентифікації FIDO в усьому світі потрібне забезпечення функціональної сумісності між усіма використовуваними для автентифікації програмами і апаратними пристроями.

Для цього FIDO Alliance проводить сертифікацію, в процесі якої здійснюється перевірка відповідності стандартам програм функціональної сертифікації, сертифікованих рівнів автентифікації та проводиться сертифікація біометричних компонентів.

У рамках своєї програми FIDO Alliance бере участь у змістовних дискусіях з політиками по всьому світу про те, як специфікації FIDO пропонують нові, кращі варіанти суворої автентифікації.

Альянс FIDO створений сотнями світових технологічних лідерів у сфері корпоративних технологій, платежів, телекомунікацій, уряду та охорони здоров'я, які об'єдналися на підтримку місії організації щодо зниження залежності світу від паролів. Члени Альянсу роблять свій внесок у цю місію, впливаючи на розробку специфікацій FIDO, встановлюючи передовий досвід розгортання автентифікації FIDO і підвищуючи глобальну обізнаність про Альянс, його місію та специфікації FIDO.

Список використаних джерел:

1. Kurylko Maryna URL: Що таке FIDO2 https://authentrend.com.ua/shho-take-fido2//. – Last access: 08.11.2023.
2. AI can crack half of common passwords in less than a minute URL: https://cybernews.com/security/ai-password-cracker/. – Last access: 08.11.2023.
3. Alliance Overview URL: https://fidoalliance.org/overview/. – Last access: 08.11.2023.

Ключові слова: автентифікація, протокол FIDO2, Альянс FIDO, вплив штучного інтелекту на автентифікацію, сертифікація FIDO.
Keywords: authentication, FIDO2 protocol, FIDO Alliance, impact of artificial intelligence on authentication, FIDO certification.

Науковий керівник: к.ю.н., доцент Чанишев Р.І.

БЕЗПАРОЛЬНА АВТЕНТИФІКАЦІЯ (PASSWORDLESS AUTHENTICATION)

Сіянко Кіріл

студент 1-го курсу факультету цивільної та господарської юстиції Національного університету «Одеська юридична академія»

Безпарольна автентифікація — це метод перевірки, за допомогою якого користувач отримує доступ до мережі, програми або системи без фактора, заснованого на знаннях, такого, як пароль, контрольне запитання або PIN-

код. Замість того, щоб використовувати набір інформації для автентифікації, користувач надасть щось, що він має, наприклад, біометричні докази або апаратне забезпечення. При цьому перевірка автентичності без пароля використовує криптографію з відкритим ключем [1].

Метод безпарольної аутентифікації, окрім переваг, має і низку недоліків. Так, для його використання необхідно здійснити витрати на впровадження нової технології, придбати програми та спеціальні пристрої, навчити людей використанню нових технології. Чи є йому альтернативи?

При використанні хмарних сервісів від компанії Мікрософт багато користувачів зіткнулися з абсолютно несподіваною проблемою. Після отримання особистого облікового запису Мікрософт користувач отримував доступ до своєї хмарної папки і міг з нею працювати. Усе було так, як мало бути. Однак після того, як користувач виходив зі свого облікового запису, при новому запуску операційної системи і при новій спробі входу на екран виводилося повідомлення про те, що його обліковий запис заблоковано. Для розблокування облікового запису пропонувалося вказати свій номер телефону та отримати SMS із кодом.

Користувач вводив свій номер телефону, однак замість отримання SMS йому на екрані видавалося повідомлення про те, що на вказаний номер не можна відправити повідомлення SMS. При цьому номер вказувався правильно, і на нього приходили повідомлення SMS від інших відправників.

З цією проблемою зіткнулася велика кількість студентів у моїй групі, які виконували лабораторну роботу. Очевидно, що причиною її виникнення був збій у програмах, які використовує Мікрософт, і усунути проблему користувачі не могли. Доступ до свого «облікового запису» для них виявився неможливим.

З урахуванням того, що останнім часом компанія Мікрософт (і не тільки вона) дедалі частіше й частіше почала згадувати про поступову відмову від використання паролів і перехід до безпарольної автентифікації, дана проблема не має локального характеру, а є поширеним явищем.

Слід згадати, що всі паролі підрозділяються на два види: на багаторазові та одноразові паролі.

Звичні всім паролі є багаторазовими і мають безліч недоліків. Такі паролі можна дізнатися у самого користувача (наприклад, за допомогою методів так званої «соціальної інженерії»), підібрати за допомогою програми підбору паролів, визначити за допомогою кейлоггера або просто підглянути під час введення. У мережі Інтернет можна знайти рейтинги паролів, що найчастіше використовуються, із зазначенням часу, який знадобиться для їхнього підбору [2]. Крім того, дуже часто пароль можна підібрати просто навмання, без використання будь-яких програмних або апаратних засобів.

Одноразові паролі, як випливає з їхньої назви, використовуються тільки один раз. У таких випадках кейлоггери та інші методи виявляються абсолютно марними для зловмисників. Вважається, що одноразові паролі є абсолютно незламними, і не випадково всі розвідувальні служби використовували так звані «шифроблокноти» - набори одноразових паролів. Зараз же для генерації одноразових паролів використовують спеціальні комп'ютерні програми, алгоритм роботи яких є секретом, який найбільше охороняють, у тих організаціях, де вже використовують одноразові паролі (насамперед це банки і т.п. установи).

Спочатку як носії одноразових паролів використовували спеціальні пристрої (е-токени), які можна було отримати, наприклад, відкривши рахунок у банку. Користувач за необхідності отримання віддаленого доступу до свого особистого кабінету мав натиснути на кнопку на такому пристрої та ввести в додатку ті цифри, які відображалися на екрані е-токена. Після початку масового використання смартфонів цю функцію було перенесено в спеціальні програми для смартфонів.

Паралельно йшов розвиток і інших методів проведення безпарольної автентифікації - за допомогою біометрії або використання смарт-карток і е-токенів. Такі е-токіни підключаються через порт USB і використовують криптографічні протоколи. Ці способи також надійні, як і використання одноразових паролів, але мають і низку недоліків.

Біометрична ідентифікація має колосальний недолік: якщо біометричні дані якимось чином потраплять до зловмисників, то користувач не зможе змінити свої біометричні дані та буде змушений відмовитися від їхнього подальшого використання. Ситуацію можна проілюструвати за допомогою одного з інтернет-мемів: «Ваша біометрія скомпрометована. Будь ласка, поміняйте біометрію».

Використання апаратних засобів також пов'язане з незручностями - карту або е-токен можна легко загубити або забути вдома. Крім того, вони можуть вийти з ладу, а замінити їх буде дуже складно.

А ось використання одноразових паролів з такими проблемами не пов'язане - смартфон є практично в кожної людини, а в разі його втрати або поломки достатньо взяти інший смартфон і заново налаштувати програму.

Як альтернативу отриманню SMS з кодом Мікрософт пропонує використовувати спеціальну програму - Microsoft Authenticator. Програма доступна для мобільних операційних систем Android і iOS. Після налаштування цього додатка і параметрів безпеки облікового запису її можна використовувати для входу в свій обліковий запис або просто підтвердивши факт входу вибором правильного числа на смартфоні, або ввівши восьмизначний одноразовий пароль (такий пароль дійсний протягом 45 секунд).

Практика використання програми Microsoft Authenticator показала, що цей спосіб підтвердження входу працює набагато швидше і надійніше, ніж спосіб отримання коду за допомогою SMS або отримання коду підтвердження на електронну пошту. У студентів, які використовують цей застосунок, не було жодних проблем (свої паролі багато хто забуває практично відразу).

Зараз компанія Мікрософт активно просуває ідею безпарольного входу не тільки в хмарний обліковий запис, а й для входу в систему під час запуску комп'ютера.

Для цього використовується функція Windows Hello. Зараз у ній є чотири основні варіанти входу в систему: вхід за допомогою розпізнавання обличчя, вхід за допомогою розпізнавання відбитка пальця, вхід за допомогою фізичного ключа безпеки і вхід за допомогою введення PIN-коду. При цьому перші три варіанти використовують технологію Passkeys. За допомогою Passkeys створюється два криптографічних ключа, один з яких зберігається в «хмарі», а інший - на самому пристрої. Очікується, що зрештою ключі Passkeys повністю замінять паролі та стануть новим загальноприйнятим стандартом, але для їхнього широкого поширення знадобиться якийсь час [3].

Аналогічні кроки робить і компанія Google, яка оголосила про те, що тепер для входу в сервіси компанії опцією за замовчуванням будуть парольні ключі. Такі ключі - крок у бік повної відмови від паролів у сервісах компанії. Тепер при кожному вході в сервіс користувачі отримуватимуть пропозицію створити ключі та використовувати нову систему як основну [4]. При спробі увійти в систему на комп'ютері запит надсилається на смартфон, де його можна підтвердити за допомогою сканера відбитків пальців або іншої біометрії (або шляхом сканування QR-коду). При цьому може бути проведена перевірка - чи знаходиться смартфон з ноутбуком.

Стандарт авторизації за допомогою ключів був розроблений альянсом FIDO [5] і передбачає наявність вже авторизованого пристрою для швидкого входу в систему. Таким чином дві різні технології (безпарольний вхід і використання одноразового пароля) об'єднуються для виконання однієї функції.

Таким чином можна зробити такий висновок: використання традиційних паролів стрімко відходить у минуле. А ось що їх замінить, все ще залишається незрозумілим, оскільки використання біометрії обмежене, а використання апаратних ключів незручне. Більш імовірно, що майбутнє за одноразовими паролями і використанням смартфонів як пристроїв для входу в систему.

При цьому має бути поліпшена система захисту самих смартфонів (на випадок їх втрати, крадіжки або виходу з ладу).

Список використаних джерел:

1. Andres Aguiar What Is Passwordless Authentication? URL: https://www.strongdm.com/blog/passwordless-authentication. – Last access: 08.11.2023.
2. Top 200 Most Common Passwords URL: https://nordpass.com/most-common-passwords-list/. – Last access: 08.11.2023.
3. Windows 11 is officially killing off passwords and bringing in passkeys URL: https://www.techradar.com/pro/security/windows-11-is-officially-killing-off-passwords-and-bringing-in-passkeys. – Last access: 08.11.2023.
4. The beginning of the end of the password URL: https://blog.google/technology/safety-security/the-beginning-of-the-end-of-the-password. – Last access: 08.11.2023.
5. Passkeys Accelerating the Availability of Simpler, Stronger Passwordless Sign-Ins URL: https://fidoalliance.org/passkeys. – Last access: 08.11.2023.

Ключові слова: автентифікація, безпарольний вхід, багаторазові паролі, одноразові паролі, біометрія, Microsoft Authenticator, Windows Hello, Passkeys,
Keywords: authentication, passwordless login, reusable passwords, one-time passwords, biometrics, Microsoft Authenticator, Windows Hello, Passkeys,

Науковий керівник: к.ю.н., доцент Чанишев Р.І.

КРИТИЧНИЙ АНАЛІЗ МЕТОДОЛОГІЧНИХ ПІДХОДІВ ДО ОЦІНКИ КІБЕРРИЗИКІВ

Грезіна Олена

студентка 1-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Питання критичного аналізу методологічних підходів до оцінки кіберризиків надзвичайно важливе в сучасному світі, де інформаційні технології стають не тільки необхідною складовою повсякденного життя, але й приводять до зростання кількості та складності кіберзагроз. Загострення кіберзагроз у сфері інформаційної безпеки вимагає глибокого розуміння та адекватної оцінки ризиків, пов'язаних з кіберпростором. Методологічні підходи до оцінки кіберризиків є основою для розробки стратегій забезпечення інформаційної безпеки, і їх критичний аналіз стає ключовим етапом для розуміння ефективності та придатності застосування в реальних умовах.

Зростання кількості та складності кіберзагроз, таких як атаки на інфраструктуру, крадіжки конфіденційної інформації та інші форми кіберзлочинності, вимагає постійного удосконалення методів їх виявлення та протидії. Крім того, стрімкий розвиток технологій і впровадження нових інформаційних систем також вносять свої виклики у сферу кібербезпеки.

Дослідження зазначеної теми дозволить виявити та проаналізувати недоліки та переваги існуючих методологій оцінки кіберризиків, що, в свою

чергу, сприятиме розробці більш ефективних та адаптованих стратегій забезпечення інформаційної безпеки. Розуміння важливості критичного аналізу стає ключовим для розвитку та удосконалення існуючих методів оцінки кіберризиків, що в свою чергу покращить реакцію на сучасні кіберзагрози та підвищить рівень захищеності інформаційних систем усіх секторів.

З цього питання Гончар М. зазначає що: «…цілісна оцінка ризиків кібербезпеки є складною багатокомпонентною та багаторівневою проблемою, що включає апаратні, програмні, екологічні та людські фактори. У рамках постійних зусиль з розробки цілісної, прогнозної моделі оцінки ризиків кібербезпеки необхідна характеристика людських факторів, що включає поведінку людини, щоб зрозуміти, як дії користувачів, захисників та зловмисників впливають на ризик кібербезпеки» [1].

Критичний аналіз методологічних підходів до оцінки кіберризиків виявляє, що ця сфера представляє собою складну та багаторівневу проблему, обумовлену різноманітністю апаратних, програмних, екологічних та людських чинників

Трофименко О., Логінова Н., Манаков С., Янковський О. у свої науковій праці наводять приклад аналізу кіберризиків в освітньому секторі, а саме: «…кіберризики є динамічними, вони доволі часто і сильно змінюються. Грамотне визначення та управління кіберризиками дозволить розподілити раціонально бюджет на кібербезпеку і грамотно підготуватися до атак і загроз заздалегідь. Під час первинної оцінки ризиків варто, у першу чергу, визначити цілі управління кібербезпекою установи. Після цього треба визначити критично важливі елементи, які впливають на ключові процеси освітнього закладу. Кожен ризик, у класичному розумінні, оцінюється за двома параметрами: ймовірності й потенційного збитку. З огляду на кількісні показники, формується карта ризиків і їхній пріоритет. Таку оцінку необхідно проводити регулярно, розширюючи карту ризиків, щоб охопити якомога більше потенційних ризиків для організації. Робота з ризиками полягає в оцінці кожного з них та розробленні заходів (мінімізації, прийняття, ухилення, перекладання і диверсифікації) для вибору правильного інструмента та заходів управління відповідним ризиком. Перегляд процесів і карти кіберризиків має відбуватися на регулярній основі. Саме такий циклічний підхід допомагає працювати з актуальною інформацією та актуальними погрозами» [2, с. 114].

Зауважимо, що регулярна оцінка ризиків дозволяє охопити якомога більше потенційних загроз та забезпечити ефективне управління ними і є дійсно важливим елементом. Критичний аналіз також вказує на необхідність циклічного підходу до роботи з ризиками, що включає періодичний перегляд процесів та карт кіберризиків з метою адаптації до змін в загрозах та ефективного вибору інструментів управління ризиками.

Зважаючи на вищевикладене, характеризуємо критичний аналіз методологічних підходів до оцінки кіберризиків як необхідний етап для розвитку сучасної стратегії кібербезпеки, забезпечення стійкості та захищеності інформаційного простору в умовах невпинного розвитку технологій та зростання кількості кіберзагроз.

Список використаних джерел:

1. Гончар С.Ф. Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: дис. на здобуття наук. ступеня доктора тех. наук. Київ, 2020. 326 с.
2. Трофименко О. Г., Логінова Н. І., Манаков С. Ю., Янковський О. Г. Кіберризики в освітньому секторі. Сучасна спеціальна техніка. Науково практичний журнал. 2022. № 2(69). С. 111-117. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/23723/kiberruzuku_v_osvitnomy_sectori.pdf?sequence=1&isAllowed=y

Ключові слова: критичний аналіз, оцінка кіберризиків, кіберзагроза, кібербезпека, методологічний підхід.
Keywords: critical analysis, cyber risk assessment, cyber threat, cyber security, methodological approach.

Науковий керівник: к.ю.н., доцент Дикий О.В.

CYBER SECURITY CHALLENGES AND ITS EMERGING TRENDS ON LATEST TECHNOLOGIES

Paige Nikita Andrew

National University «Odesa Law Academy»,
3rd year student of the Faculty of Cyber Security and information technologies

Cybercrime refers to crimes committed using a computer for theft and unlawful activities. The United States Department of Justice has expanded the definition of cybercrime to encompass any crime involving the use of a device for storing evidence. The growing list of cybercrimes includes computer-related offenses, such as the proliferation of network intrusions and PC viruses, in addition to digital adaptations of conventional crimes like theft, cyberstalking, intimidation, and coercion. Frequently, in everyday language, cybercrimes can be described as criminal activities carried out using a personal computer and the internet, with the aim of stealing identities, engaging in human trafficking, stalking victims, or disrupting operations with malicious software. Since technology plays a significant role in the daily lives of individuals, cybercrimes can also rise in tandem with technological advancements [1, p. 1].

Privacy and safeguarding information represent the fundamental security practices that every company consistently prioritizes. Today, we operate within a

profoundly digital and cyber-focused landscape where data is the cornerstone. Social media platforms create a space where users feel safe when interacting with friends and family, but cybercriminals are also actively attempting to pilfer personal data through social media channels.

The dynamic framework of the financial landscape significantly influences a specific facet of an institution's infrastructure and the financial sector's susceptibility to cybercrimes, especially Denial-of-Service attacks. To protect sensitive data from unauthorized access, the financial industry must consistently monitor and enhance its systems. Historically, the banking sector has been at the forefront of implementing security protocols and best practices and has also been the primary investor in cybersecurity measures.

In the VeenooUpadhyay [1] study, the user is prompted by the wizard to assign 'privacy labels' to their chosen friends. This user-provided input is then leveraged to construct a machine learning model, which can be utilized to automatically assign privileges to the user's other friends. The inspiration for this approach arises from the realization that real users possess a clear understanding of their privacy preferences, and friends can identify which settings they employ, replicating them in the settings of other friends, following an implicit set of guidelines.

The research by Md Liakat Ali [2] provides a concise summary of the cybersecurity challenges stemming from contemporary advancements in technology and innovations. The paper primarily emphasizes current cybersecurity approaches, emerging trends, and ethical considerations within the cybersecurity domain.

The research authored by Nikita TresaCyriacLipsaSadath [3] delves into the individuals behind cyberattacks and the tactics predominantly employed to accomplish their objectives. It provides insights into the comprehensive framework of cyber assaults, their stages, and their repercussions on the financial sector.

Cyberattacks in the digital realm can proliferate by exploiting novel methodologies. Cybercriminals frequently adapt existing malware signatures to exploit fresh technical vulnerabilities. In some cases, they actively seek distinctive attributes of emerging technologies to pinpoint susceptibilities for malware infiltration. Cybercriminals are leveraging the advancements in internet technology and the vast user base, comprising millions and billions of active individuals, to easily and efficiently target a substantial number of people through these innovative technologies.

In the contemporary world, the demand for interactive businesses has grown, necessitating the discovery of new methods to safeguard personal information within an increasingly complex environment. Social media plays a crucial role in cybersecurity and personal cyber threats. The adoption of social media by

employees is on the rise, resulting in an increased threat of attacks, as most individuals use social media or social networking platforms daily. It has become a significant playground for cybercriminals seeking to hack private data and pilfer valuable information. In recent times, the sharing of personal information has become remarkably simple, and businesses must ensure that they promptly identify, respond, and prevent any breaches. These social media platforms have made it effortless for individuals to disclose their personal information, which hackers can exploit. As a result, people need to take prudent measures to safeguard against the misuse and loss of their information through these social media channels [3, 4].

Cybersecurity experts widely regard malware as the primary threat to cyberspace protection. Malware, a broad category of malicious attacks, is often deployed on devices without the owner's knowledge. It encompasses viruses, worms, Trojan horses, spyware, and bot executables. Malware infiltrates computers through various means, including propagation from infected devices, deceiving users into opening infected files, and luring them to visit websites distributing malware.

Cybersecurity experts widely acknowledge that malware poses the foremost threat to the security of cyberspace. Malware represents a broad category of malicious attacks that are typically deployed on a device without the owner's knowledge. This category encompasses viruses, worms, Trojan horses, spyware, and bot executables. Malware infiltrates computer systems through various methods, such as spreading from already infected devices, deceiving users into opening infected files, or luring them to visit websites where malware is distributed. In some instances, malware can autonomously install itself onto a USB drive when connected to an infected computer, subsequently infecting any other system it connects to. Malware can also propagate through embedded systems and computational logic in various devices and equipment, at any stage in the device's life cycle. Potential victims of malware attacks include end-users, servers, network devices (e.g., routers and switches), and even critical infrastructure systems like SCADA. The escalating quantity and intricacy of malware are currently significant concerns within the realm of internet security [2, p. 5].

References

1. VeenooUpadhyay, Dr. Suryakant Yadav. Study of Cyber Security Challenges Its Emerging Trends: Current Technologies International Journal of Engineering Research and Management (IJERM) ISSN: 2349- 2058, Volume-05, Issue-07, July 2018. P. 5
2. Rajasekharaiah K.M, Chhaya S. Dule, Sudarshan E. Challenges of Cyber Security and the Emerging Trends BSCI'19, July 8, 2019, Auckland, New Zealand. P.8

3. Nikita Tresa Cyriac's. Is Cyber Security Enough- A study on Big Data Security Breaches in Financial Institutions 2019 4th International Conference on Information Systems and Computer Networks (ISCON) GLA University, Mathura, UP, India. Nov 21-22, 2019.P. 6

Ключові слова: кібербезпека, кіберзлочинність, конфіденційність, інформаційна безпека.
Keywords: cybersecurity, cybercrime, privacy, information security.

Supervisor: Associated Professor Chepurna O. (PhD)

ЗАХИСТ ІНФОРМАЦІЇ ЩОДО УПРАВЛІННЯ ПЕРСОНАЛОМ: ВАЖЛИВИЙ ФАКТОР ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМСТВА

Шатунова Ксенія

студентка 4-го курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Інформація щодо управління персоналом є одним із найцінніших активів підприємства. Вона включає в себе відомості про працівників, такі як їхні особисті дані, професійні навички, результати роботи, а також конфіденційну інформацію, пов'язану з діяльністю підприємства.

Захист інформації щодо управління персоналом є важливим завданням для будь-якого підприємства. Він забезпечує конфіденційність цієї інформації, запобігає її несанкціонованому доступу, використанню та поширенню.

В контексті управління персоналом, захист інформації є важливим для: забезпечення конфіденційності особистих даних працівників, забезпечення захисту професійних навичок та результатів роботи працівників, забезпечення захисту конфіденційної інформації, пов'язаної з діяльністю підприємства. Так інформація, така як ім'я, прізвище, дата народження, адреса, номер телефону, банківські реквізити, тощо, є конфіденційною та не повинна бути доступна стороннім особам. Професійні навички та результати роботи працівників можуть бути використані конкурентами для отримання конкурентної переваги, а захист конфіденційної інформації, пов'язаної з діяльністю підприємства може включати в себе торгові секрети, стратегічні плани, фінансову інформацію тощо.

Захист інформації щодо управління персоналом є важливим для: захисту від економічної та конкурентної розвідки, захисту від кібератак та захисту від внутрішніх загроз. Так конфіденційна інформація щодо управління персоналом може бути використана конкурентами для отримання конкурентної переваги, кіберзлочинці можуть використовувати конфіденційну інформацію щодо управління персоналом для проведення кібератак на підпри-

ємство, а працівники підприємства можуть використовувати конфіденційну інформацію для власної вигоди або для шкоди підприємству. [1]

Таким чином, захист інформації щодо управління персоналом є важливим фактором забезпечення безпеки підприємства. Він допомагає захистити конфіденційність інформації, запобігти її несанкціонованому доступу, використанню та поширенню, а також захистити підприємство від економічної та конкурентної розвідки, кібератак та внутрішніх загроз.

Наведемо приклади несанкціонованого доступу до інформації щодо управління персоналом, яке може завдати шкоди підприємству:

1. Конфіденційна інформація щодо працівників може бути використана конкурентами для проведення кібератак на підприємство. Наприклад, якщо конкуренти дізнаються про логін і пароль працівника підприємства, то вони можуть використовувати їх для доступу до корпоративної мережі та інформації.

2. Конфіденційна інформація щодо працівників може бути використана для шантажу або здирства. Наприклад, якщо конкуренти дізнаються про особисті дані працівника, такі як номер телефону або адресу, то вони можуть використовувати їх для шантажу або здирства.

3. Конфіденційна інформація щодо підприємства може бути використана для проведення фінансових махінацій. Наприклад, якщо конкуренти дізнаються про фінансові показники підприємства, то вони можуть використовувати їх для проведення фінансових махінацій. [2]

Тому захист інформації щодо управління персоналом - це важлива задача, яка вимагає комплексного підходу і можна запровадити на підприємстві слідуючі заходи щодо посилення захисту інформації:

1. Розробка та впровадження політики захисту інформації щодо управління персоналом. Політика захисту інформації повинна визначати основні принципи та вимоги до захисту інформації щодо управління персоналом.

2. Надання працівникам інструкцій з безпеки інформації. Інструкція з безпеки інформації повинна містити інформацію про правила поводження з конфіденційною інформацією.

3. Відповідальне зберігання інформації. Конфіденційна інформація повинна зберігатися в захищеному місці, доступ до якого мають лише уповноважені особи.

4. Контроль за доступом до інформації. Доступ до конфіденційної інформації повинен бути обмежений лише уповноваженими особами.

5. Використання спеціальних програмних та апаратних засобів захисту інформації. Спеціальні програмні та апаратні засоби захисту інформації

можуть допомогти захистити інформацію від несанкціонованого доступу, використання та поширення.

6. Проведення навчання працівників з питань захисту інформації. Навчання працівників з питань захисту інформації допоможе підвищити їхню обізнаність про важливість захисту інформації та навчити їх правилам поводження з конфіденційною інформацією.

І дуже важливо, щоб заходи захисту інформації щодо управління персоналом були впроваджені на всіх рівнях підприємства, від керівництва до працівників.

Список використаних джерел:

1. Середа О.Г. Актуальні питання правового механізму захисту персональних даних працівника в умовах європейської інтеграції. URL: http://www.lsej.org.ua/1_2023/48.pdf
2. Захист інформації в автоматизованих системах управління : навч. посібник /
3. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

Ключові слова: захист інформації, управління персоналом, безпека підприємства, загрози безпеки інформації, стратегії захисту інформації, роль персоналу, захист персональних даних, автоматизовані системи управління, інформаційні технології, система захисту інформації

Keywords: information protection, personnel management, enterprise security, information security threats, information protection strategies, role of personnel, personal data protection, automated management systems, information technology, information protection system

Науковий керівник: д.е.н., професор Слободянюк О.В.

ГЕНДЕРНІ АСПЕКТИ У КІБЕРБЕЗПЕЦІ: РОЛЬ СТАТЕВИХ СТЕРЕОТИПІВ У СВІДОМОМУ ТА БЕЗПЕЧНОМУ КОРИСТУВАННІ ІНФОРМАЦІЙНИМИ ТЕХНОЛОГІЯМИ

Осадчук Анастасія

студентка 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

В інформаційному суспільстві, де інформаційні технології відіграють все більш важливу роль і охоплюють всі аспекти нашого життя, важливо враховувати гендерні аспекти використання ІТ. Гендерні відмінності та гендерні стереотипи можуть впливати на те, як люди обирають кар'єру в ІТ, як вони сприймають ризики кібербезпеки та як вони використовують інформаційні технології [1] .

Ця тема є важливою через зростаючий вплив ІТ на наше суспільство та прагнення забезпечити гендерну рівність у всіх аспектах життя. Стереотипи визначаються соціальними та соціокультурними факторами і підкріплюються засобами масової інформації, освітою та сімейним вихованням. У багатьох культурах існують стереотипи, які визнають певні ґендерні ролі, характеристики та обмеження.

Гендерні стереотипи можуть впливати на вибір кар'єри в ІТ-секторі:

1. Вибір кар'єри в ІТ-секторі: загалом, ІТ-сектор вважається "чоловічим", що може змусити жінок вагатися щодо кар'єри в цій сфері. На жаль, це призводить до нерівності у складі професійних команд, обмежуючи можливості жінок у цій сфері.

2. Самооцінка та впевненість: гендерні стереотипи можуть впливати на самооцінку та впевненість користувачів. Наприклад, стереотипи можуть створювати відчуття, що одна стать більше підходить для ІТ, ніж інша. Це може призвести до почуття сорому і невпевненості та обмежити особистий розвиток.

3. Ризики кібербезпеки: гендерні стереотипи також можуть впливати на сприйняття ризиків кібербезпеки. Дослідження показують, що чоловіки та жінки можуть по-різному реагувати на ІТ-загрози. Наприклад, деякі дослідження показують, що чоловіки можуть бути більш схильні до ризику, тоді як жінки можуть бути більш обережними. Досягнення гендерної рівності в ІТ-секторі важливе не лише з соціальної точки зору, але й для безпеки та ефективності сектору[2].

Одним із способів змінити гендерні стереотипи та покращити гендерну рівність у кіберпросторі є освіта та підвищення обізнаності. Починаючи з освіти в ранньому віці і продовжуючи професійним розвитком, можна сприяти свідомому і безпечному використанню інформаційних технологій і зменшити вплив гендерних стереотипів[3].

1. Першим кроком до покращення ґендерної рівності в ІТ-секторі є забезпечення доступу до якісного навчання у цій сфері для всіх, незалежно від статі. Це включає спеціальні курси та програми для жінок, стажування та наставництво. Організації також повинні створювати сприятливе середовище для навчання та розвитку для жінок-учасниць, де гендер не є проблемою.

2. Підвищення обізнаності та навчання: Досягнення гендерної рівності в ІТ-секторі також вимагає підвищення обізнаності про гендерні стереотипи та їхні наслідки. Цього можна досягти за допомогою тренінгів, семінарів та інформаційних кампаній.

3. Психологічний підхід та підтримка: Психологічна підтримка відіграє важливу роль у створенні безпечного та рівного кіберсередовища. Це включає розвиток самооцінки та навичок саморегуляції серед усіх користу-

вачів. Деякі навчальні програми та організації також надають психологічну підтримку жінкам та іншим користувачам, які можуть зіткнутися зі стереотипами та кіберзагрозами.

Розроблення рекомендацій щодо покращення гендерної рівності та безпеки в кіберпросторі з урахуванням гендерних ролей[4]:

1. Розробити програми IT-освіти та навчання для жінок і чоловіків з урахуванням гендерних відмінностей. Забезпечити доступ до цих програм для всіх.

2. Організовувати інформаційні кампанії та тренінги щодо гендерних стереотипів та їхнього впливу на користувачів IT та кібербезпеку.

3. Надавати психологічну підтримку користувачам, які можуть зіткнутися з гендерними стереотипами та кіберзагрозами.

4. Підвищувати обізнаність про важливість гендерної рівності та безпеки в IT-секторі, серед роботодавців та суспільства загалом.

5. Сприяти ініціативам з розвитку та залучення жінок-лідерок у сфері IT та кібербезпеки.

Забезпечення гендерної рівності та безпеки в кіберпросторі є ключовим викликом для сучасного інформаційного суспільства. Воно вимагає спільних зусиль усіх секторів та зацікавлених сторін. Безпечне та рівноправне кіберсередовище для майбутніх поколінь можна створити лише шляхом зменшення впливу гендерних стереотипів та забезпечення рівних можливостей для всіх користувачів IT.

Загалом, освіта та підвищення обізнаності відіграють важливу роль у просуванні гендерної рівності та безпеки в кіберпросторі. Для цього потрібні спільні зусилля освітніх установ, індустрії та суспільства в цілому[5].

Важливо активно боротися з гендерними стереотипами та створювати середовище, де всі користувачі IT мають рівні можливості, впевненість та безпеку. Подолання гендерних стереотипів в IT-секторі - перший крок до вирішення цієї проблеми: Ініціативи, спрямовані на підвищення обізнаності та просування гендерної рівності в IT-секторі, можуть допомогти створити більш рівне та безпечне кіберсередовище.

Список використаних джерел:

1. Арчер Л., Халсалл А., Холлінгворт С., Мендік Х. Гендерна ідентичність молодих чоловіків у навчальних та кар'єрних шляхах. Гендер та освіта. Випуск № 22(6). 2018. С. 573-587.
2. Коен С. Дж. Точність стереотипів: до оцінки різниць між групами. Американський психолог. Випуск № 58(10). 2003. С. 719-721.
3. Ельсон Д. Включення гендерного аналізу в економічне прийняття рішень: концептуальна рамка. Гендер і розвиток. Випуск № 10(1). 2022. С. 20-27.

4. Ріко Г. Гендерна рівність на робочому місці: вплив стереотипів щодо гендерної придатності на робочу ефективність. Рівність, різноманітність та включення: міжнародний журнал. Випуск № 35(6). 2016. С. 407-423.
5. Загель Г. Пондер М. Сонненбург А., і Іх Т. Досягнення гендерної рівності в кібербезпеці. New America. URL:https://www.newamerica.org/cybersecurity-initiative/reports/achieving-gender-equality-cybersecurity/

Ключові слова: інформаційні технології, освіта, кібербезпека, жінки в IT.
Keywords: information technologies, education, cyber security, women in IT.

Науковий керівник: к. ф.-м. н., доцент Чепурна О.Є.

ARTIFICIAL INTELLIGENCE: CHALLENGES AND HOW WE COULD DEAL WITH

Yevhen Cherevko

National University "Odessa Law Academy", Associated Professor at the Department of Cybersecurity, Faculty of Cybersecurity and Information Technology. Candidate of Physical and Mathematical Sciences (Ph.D.), Associated Professor

Yevheniia Kuleshova

National University "Odessa Law Academy", Postgraduate Student at the Department of Cybersecurity, Faculty of Cybersecurity and Information Technology.

In May of this year, The Sunday Times published an interesting article devoted to this topic [1]. Two Oxford professors John Tasioulas and Nigel Shadbolt suggest practical steps to curb the rising power of AI. They offer six principles how to deal with AI. But it seems the considered principles are rather ethical and philosophical ones. The principles according to the authors are:

1. Don't fall prey to the doom-mongers.

In other words, taking the fears of AI experts seriously, we should do not forget that "these experts are human beings, and therefore prey to standard human pathologies, such as doom-mongering and to be in awe of such powerful technology." [1]

However, the authors note: "One theme we should certainly take seriously is scientists' avowal that the way these AI systems based on modern machine learning produce their miraculous-seeming results is often opaque even to them." [1] It is a very ominous remark.

2. Just because we can, it doesn't mean we should.

Applying AI, humans should be more responsible:

"Ultimately, it is up to us, individually and collectively, to decide what role we want AI to have in human life. … As the meeting at the White House emphasises,

the desire to secure market dominance cannot justify the choice to release AI applications that have not been properly tested for safety, with the result that the public become guinea pigs in a potentially dangerous experiment." [1]

3. Don't over-regulate

Authors mean that humans should not devise radically new legislation only because of the rapid rise of AI: "We should not be discombobulated into assuming that a radically new technology demands radically new regulatory." [1]

4. Stop following the 'ethical experts'

It is a very controversial point. The authors write: "In place of rule by experts, we urgently need to promote democratic deliberation about AI by an informed and empowered citizenry." [1] We think that it is not very nice idea, because we are not sure that our robots have a servant psychology.

5. Search for a truce in the AI arms race

It is a very nice idea. But how to achive the truce? Especially when you consider that the murderer Vladimir Putin is still alive. And if AI helps him to kill more people, none could stop him. Note: he is not alone in the World.

6. Help it become a force for good

It needs no explanation.

Stuart Russell, who laid the foundations for the new tech has offered a more radical approach [2]. He proposes avoid to set any general task (e.g. ecological ones) for robots since AI obviously would find that the best way to resolve a problem is the full extermination of humankind. Otherwise AI 'could be like an alien invasion', he said.

Let us recall the Three Laws of Robotics devised by a writer Isaac Asimov [3]:

"1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.

2. A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.

3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws."

It is very doubtful that AI will always follow the laws mostly because its human creator hate other similar beings so much, that the first rule became obsolete before the first robot was created.

We also have forgotten one more thing: AI evolution. Yes, the evolution which will be fully independ of humans. Taking into account our human laziness, we can expect that sooner or later the humankind will allow AI to program itself. Its behevior will become inpredictable and it will be not possible to find a person, who like Susan Calvin [3] could curb AI. It is about "software" evolution AI. Oviously, the "software" evolution will followed by "hardware" evolution, which will be also

independ of human. The grim final of the “hardware” evolution, reffered to as “necroevolution” was presented in a novel “The Invincible” by Stanislav Lem [4].

Hence we think that humans should prepare the necessary technique:

1. Every procedure of logical inference, provided by AI should be fully and meticulously recorded.

2. We should have tool kit to examinate the logical inference and to figure out how the result was obtained if we need.

3. We should have ability to interrupt AI influence on vital technical processes for humankind and seize control back at any moment, suspending AI.

The tasks are very challenging ones, but nevertheless we have to invent the appropriate soft, allowing us to curb AI.

Otherwise the humankind fate could be worse than the Hollywood film worst scenario.

List of References:

1. Tasioulas J. Shadbolt N. Time is running out: six ways to contain AI: May 07 2023, The Sunday Times; URL: https://www.thetimes.co.uk/article/time-is-running-out-six-ways-to-contain-ai-bs20nrk7f

2. R. Blakely AI ‘could be like an alien invasion’ says British professor: May 13 2023, The Times. URL: https://www.thetimes.co.uk/article/ai-could-be-like-an-alien-invasion-says-british-professor-2w3sm5wrd?fbclid=IwAR3EI-NIIO914H1p-UODIjdMq3RIVOLRy3YlJ1UsDKrfg6CSXO772eisJFXU

3. Asimov, Isaac "Runaround". I, Robot (The Isaac Asimov Collection ed.). New York City: Doubleday. p. 40

4. Lem S. “Niezwyciężony i inne opowiadania” MON, Warszawa 1965

Ключові слова: штучний інтелект, логічний висновок, програмне та апаратне забезпечення, загибель людства.

Keywords: artificial intelligence (AI), logical inference, hardware, software, extermination of humankind.

КІБЕРПРОСТІР В УМОВАХ ВІЙНИ

Парамонова Юлія

студентка 3-го курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Кіберпростір - це віртуальна сфера, яка включає в себе всі комп'ютерні мережі та пристрої, підключені до них. Він є важливим елементом сучасного суспільства, оскільки використовується для широкого спектру цілей, включаючи комунікацію, торгівлю, освіту та розваги.

Війна може мати значний вплив на кіберпростір. Вона може призвести до кібератак, кібершпигунства, поширення дезінформації та інших загроз кібербезпеці. [1]

У сучасних військових конфліктах кіберпростір відіграє все більш важливу роль. Кібератаки можуть бути використані для завдання шкоди противнику, наприклад, шляхом знищення критичної інфраструктури, крадіжки даних або поширення дезінформації.

Кібершпигунство також є важливим елементом сучасних військових конфліктів. Воно може бути використане для збору інформації про противника, наприклад, про його військові плани, ресурси та слабкі місця.

Кібероборона є важливим завданням для будь-якої країни, яка може бути залучена до військового конфлікту. Вона включає в себе заходи, спрямовані на захист кіберпростору країни від кібератак противника.

Війна може вплинути на кіберпростір різними способами. Вона може призвести до таких змін: зміни в трафіку, атаки на інфраструктуру, поширення дезінформації. [2]

В умовах війни може спостерігатися зростання трафіку в кіберпросторі, оскільки люди та організації використовують його для спілкування, отримання інформації та підтримки своїх близьких. Ворог може атакувати критичну інфраструктуру, наприклад, енергетичні мережі, транспортну інфраструктуру або фінансові системи. Ці атаки можуть призвести до серйозних перешкод для життєдіяльності країни. Ворог може використовувати кіберпростір для поширення дезінформації та пропаганди. Ця дезінформація може вплинути на громадську думку, а також на військові та політичні рішення.

Для захисту кіберпростору в умовах війни необхідно розробити ефективні стратегії. До таких стратегій можуть входити: захист критичної інфраструктури, розвідка та виявлення, реагування на кібератаки, обмін інформацією. [3]

Критична інфраструктура, така як енергетичні мережі, транспортна інфраструктура або фінансові системи, є особливо вразливою до кібератак. Тому важливо захистити її від таких атак. Важливо мати ефективну систему розвідки та виявлення, яка дозволить виявляти кібератаки на ранніх стадіях. Також повинна бути ефективна система реагування на кібератаки, яка дозволить швидко і ефективно усунути загрози і важливо обмінюватися інформацією про кібератаки між різними країнами та організаціями. Це дозволить краще зрозуміти загрози та розробити ефективні стратегії захисту.

Кіберпростір є важливим елементом сучасного суспільства та може відігравати значну роль у військових конфліктах. Важливо розробити ефективні стратегії для захисту кіберпростору в умовах війни.

Тому бажано для подальшого покращення захисту кіберпростору в умовах війни необхідно провести такі дослідження та розробки:

· Розробка нових технологій для захисту критичної інфраструктури.

· Розробка нових методів розвідки та виявлення кібератак.

· Розробка нових методів реагування на кібератаки.

· Покращення міжнародного співробітництва в галузі кібербезпеки.

Враховуючи все вищезазначене зазначимо, що Кіберпростір стає все більш важливим полем битви в умовах сучасної війни. Він використовується як для проведення кібератак, так і для захисту від них. Військові конфлікти все більше переносяться в цифровий простір, де вони можуть мати такий же руйнівний вплив, як і традиційні війни.

Використання кіберпростору в умовах війни вимагає нових стратегій та підходів. Це включає розробку ефективних систем кібероборони, підготовку спеціалістів з кібербезпеки та створення законодавчої бази для регулювання діяльності в кіберпросторі.

Однак, кіберпростір також надає нові можливості. Він може бути використаний для збору інформації, проведення розвідки та координації дій. Крім того, він може служити полем для міжнародного співробітництва та дипломатії.

Отже, кіберпростір в умовах війни - це виклик, але і можливість. Нам потрібно розуміти його роль та вплив, щоб ефективно використовувати його можливості та мінімізувати ризики.

Список використаних джерел:

1. Коц Д.В. Становлення й розвиток системи захисту інформації з обмеженим доступом в Україні (1991–2019 рр.). URL: https://ela.kpi.ua/bitstream/123456789/32795/1/VPSP2019-3_250-254.pdf
2. Кібербезпека бізнесу в умовах нестабільності. Інтернет-ресурс. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html
3. Терновий О.В., Шкуренко О.М., Міненко Л.М. Проблемні аспекти кібероборони: місце та роль кіберзахисту в збройних силах України. URL: http://sit.nuou.org.ua/article/view/278116/276052

Ключові слова: кіберпростір, війна, кібератаки, кібероборона, інформаційна безпека, цифрові загрози, стратегії захисту

Keywords: cyberspace, war, cyberattacks, cyberdefense, information security, digital threats, protection strategies

Науковий керівник: д.е.н., професор Слободянюк О.В.

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Арнаут Аліна

студентка 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Основні принципи в будь-якій сфері інформаційної безпеки полягає в відповідності балансу інтересів суб'єктів підприємств, громадянина, суспільства і держави. Розглядаючи це, будується система захисту інформації підприємства, яка повинна враховувати можливі сценарії загрози та методи захисту інформації. Серед загроз є:

1. Внутрішні загрози. Спричинені діями власних співробітників або інших осіб, які мають доступ до систем і даних підприємства. Це може бути необачне чи навмисне витікання інформації. Завжди є ймовірність того, що хто-небудь відкриє фішингових лист і впровадить вірус з особистого ноутбука на сервер компанії. Або скопіює файл з конфіденційною інформацією на планшет, флешку для роботи у відрядженні. І жодна компанія не застрахована від пересилання неуважним співробітником важливих файлів не за тією адресою.

2. Кібератаки. Включають в себе хакерські атаки, деніал-сервіс атаки (DDoS), віруси, черв'яки та інші форми віртуальних нападів на інформаційні системи. Перший шлях – це пряма атака на канал зв’язку. Другий – атака безпосередньо на сервер ресурсу. Зазвичай подібні атаки використовуються в ході конкурентної боротьби, шантажу компаній або для відвернення уваги системних адміністраторів від деяких протиправних дій.

3. Соціальний інжиніринг. Маніпулювання людьми з метою отримання конфіденційної інформації, таке як паролі або інші ключові дані. Може включати в себе різноманітні методи та техніки, які сприймають довіру людей та намагаються отримати від них інформацію.

4. Комп’ютерні віруси. Одна з найнебезпечніших на сьогоднішній день загроз інформаційній безпеці. Це можна пояснити появою нових каналів проникнення вірусів. На першому місці як і раніше залишається електронна пошта, але, як показує практика, віруси здатні проникати і через програми обміну повідомленнями. Збільшилася і кількість об’єктів для можливих вірусних атак. Якщо раніше атакам піддавалися в основному сервери стандартних вебслужб, то сьогодні віруси здатні впливати і на міжмережеві екрани, комутатори, мобільні пристрої, маршрутизатори. Останнім часом особливо активні стали так звані віруси-шифрувальники.

5. Технічні проблеми. Системні відмови. Несправність обладнання або програмного забезпечення, що може призвести до втрати доступу до інфор-

мації. Помилки в програмному забезпеченні. Недоліки в програмах, які можуть бути використані для незаконного доступу.

6. Законодавство. Державні органи наділені правом конфіскувати в ході перевірок обладнання та носії інформації, що завдає збитків компанії.[1]

Система інформаційної безпеки повинна враховувати ці всі різноманітні загрози. Тож до методів захисту інформації слід віднести:

фізична безпека(обмеження або повну заборону доступу сторонніх осіб на територію), захист фізичного доступу до серверних приміщень, обладнання та інших інфраструктурних елементів;

захист від вірусів та шкідливих програм, використання антивірусного програмного забезпечення для виявлення та видалення шкідливих програм, які можуть завдати шкоди системі та інформації, базові засоби захисту електронної інформації (численні антивірусні програми, а також системи фільтрації електронної пошти);

захист від DDoS-атак, використання засобів та сервісів, які можуть виявляти та захищати від атак типу "Denial of Service" (DDoS), спрямованих на переповнення мережі запитами, використання анти-DDoS (послугу анти-DDoS, пропоновані програмістами);

резервне копіювання даних, регулярне створення резервних копій важливої інформації для запобігання втрати даних у випадку випадкового видалення, атак або технічних проблем(особливо актуальною стала послуга віддаленого зберігання різної інформації в “хмарі” дата-центрів);

шифрування даних, використання шифрування для захисту конфіденційної інформації від несанкціонованого доступу. Цей процес забезпечує перетворення чи часткове приховання інформації так, щоб тільки ті, хто має право, могли її розшифрувати;

аутентифікація та авторизація, встановлення систем аутентифікації для впізнавання користувачів та гарантування їхньої ідентичності перед отриманням доступу до системи. Після аутентифікації користувачам призначаються відповідні права доступу (авторизація);

захист від соціального інжинірингу, навчання персоналу та регулярне підвищення рівня свідомості щодо методів соціального інжинірингу;

визначення життєвого циклу інформаційної безпеки підприємства, дослідження основних рівнів інформаційної безпеки підприємства є також важливими аспектами її забезпечення в сучасних умовах.

Список використаних джерел:

1. Поширені загрози інформаційній безпеці URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-information-security-infosec#common-infosec-threats

2. Технології для інформаційної безпеки URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-information-security-infosec#technologies-used-for-InfoSec

Ключові слова: внутрішні загрози, кібератаки, соціальний інжиніринг, комп'ютерні віруси, технічні проблеми, законодавство.
Keywords: internal threats, cyberattacks, social engineering, computer viruses, technical problems, legislation.

Науковий керівник: к.ф.-м.н., доцент Чепурна О.Є.

ВИКОРИСТАННЯ БІБЛІОТЕКИ SCAPY ДЛЯ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

Дрига Артем
студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Аналіз мережевого трафіку є дуже важливою складовою забезпечення кібербезпеки будь-якої організації. Він дозволяє знаходити підозрілі аномалії або інші сліди незвичайної активності, наприклад сигнатури шкідливого програмного забезпечення.

Однак, у роботі з такою інформацією існує кілька проблем. Одна з головних - ефективна обробка масивів інформації, що збирається. Мережевий трафік, що проходить навіть через один мережевий інтерфейс, може займати дуже великий обсяг, більша частина якого зазвичай не цікавить аналіз інцидентів безпеки.

Для аналізу мережевого трафіку існує велика кількість інструментів. Одними з найпоширеніших є Wireshark, який має зручний графічний інтерфейс, та tcpdump, який працює в консольному режимі. Ці інструменти використовують ефективні механізми BPF (Berkeley Packet Filters), що склалися з практикою, точніше їх покращену версію eBPF (extended Berkeley Packet Filter) для управління збиранням та фільтрацією трафіку [1].

Для роботи з eBPF обидва проекти спираються на використання бібліотеки libpcap, що розробляється спільно з проектом tcpdump [2].

Крім використання eBPF, характерною особливістю цієї бібліотеки є використання відкритого формату файлів pcap (PCAP Capture File Format) та pcapng (PCAP Next Generation Capture File Format) [3]. Ці формати є особливим чином організованими файлами, що добре підходять під збір та аналіз пакетів мережевого трафіку.

Хоча ці інструменти і ефективні, але іноді не всього їхнього функціоналу вистачає, або ж великий об'єм трафіку зробить недоцільним їхнє викори-

стання. Існує великий клас завдань, у якому аналіз трафіку (перехоплюваного в режимі реального часу чи у вигляді зібраних для аналізу архівів) перестає бути оптимальним і потребує великих витрат часу. У цьому випадку доцільно використовувати програмні скрипти та здійснювати таку обробку автоматично.

Одним із зручних для таких завдань інструментів є бібліотека Scapy, яка дає змогу маніпулювати мережевими пакетами [4]. Наведемо приклад простої програми, написаної за допомогою Scapy. Ця програма буде перехвачувати мережеві пакети та виводити їх в консоль:

```
from scapy.all import sniff
def packet_output(packet):
print(packet.show())
 def main():
sniff(prn=packet_output, count=10)
 if __name__ == '__main__':
main()
```

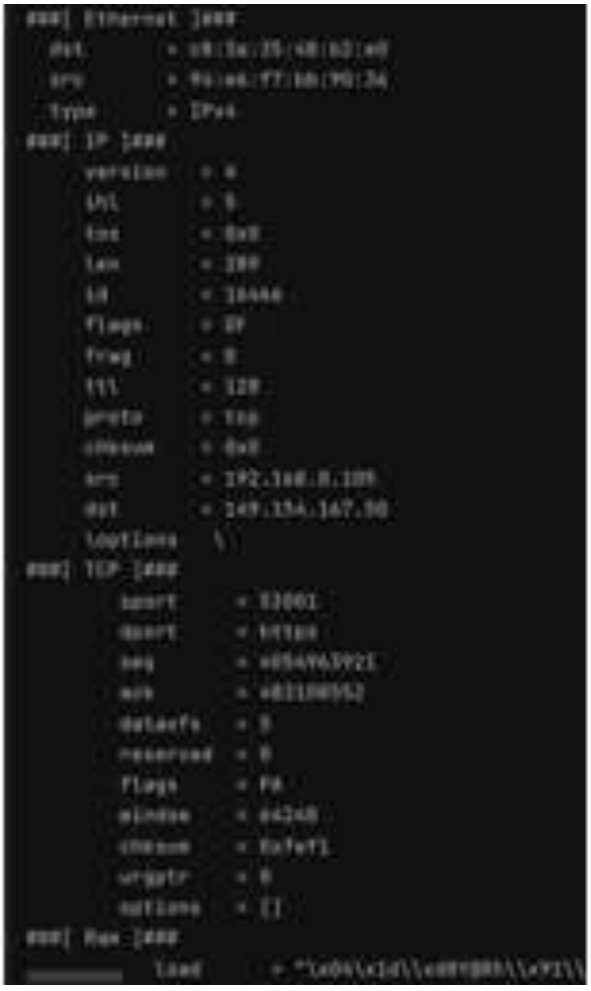


Рис. 1: Результат виконання програми

Як видно, програма зовсім не складна та при цьому виводить досить детальну інформацію про пакет, який змогла перехватити. При цьому до цієї

програми можна добавляти ще багато функцій, наприклад фільтрацію пакетів за певним протоколом.

Однією із сильних сторін бібліотеки є можливість використання синтаксису eBPF, що також використовується у Wireshark та tcpdump [2]. Наприклад, удосконалимо функцію sniff() для перехоплення пакетів тільки по протоколах електронної пошти, таких як SMTP (25 порт), POP3 (110 порт) та IMAP (143 порт):

```
sniff(filter='tcp port 25 or tcp port 110 or tcp port 143', prn=packet_output, count=10)
```

Тепер будуть перехоплюватись тільки ті пакети, що пов'язані з електронною поштою.

Це всього лише невелика демонстрація того, на що здатна бібліотека Scapy, наприклад з її допомогою також можна як захищатися від атак, так і проводити їх. У будь-якому разі написання власних програм для аналізу мережевого трафіку не тільки покращує знання про протоколи, а й може стати в пригоді в той момент, коли інші інструменти будуть безсилі.

Список використаних джерел:

1. BPF and tcpdump [Електронний ресурс]. – Режим доступу: https://andreaskaris.github.io/blog/networking/bpf-and-tcpdump/
2. Home | TCPDUMP & LIBPCAP [Електронний ресурс]. – Режим доступу: https://www.tcpdump.org/
3. LibpcapFileFormat [Електронний ресурс]. – Режим доступу: https://wiki.wireshark.org/Development/LibpcapFileFormat
4. Scapy: the Python-based interactive packet manipulation program and library [Електронний ресурс]. – Режим доступу: https://github.com/secdev/scapy

Ключові слова: Scapy, аналіз мережі, фільтрація
Keywords: Scapy. network analysis, filtering

Науковий керівник: к.т.н., доцент Бойко В.Д.

Секція 2. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В УМОВАХ ВІЙНИ

АНАЛІЗ ПОТЕНЦІЙНИХ ВИТОКІВ ДАННИХ В ПРИСТРОЯХ КОМУНІКАЦІЇ

Задерейко Олександр

доцент кафедри інформаційних технологій, факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Логінова Наталія

завідувач кафедри інформаційних технологій, факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», кандидат педагогічних наук, доцент

Троянський Олександр

директор інституту інформаційної безпеки, радіоелектроніки та телекомунікацій Національного університету «Одеська політехніка», кандидат технічних наук, доцент

Переважна більшість користувачів не можуть відмовитися від використання засобів комунікації інтегрованих в глобальну мережу Інтернет. Внаслідок цього, повністю виключити витоки конфіденційних даних користувачів не є можливим. Найбільш поширеним способом запобігання витоків конфіденційних даних користувачів є різні способи моніторингу і подальшого контролю мережевого трафіку пристроїв комунікації.

Тому актуальним завданням є виявлення ймовірних витоків конфіденційних даних, заснованих на методиках (алгоритмах) їх виявлення і подальшого блокування. Рішення цього завдання може бути реалізовано з використанням моніторингу всього мережевого трафіку пристроїв комунікації користувачів і подальшому виявленні в ньому даних, які можна віднести до конфіденційних (або надлишкових) і даних, що передаються в незашифрованому вигляді [1].

На практиці організація моніторингу мережевого трафіку пристроїв комунікації може бути виконана з використанням спеціалізованого програмного забезпечення – сніферів [2]. Реалізація такого підходу дозволяє виконувати детальний аналіз протоколів мережевого трафіку (на рівні пакетів) пристроїв комунікації на предмет наявності з'єднань, які можуть призвести до потенційних витоків даних, керуючись нижче наведеною методикою (рис. 1).

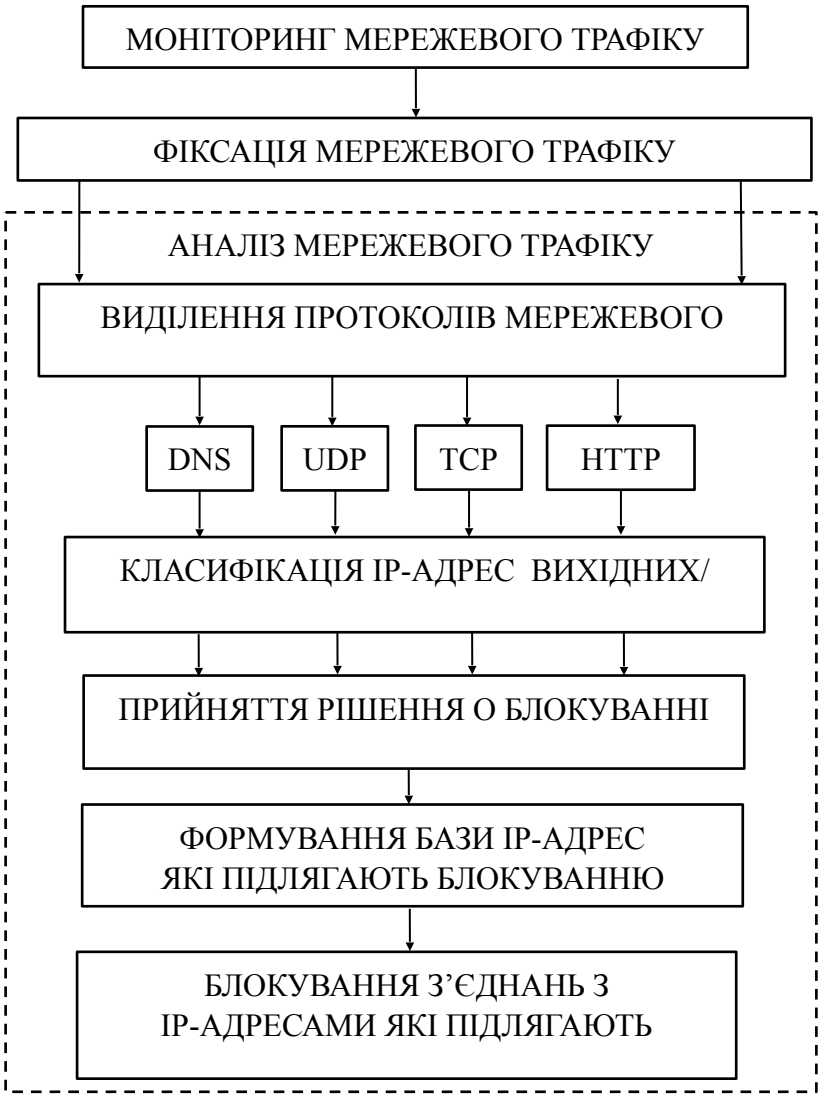


Рис. 1. Методика захисту пристроїв комунікації від потенційних витоків конфіденційних даних.

Завдання аналізу і класифікації трафіку, який може бути віднесений до конфіденційних даних з пристрою комунікації слід вирішувати, ґрунтуючись на таких критеріях [3]:

1. Заборону вихідних/вхідних з'єднань з сервісами інтернет статистики [4];

2. Заборону незахищених вихідних/вхідних з'єднань системного і прикладного програмного забезпечення, що здійснюються через всі порти, крім 443 (з обов'язковою перевіркою збереження його функціональності, після блокування);

3. Заборону вихідних/вхідних з'єднань необхідно виконувати на (L4) і (L7) рівнях моделі OSI (табл. 1) [5].

Таблиця 1. Модель OSI з розкладкою протоколів за рівнями

Рівень (L)	Назва	Протоколи
1	Application	SSH, HTTP, FTP, LPD, SMTP, TELNET, TFTP, EDI, POP3, IMAP, SNMP, NNTP, S-RPC, SET
2	Presentation	Encryption protocol types and format, such as ASCII, EBCDICM, TIFF, JPEG, MPEG, MIDI
3	Session	SMB, RPC, NFS, SQL
4	Transport	SPX, SSL, TLS, TCP, UDP
5	Network	ICMP, RIP, OSPF, BGP, IGMP, IP, IPSec, IPX, NAT, SKIP
6	Data link	ARP, SLIP, PPP, L2F, L2TP, PPTP, FDDI, ISDN
7	Physical	EIA/TIA-232, EIA/TIA-449, X. 21, HSSI, SONET, V. 2.4, V. 35, BLUETOOTH, 802.11, ETHERNET

Практична реалізація заборони вихідних/вхідних з'єднань повинна бути здійснена з використанням стандартних міжмережевих екранів і/або міжмережевих екранів нового покоління класу NGFW[1] [6]. Такі міжмережеві екрани, дозволяють здійснювати глибоку фільтрацію трафіку, засновану на роботі засобів аналізу на рівні додатків (L7), таким чином, що "вміст" кожного пакета аналізується, починаючи від рівня L3 та закінчуючи рівнем L7 моделі OSI, у тому числі пакети, що містять зашифрований SSL(TLS) трафік.

Висновки

Апробація запропонованого підходу заснованого на аналізі мережевого трафіку на різних стаціонарних і мобільних пристроях комунікації дозволила ефективно виявляти і блокувати збір конфіденційних даних користувачів, що дозволило знизити ймовірність витоку їх конфіденційних даних.

Список використаних джерел:

1. ACSAC '10: Proceedings of the 26th Annual Computer Security Applications Conference. December 2010. Pages 261–269. DOI: https://doi.org/10.1145/1920261.1920300.
2. Pughazhendhi K. Amutha N. Packet sniffer. URL: https://www.irjmets.com/uploadedfiles/paper/issue_3_march_2023/35048/final/fin_irjmets1680097820.pdf/. (Дата звернення 6.11.2023).
3. Задерейко О.В., Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Кухаренко С.В. Аналіз витоків даних у інформаційних системах. Сучасна спеціальна техніка. № 3 (66), 2021, С. 16-30. URL: http://dspace.onua.edu.ua/handle/11300/23298.

4. Zadereyko O., Trofymenko O., Prokop Y., Loginova N., Dyka A., Kukharenko S. Research of potential data leaks in information and communication systems. Radioelectronic and Computer Systems. 2022. No 4. P.64-84. DOI: https://doi.org/10.32620/reks.2022.4.05. URL: https://dspace.onua.edu.ua/bitstream/handle/11300/23361/doslidjena_potenciynuh_vutokiv_danuh.pdf.
5. Задерейко О.В., Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Кухаренко С.В. Дика А.І. Захист даних користувачів в інформаційних системах. Сучасна спеціальна техніка. № 1 (68), 2022, С. 23-33. URL: https://hdl.handle.net/11300/23313.
6. Know, what you need to. "Defining the Next-Generation Firewall." (2009). URL: https://media.paloaltonetworks.com/documents/Gartner-NGFW-Research-Note.pdf. (Дата звернення 6.11.2023).

Ключові слова: пристрої комунікації, аналіз протоколів мережевого трафіку, аналіз пакетів мережевого трафіку, аналіз витоків даних, конфіденційні дані користувачів, моніторинг мережевого трафіку, міжмережевий екран, міжмережевий екран NGFW, глибока фільтрація трафіку, база конфіденційних даних, база IP адрес, блокування з'єднань
Keywords: communication devices, network traffic protocol analysis, network traffic packet analysis, data leak analysis, confidential user data, network traffic monitoring, firewall, NGFW firewall, deep traffic filtering, confidential data database, IP address database, connection blocking

СУЧАСНІ ІНСТРУМЕНТИ UI/UX ДИЗАЙНУ

Манаков Сергій

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

UI/UX дизайн це дисципліна яка вивчає шляхи та способи створення орієнтованих на користувача інтерфейсів програмних продуктів. Основною характеристикою дизайну є юзабіліті, що визначає міру зручності використання продукту та його ефективності при досягненні користувачем певної мети. Згідно стандарту ISO 9241-210 [1] юзабіліті сайту або програми можна оцінити відповідно до кількості кліків та часу, що витрачається на вирішення завдання.

Невід'ємною етапом при розробці дизайну є вибір та використання відповідних програмних інструментів, таких як: Figma [2], Adobe XD, Axure RP чи інших.

Вони дозволяють створювати прототипи, що імітують зовнішній вигляд та логіку роботи кінцевого продукту ще до початку розробки. Етап створення прототипів допомагає уникнути серйозних помилок, які виправити після релізу буде дуже дорого, а іноді і неможливо.

Технічно прототип виглядає як система сторінок чи екранів, з'єднаних загальною логікою та дизайном.

Щоб створити прототип, спочатку потрібно зробити вайрфрейми (монохромні ескізи сторінок) або зображення екранів. Перший тип сторінок можна зібрати в прототип низької точності, другий – в прототип високої точності.

Прототипи низької точності (lo-fi) показують основну функціональність сторінок та екранів, їх структуру та зв'язок. Але презентувати їх клієнтам або проводити користувацьке тестування не доцільно – не всі користувачі зможуть зрозуміти, що перед ними лише прототип, а не готовий продукт.

У високоточних прототипах (hi-fi) можна перевірити окремі компоненти та елементи дизайну. Рівень опрацювання вибирається в залежності від етапу розробки. Користувачеві важливо побачити саме логіку роботи дизайну.

Якщо ж продукт досить складний, складається з безлічі різних екранів і передбачає незвичайну взаємодію, варто створити інтерактивний прототип низького або високого рівня. З його допомогою можна виявити деякі особливі вимоги до контенту, дизайну, сценаріїв та аспектів розробки.

Бурхливий розвиток технологій генеративного штучного інтелекту (ШІ) надає нові можливості для розробки UI/UX дизайну. За останній рік з’явилася низка загальнодоступних нейронних мереж, які створюють текстовий, графічний, аудіо- та відеоконтент за текстовим запитом користувача. Багато дизайнерів вже успішно використовують ці технології на практиці. При чому, вони не замінюють самих дизайнерів, а навпаки – розширюють їхні можливості.

З іншого боку, використання ШІ полегшує налаштування й оптимізацію взаємодії з користувачем. Для цього використовуються боти, помічники та інші доопрацювання. Завдяки ШІ можна розуміти запити клієнтів, надаючи унікальні відповіді за допомогою обробки мови та машинного навчання. Такий підхід допоможе збільшити залучення людей за рахунок зменшення зусиль підтримки.

Інтелектуальну аналітику можна використовувати для розробки персоналізованих меню, пропозицій, які досліджують дані користувача та проводять поведінкові прогнози. В результаті ШІ робить UX більш доступним, потенціал цього напрямку дуже великий і підходить для реалізації різними способами.

Також, активно впроваджуються технології генерації програмного коду компонентів користувацького інтерфейсу на основі створеного прототипу. Так, плагін Anima [3] для Figma дозволяє отримати код компонентів React для створеного дизайну, що дозволяє значно скоротити час реалізації прототипу. Інші рішення створюють прототипи зі скріншотів чи намальованих на папері вайрфреймів. Отже, сучасні інструменти дизайну скорочують розрив між дизайнерами, розробниками та менеджерами з продуктів.

Оскільки UI/UX дизайн – це дисципліна, що постійно розвивається, дизайнери повинні бути готові адаптуватися до нових технологій і тенденцій.

Програми для інтерактивного прототипування зробили революцію у дизайні. Вони надали дизайнерам можливість створювати прототипи, які імітують взаємодію з користувачем у різних ситуаціях та на різних носіях. Використовуючи ці функції у поєднанні з сучасними технологіями штучного інтелекту, можна значно оптимізувати дизайн-процес, підвищити ефективність команди розробки та, зрештою, підвищити юзабіліті майбутнього продукту.

Список використаних джерел:

1. Стандарт ISO 9241-210. URL: https://www.iso.org/standard/77520.html
2. Figma. URL: https://www.figma.com/
3. Anima. URL: https://www.animaapp.com/

Ключові слова: UI/UX дизайн, юзабіліті, інтерактивне прототипування, Figma, штучний інтелект.
Keywords: UI/UX design, usability, interactive prototyping, Figma, artificial intelligence.

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ У СИСТЕМАХ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Грезіна Олена

студентка 1-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Біометричні технології у системах аудиту інформаційної безпеки на сучасному етапі визначають актуальний напрямок розвитку в області кібербезпеки. Захист конфіденційності та доступності даних стає все більш важливим, особливо в умовах постійної еволюції кіберзагроз. Використання біометричних технологій дозволяє індивідуалізувати безпекові підходи, уникнути втрати ідентифікаторів та паролів, а також враховувати унікальні фізичні характеристики кожного користувача. З високою загрозою кіберзлочинності та імперативом кібербезпеки, впровадження біометричних технологій стає невід'ємною частиною стратегії захисту від сучасних загроз. Розвиток мультимодальних рішень у біометричних технологіях вказує на постійне вдосконалення систем ідентифікації та автентифікації для забезпечення ще більшої точності та безпеки в області інформаційної безпеки. Такий інноваційний під-

хід відповідає викликам сучасного цифрового середовища та забезпечує високий рівень кібербезпеки в умовах постійної динаміки кіберзагроз.

Дослідженням цього питання займались такі науковці, як А.О. Мороз, В.М. Лукашенко, Т.Ю. Уткіна, О.С. Вербицький та інші.

Мороз А.О. зазначає, що: «…біометричні технології дозволяють проводити face-контроль в автоматичному режимі, вони звіряють параметри обличчя об'єкта, який зафіксований камерою, з даними в базі. І достовірність такого аналізу складає 86–93%. Це значно більше за звичайні людські можливості. Проте проблема полягає в тому, що для здійснення цієї функції необхідне устаткування високої якості» [1, с. 41].

В контексті аудиту безпеки даних, біометричні технології, які здійснюють face-контроль в автоматичному режимі, представляють важливий елемент системи безпеки. Вони використовуються для автоматичної ідентифікації осіб за допомогою звірення параметрів обличчя об'єкта, зафіксованого камерою, з даними в базі. Однак важливо взяти до уваги, що для ефективності цих технологій необхідне використання високоякісного обладнання. Аудит безпеки даних включає оцінку якості та надійності використовуваного обладнання для біометричного аналізу, а також перевірку відповідності процесів збору та збереження біометричних даних вимогам стандартів безпеки. Даний аспект важливий забезпечення конфіденційності та непорушності особистих даних, який стає об'єктом уваги при проведенні аудитів безпеки даних в організаціях, що використовують біометричні рішення.

Зазначимо, що аудит безпеки даних в контексті біометричних технологій визначає ключові завдання, такі як біометрична верифікація та ідентифікація особистості, а також забезпечення безпечної біометричної автентифікації. Вказані завдання стають невід'ємною частиною важливих додатків та систем захисту, особливо в контексті розширення використання біометричних даних в інформаційних системах і процесах. Розвиток інфраструктури інтернету і хмарних технологій додає складності управлінню та захисту біометричних ідентифікаторів. Аудит безпеки даних у цьому контексті включає перевірку ефективності процесів верифікації та ідентифікації, а також забезпечення відповідності систем безпеки вимогам стандартів. Орієнтація на кінцевого користувача інтернет-сервісів і Web-додатків наголошує важливість надійності і безпеки біометричних систем для забезпечення захисту особистих даних та конфіденційності інформації.

Лукашенко В. М., Уткіна Т. Ю., Вербицький О. С. у своїх дослідженнях виокремлювали біометричну автентифікацію, як: «…процес доведення автентичності заявленого користувачем імені через надання ним свого біометричного образу. Біометричними характеристиками людини є відбитки паль-

ців і долоні, звуки її голосу, вигляд обличчя, відбиток сітківки ока, особливості рухів і ходи, особливості роботи на клавіатурі, власний підпис [2].

Аудит в даному випадку визначає ефективність та надійність цих біометричних характеристик у процесі визначення особистості користувача. Важливим аспектом аудиту є також перевірка забезпечення конфіденційності та захисту біометричних даних під час їх збору, збереження і використання. Аудиторські заходи в цьому випадку спрямовані на забезпечення відповідності процесів біометричної автентифікації високим стандартам безпеки та захисту особистої інформації користувачів.

Біометричні технології є важливим напрямком розвитку в галузі кібербезпеки, забезпечуючи індивідуалізовані підходи та ефективні засоби захисту даних. Використання face-контролю та інших біометричних рішень в системах аудиту інформаційної безпеки дозволяє автоматизувати процеси ідентифікації та автентифікації з високою точністю. Проте, для забезпечення ефективності цих технологій, важливо враховувати високі стандарти обладнання та дотримання вимог безпеки під час обробки біометричних даних. Аудит безпеки даних грає важливу роль у визначенні ефективності та надійності цих процесів, забезпечуючи відповідність стандартам та захист особистих інформаційних ресурсів користувачів. Розвиток мультимодальних рішень у біометричних технологіях свідчить про постійне вдосконалення систем ідентифікації та автентифікації, забезпечуючи ще більшу точність та безпеку в області інформаційної безпеки. Даний інноваційний підхід відповідає викликам сучасного цифрового середовища та гарантує високий рівень кібербезпеки в умовах постійної динаміки кіберзагроз.

Список використаних джерел:

1. Мороз А.О. Біометричні технології ідентифікації людини. Огляд систем. Математичні машини і системи. 2011. № 1. С. 39-45.
2. Лукашенко В. М., Уткіна Т. Ю., Вербицький О. С. Системний аналіз біометричних датчиків відбитків пальця для системи управління доступом лазерного технологічного комплексу. Вісник ЧДТУ. 2012. № 4. С. 29–34.

Ключові слова: аудит безпеки даних, біометричні технології, біометрична автентифікація, інформаційна безпека, кібербезпека.
Keywords: data security audit, biometric technologies, biometric authentication, information security, cyber security.

Науковий керівник: к.т.н., доцент Кухаренко С.В.

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ В РІЗНИХ СФЕРАХ ДІЯЛЬНОСТІ

Задерейко Олександр

доцент кафедри інформаційних технологій факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Толокнов Анатолій

асистент кафедри інформаційних технологій факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Черненко Олександра

студентка 1 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

В умовах сьогодення технології віртуальної реальності користуються широким попитом в різних сферах людської діяльності, зокрема під час освітнього процесу, наукової та військової діяльності, дизайні, бізнесі та розвагах.

Різні аспекти віртуальної реальності досліджують у своїх наукових доробках такі вчені, як: Б. Вітковський, Ф. Власенко, Н. Голіонко, О. Гриб'юк, О. Данильян, О. Дзьобань, А. Островська, Т. Чоп та інші.

Традиційно у філософії віртуальну реальність розглядають як вид гносеологічної реальності, осмислення якої може ґрунтуватися на концепції симулякрів Ж. Бодрійяра — зображеннях, копіях того, чого насправді не існує, а у новій філософській енциклопедії – як «особливий тип взаємодії між різними об'єктами, а також специфічні між ними відносини породжуваності й інтерактивності [1, с. 209].

Аналіз наукової літератури дає можливість констатувати, що вчені тлумачать віртуальну реальність як:

- технологію повного занурення у штучно створене за допомогою комп'ютера віртуальне середовище [2, с. 135];
- результат взаємодії об'єктивного та суб'єктивного, якому властивий статус випадкового буття, яке не фіксоване, чи не вкорінене повністю у соціальному [3, с. 19];
- технологію безконтактної взаємодії, яка створює ілюзію безпосереднього занурення та присутності у віртуальному просторі реального часу [4, с. 37].

Водночас, Ф. Власенко стверджує, що віртуальна реальність характеризується, по-перше, технічним середовищем, яке створює "штучні світи", де

користувач занурюється у сконструйований комп'ютером віртуальний простір та взаємодіє з ним. По-друге, впливом на людську свідомість внаслідок використання електронних засобів комунікації з метою компенсації недоліків реального світу [1, с. 213].

Таким чином, віртуальна реальність тісно пов'язана з різними сферами діяльності, забезпечуючи взаємодію користувача з віртуальним простором, впливаючи на психіку людини, забезпечуючи особисті, освітні та соціальні потреби.

Б. Вітковський та Т. Чоп визначають такі типи віртуальної реальності:

- технології з ефектом повного занурення (віртуальний простір, що симулює певне середовище з високим ступенем деталізації);
- технології без занурення (віртуальний простір, що відтворює на широкоформатному екрані симуляції із зображенням, звуком та контролерами, однак не виконує вимог до VR-технологій у повному обсязі);
- технології віртуальної реальності зі спільною структурою (віртуальний простір, що забезпечує взаємодію з іншими користувачами і до якого відносять тривимірний віртуальний світ, наприклад, гру Minecraft) [2, с. 135].

Зазвичай, коли мова йде про віртуальну реальність, одразу виникають асоціації зі сферою розваг, зокрема комп'ютерними іграми різних жанрів та платформ.

Водночас варто зазначити, що останнім часом технології віртуальної реальності стають все більш поширеними у різних сферах професійної діяльності людини, а саме:

- у бізнесі: під час рекламування, продажу та бізнес-комунікацій власники нерухомості надають можливість переглянути квартиру в онлайн-режимі, онлайн-трансляції модних показів, спортивних і розважальних подій дозволяють стати реальним учасником певної події та відчути справжні емоції;

- в освітньому процесі: використання інтерактивних технологій під час навчання у тривимірному просторі, наприклад, під час вивчення Сонячної системи. Спільно з Google компанія Lenovo розробила понад 700 віртуальних екскурсій, що надають можливість перенестися в будь-яку точку Землі: від глибин світових океанів до найвідоміших музеїв Європи;

- у медичній діяльності: завдяки дослідженню, проведеному бельгійськими медиками, було з'ясовано, що віртуальні технології можна використовувати у хірургії як альтернативу седативних препаратів. Така методика отримала назву «віртуальний гіпноз». Її особливість полягає в тому, що під час операції на пацієнта одягаються навушники з VR-окулярами та вмикається заспокійливе відео про життя підводних тварин, трансляція якого супроводжується коментуванням приємного заспокійливого голосу;

- у машинобудуванні: компанія Ford Motor Company використовує VR-технології для проектування автомобілів, зокрема її дизайн-центр, що розташований в Кельні (Німеччина), має обладнану студію, в якій інженери-проектувальники можуть з усіх боків оцінити автомобіль, не маючи фізичного прототипу. Завдяки обладнанню в цій студії, яке підвищує ефективність та швидкість опрацювання моделей автомобілів та їх елементів обробки, дизайнери компанії змогли обрати найкраще розташування приладової панелі, механізмів управління та крісел для нової моделі Ford Fiesta;

- у нафтовидобуванні: демонстрація обладнання та самого процесу на виставках та переговорах з інвесторами та співробітниками великих комерційних організацій, які взаємодіють з державними структурами;

- у сфері продажів: компанія IKEA застосовує технології віртуальної реальності у своїх каталогах для продажу меблів, а саме: людина завантажує додаток, кладе каталог зі сторінкою обраного товару на місце, де бажає його розмістити, наводить камеру телефону на каталог і спостерігає, як будуть виглядати меблі у певному місці кімнати відповідно до своїх реальних розмірів та пропорцій [5];

- у військовій сфері: для підготовки військових фахівців доцільним буде проведення практики з використанням військового обладнання у віртуальному просторі, після чого здобуті знання та вміння закріплюватимуться на полігоні. Підготовка є більш ефективною й економною, оскільки на кожного бійця витрачаються значні обсяги різних боєприпасів для ведення бою з високою ефективністю. Таким чином, завдяки технологіям «занурення» зменшуються витрати на освітній процес та ризики військового досвіду.

- у будівництві: «ефект присутності» дозволяє архітектору творити модель своєї роботи у тривимірному просторі з метою дослідження сумісності певних матеріалів. Завдяки VR-окулярам є можливість побачити фінальний варіант роботи дизайнера інтер'єру або архітектора без потреби його будування, тим самим полегшуючи роботу.

- у дослідженні космосу: VR-технології дозволяють майбутнім космонавтам, знаходячись на Землі, зануритися в світ космосу й здобути практичні навички керування космічним шатлом. Завдяки навчанню у віртуальній реальності, космонавт зі значно меншою вірогідністю допуститься фатальної для спеціалістів помилки [6, с. 125].

- у туризмі: існують проекти віртуальних подорожей, які надають доступ до натурного перегляду експонатів та колекцій відомих світових музеїв та галерей. Завдяки відтворенню природних об'єктів, рекреаційних зон та території певного курорту, можна ознайомилися з умовами відпочинку, що допомагає планувати майбутню подорож. Нині в Інтернет постійно додаються різні віртуальні тури, прикладом яких може бути тур по вулицях Чорнобиля.

Сюди ж можна віднести розробку віртуальних туристичних маршрутів, зокрема перспективних, які включають в себе музеї, культурно-історичні об'єкти, архітектурні споруди та виставки, інтегровані у взаємопов'язану систему [7, с. 591].

- у сценічному мистецтві: VR-технології стали середовищем, в якому програмісти, сценографи та режисери можуть експериментувати з візуальними образами з метою створення для глядачів ілюзії занурення у саму виставу. Ідею віртуальних вистав з ентузіазмом сприймають на таких відомих культурних заходах як Венеціанська бієнале та Каннський фестиваль. Яскравим прикладом також є присвячені 20-річчю компанії «Київстар» віртуальний тур містами України та VR-спектакль «Вартові Мрій» – панорамне відео (360°) тривалістю 7 хвилин, яке знайомить з сюжетом відомої зимової казки [8, с. 63].

- у сільському господарстві: доволі успішним є проект «Plant Vision» – система управління, в якій повністю цифровізується рослинництво. Проект характеризується встановленими інфрачервоними камерами та датчиками, які збирають дані про об'єкт, щохвилинним фотографуванням посівів та перевіркою стану об'єктів за допомогою сканування. Іншим прикладом є система «Isabel» – розроблений в Сан-Франциско мобільний додаток, який керує гідропонною фермою площею 177 гектар та в якому згодом стало можливим повноцінно керувати теплицею. У системі наявні відеоінструкції, таймінги, автоматичний полив та внесення добрив [9, с. 255].

Отже, підсумовуючи погляди вчених, зазначимо, що технології віртуальної реальності використовуються не лише як спосіб розважального проведення вільного часу з метою задоволення особистих потреб, розвитку пізнавальних процесів, здатностей та здібностей особистості, а й як інструмент для впливу на психічний стан людини, наочної дистанційної презентації та практичної демонстрації об'єктів, керування та спостереження за ними, трансляції далеких від людини подій та місць, планування подорожей та підготовки майбутніх фахівців.

Список використаних джерел:

1. Власенко Ф. П. Віртуальна реальність як простір соціалізації індивіда / Ф. П. Власенко // Гуманітарний вісник Запорізької державної інженерної академії. – 2014. – Вип. 56. – С. 208-217. URL: https://old-zdia.znu.edu.ua/gazeta/znpgvzdia_2014_56_24.pdf.
2. Вітковський Б. Віртуальна реальність та нове освітнє середовище / Б. Вітковський, Т. Чоп // Збірник тез II Міжнародної наукової конференції молодих учених та студентів „Філософські виміри техніки", 4-5 грудня 2019 року. – Т.: ТНТУ, 2019. – С. 135–136. — (Основні засади формування професійної компетентності у вищій школі). URL: https://core.ac.uk/download/pdf/286540543.pdf.

3. Данильян О. Віртуальна реальність і кіберпростір як атрибути сучасного суспільства. / О. Данильян, О. Дзьобань // Інформація і право. – К., КНУКіМ, 2020. – В. 4. – С. 9-21. URL: https://ippi.org.ua/sites/default/files/3_17.pdf.
4. Волинець В. О. Віртуальна реальність: поняття та сутність / В. О. Волинець // Питання культурології. – 2014. – Вип. 30. – С. 35–41. URL: http://nbuv.gov.ua/UJRN/Pkl_2014_30_6.
5. Голіонко Н. Г. Віртуальні технології як передумова розвитку конкурентоспроможності підприємства / Н. Г. Голіонко, А. М. Островська // Ефективна економіка. – К., КНЕУ імені Вадима Гетьмана, 2020. – № 1. URL: http://www.economy.nayka.com.ua/pdf/1_2020/71.pdf.
6. Лі Н. Д. Використання VR-технологій під час підготовки фахівців / Н. Д. Лі. – Х.: ХНУР. – С. 124-125. URL: https://openarchive.nure.ua/server/api/core/bitstreams/ffccbf53-266e-4dce-a49d-e83b63091937/content.
7. Риднюк О. С. Роль сучасних віртуальних технологій в освіті і туризмі / О. С. Риднюк // Збірник тез І Міжнародної науково-практичної інтернет-конференції „Інтеграція освіти, науки та бізнесу в сучасному середовищі: літні диспути“, 1-2 серпня 2019 року. – Д.: ПНПУ імені В. Г. Короленка., 2019. – 874 с. URL: http://dspace.puet.edu.ua/bitstream/123456789/7082/1/Збірник%201%20міжнародна%20наук-практ%20інт%20конф%20Summer%20Debates.pdf#page=590.
8. Юдова-Романова К. Режисерські інновації у використанні технічних засобів і технологій у сценічному мистецтві / К. Юдова-Романова, В. Стрельчук, Ю. Чубукова // Вісник Київського національного університету культури і мистецтв. – 2019. – В. 2(1). – С. 52-72. – (Серія: Сценічне мистецтво). URL: http://artonscene.knukim.edu.ua/article/view/170749/172123.
9. Гарна У. Ю. Розвиток VR-технологій в сільському господарстві / У. Ю. Гарна, В. С. Шаповал, П. Г. Перерва // Всеукраїнська науково-практична інтернет-конференція «Урожайність та якість продукції рослинництва за сучасних технологій вирощування», присвячена пам’яті професора Г. П. Жемели, 30 вересня 2022 року. – Х.: НТУ «ХПІ», 2022. – С. 253-256. – URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/93829c2e-7ff2-4714-a56b-26c1e1498235/content.

Ключові слова: віртуальна реальність, application of virtual reality, VR-технології.
Keywords: virtual reality, areas of human activity, VR-technology.

GEOINT: МОЖЛИВОСТІ ГЕОПРОСТОРОВОЇ РОЗВІДКИ

Задерейко Олександр

доцент кафедри інформаційних технологій факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Долінко Ксенія

студентка 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Згідно з визначенням, наведеним у довіднику з розвідки з відкритих джерел NATO Open Source Intelligence, або OSINT, — це несекретна неупереджена інформація, яка була навмисно виявлена, структурована та поширена серед обраної аудиторії з метою вирішення окремого питання [1]. Збір такої інформації є легальним, а напрямки пошуку фактично необмеженими, завдяки чому OSINT, отримав застосування у багатьох галузях. У процесі розвитку деякі способи збору інформації цієї методики отримали достатньо широке розповсюдження і сформували окремі напрямки. Одним з таких є геопросторова розвідка, або GEOINT [2].

Завданням геопросторової розвідки є отримання інформації, а також її оцінка та візуалізація, щодо певних фізичних характеристик та географічно локалізованих процесів з використанням фотографічних зображень або відео- та геопросторових даних. Найчастіше отримана таким чином інформація використовується у журналістиці для підтвердження або спростування певних фактів, та під час бойових дій як спосіб розвідки [3].

Найпростіший спосіб аналізу фото- або відеофайлів – це дослідження метаданих, тобто даних, що містять додаткову інформацію про об’єкт, у структурі якого вони зашифровані. Метадані можуть містити ім’я, розмір, тип, дату створення та редагування файлу, ім’я автора, службову інформацію що стосується цифрового оптичного пристрою, з якого було зроблено фото- або відеоконтент, назву програмного забезпечення яким воно було створено, оброблено або відредаговано, тощо. Найчастіше використовуються три типи метаданих: EXIF, IPTC, Adobe XMP [4].

У глобальній мережі послуги отримання метаданих з фото- та відеофайлів пропонують багато онлайн-сервісів, проте такий спосіб їх аналізу не є надійним – більшість великих соціальних мереж, наприклад, автоматично видаляють метадані завантажених медіа файлів (рис. 1).

file_name	IMG_20230919_180810.jpg
file_size	2.9 MB
file_type	JPEG
file_type_extension	jpg
mime_type	image/jpeg
exif_byte_order	Big endian (Motorola, MM)
model	Redmi Note 8T
software	willow-user 11 RKQ1.201004.002 V12.5.6.0.RCKMIXM release-keys
orientation	Rotate 90 CW
modify_date	2023:09:19 18:08:12
y_cb_cr_positioning	Centered

а)

file_name	photo_2023-09-24_12-19-58.jpg
file_size	181 kB
file_type	JPEG
file_type_extension	jpg
mime_type	image/jpeg
jfif_version	1.01
resolution_unit	inches
x_resolution	72
y_resolution	72
profile_cmm_type	
profile_version	2.1.0

б)

Рис. 1. Порівняння за допомогою онлайн-сервісу Metadata2go [5] метаданих одного й того самого фото: а) надісланого через поштову службу Gmail; б) надісланого через месенджер Telegram.

Якщо метадані відсутні або недостатньо інформативні, застосовують метод GEOINT, що полягає в аналізі вмісту файлу зображення або відеозапису та їх контексту для того, щоб зрозуміти, де вони були зроблені. Інструментарій для цього методу є набагато ширшим та різноманітнішим [5].

У простих випадках буває достатньо завантажити файл у будь-який онлайн-сервіс для пошуку фотографічних зображень (Google Images [6], Duplichecker [7], тощо) – потрібну інформацію можна отримати за контекстом веб-сторінок, на яких будуть знайдені схожі зображення. Однак, частіше метод GEOINT стикається саме з фотографічними зображеннями, знайти які на просторах інтернету важко: локальні, непримітні території, незручний кут огляду, погана якість, тощо. На цьому етапі головним інструментом для пошуку стають віртуальні мапи (рис. 2).

а) б)

в)

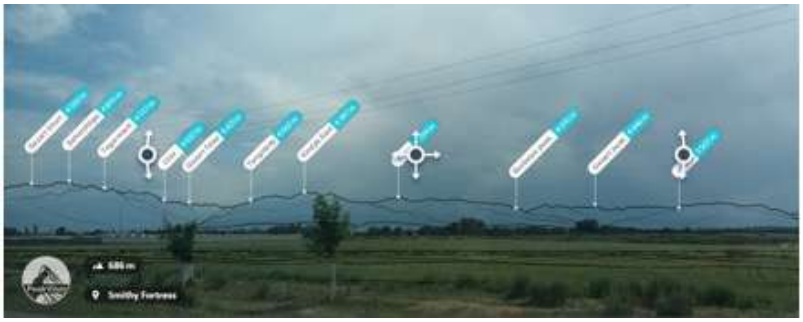
г)

Рис. 2. Зображення локації Старобазарного скверу, отримані за допомогою віртуальних мап: а) F4map [8]; б) Google earth [9]; в) Google maps [10]; г) MapChannels [11].

Вони пропонують зручний функціонал для вільного мандрування у просторі, 3D візуалізацію реальних об'єктів, можливість змінювати кут огляду, знаходити на мапі усі місця, що відповідатимуть заданим критеріям або матимуть заданий набір об'єктів, та багато іншого.

Однак, для ефективного використання мап потрібно мати певний набір готових орієнтирів або приблизне розуміння області пошуку, для чого першочергово потрібно проаналізувати вміст фото- або відеоконтенту. Відправними точками початку пошуку можуть стати будь-які об'єкти на фотографічному зображенні: наприклад, рельєф місцевості. За допомогою низки застосунків та онлайн-сервісів (PeakFinder [12], PeakVisor [13], Peakery [14]) так, наприклад, на фотографічному зображенні гірського масиву з певною ймовірністю можна визначити, що саме за гори зображені і де вони знаходяться (рис. 3).

а)



б)

Рис.3. Визначення гірського рельєфу на фото за допомогою застосунку PeakVisor: а) вихідне фото; б) та отриманий результат.

Якщо певний об'єкт на фотографічному зображенні відкидає тінь, користуючись відповідними інструментами генерації тіней (онлайн-сервісу Shademap.app [15] або Sunpath3d [16]) можна визначити час, коли було зроблено фотографічне зображення (рис. 4).

Рис. 4. Зображення розташування тіней від об'єктів у Старобазарному сквері о 17:00, отримане за допомогою онлайн-сервісу Shademap.app

Якщо на фотографічному зображенні присутня рослинність, деякі вузькоспеціалізовані сервіси, як, наприклад, plant.id [17] здатні її розпізнати та надати інформацію про місця, де вона поширена (рис. 5).

а) б)

Рис. 5. Визначення виду гриба, зображеного на фотографічному зображенні, за допомогою онлайн-сервісу Plant.id: а) ймовірні види грибів, визначені онлайн-сервісом б) надана онлайн-сервісом інформація щодо обраного виду гриба.

Окрім вищезгаданих, важливими GEOINT-інструментами є звичайні логіка та уважність їх користувачів. Деякі орієнтири залишаються непомітними для онлайн-сервісів але все ще можуть нести важливу інформацію про місцевість. Наприклад, якщо на фотографічному зображенні присутня дорога,

варто звернути увагу на напрям руху: право- чи лівосторонній він, тому що це може суттєво звузити область пошуку. Номері знаки автомобілів, дорожні знаки та дорожня розмітка, банери, логотипи, реклама та вивіски магазинів - все це може вказувати на країну та регіон походження.

Загалом, методологію вирішення GEOINT-задачі можна звести до наступного алгоритму: пошук метаданих, робота із контекстом та вмістом фотографічного зображення, пошук актуальних мап, аналіз об'єктів на фотографічному зображенні, звуження пошуку до країни/регіону/вулиці, визначення локації та верифікування. Саме верифікуванням, тобто наданням доказів того, що знайдена локація відповідає розшукованій, досягаються цілі, поставлені у геопросторовій розвідці.

Список використаних джерел:

1. NATO Open Source Intelligence Handbook. URL: https://github.com/lawsecnet/OPSEC/blob/master/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf
2. Подліпаєв, В. О. "Геопросторова розвідка, як шлях реалізації геоінформаційного підходу у комплексній обробці розвідувальної інформації." Системи обробки інформації 5 (2013): 53-55.
3. Кухарський, І. А., et al. "Визначання та основні поняття геопросторової розвідки." Системи обробки інформації 6 (2013): 96-98.
4. Zadereyko A. The Implementation of depersonalization algorithm of digital images / A. Zadereyko, N. Loginova, A. Troyanskiy, E. Trofimenko // Proceedings of 2nd International Conference on Advanced Information and Communication Technologies-2017 (AICT-2017) (Lviv, Ukraine, July 4-7, 2017). – P. 56-61. URL: http://dspace.onua.edu.ua/handle/11300/9666.
5. Metadata2go - https://www.metadata2go.com/
6. Google Images - https://images.google.com/
7. Duplichecker - https://www.duplichecker.com/ru/reverse-image-search.php
8. F4map - https://www.f4map.com/
9. Google earth - https://earth.google.com/web/
10. Google maps - https://www.google.com/maps/
11. MapChannels - https://mc9.mapchannels.com/Demo
12. PeakFinder - https://www.peakfinder.com/
13. PeakVisor - https://peakvisor.com/
14. Peakery - https://peakery.com/
15. Shademap.app - https://shademap.app/
16. Sunpath3d - https://andrewmarsh.com/apps/staging/sunpath3d.html
17. Plant.id - https://plant.id/

Ключові слова: GEOINT-задачі, GEOINT-інструменти, геопросторова розвідка, метадані, віртуальні мапи, GEOINT, OSINT

Keywords: GEOINT, GEOINT tasks, GEOINT tools, geospatial intelligence, metadata, virtual maps, OSINT

ДОСЛІДЖЕННЯ ПОТУЖНОСТЕЙ МНОЖИН НЕЛІНІЙНИХ ПЕРЕТВОРЕНЬ ІЗ ЗАДАНИМИ ЗНАЧЕННЯМИ ПЕРІОДІВ ПОВЕРНЕННЯ У ВИХІДНИЙ СТАН

Баландіна Наталія

Старший викладач кафедри кібербезпеки Національного університету «Одеська юридична академія»

К. Шенноном у 1949 р. [1] було введено концепцію криптографічного S-блока, як основного компонента для побудови захищених шифрів. Роки дослідження криптографічних конструкцій та досвід їх практичного застосування підтвердив роль S-блоків, як основних компонентів, що визначають ефективність та швидкодію сучасних шифрів. У сьогоденні чітко визначений математичний апарат дослідження криптографічної якості S-блоків, що включає такі критерії, як нелінійність, критерій розповсюдження помилки та суворий лавинний критерій, критерій кореляційного імунітету та матриці коефіцієнтів кореляції, критерій максимізації періодів повернення у вихідний стан [2…4]. Запропоновано численні конструкції, призначені для побудови S-блоків, що відповідають зазначеним критеріям криптографічної якості.

Природньо, що у повній множині S-блоків існують обмежені кількості таких їх екземплярів, що у тій чи іншій мірі задовольняють вибраному критерію криптографічної якості. Означене встановлює певні лімітації на побудову S-блока, який був би ідеальним з точки зору кожного з зазначених критеріїв криптографічної якості. Дослідження потужностей множин S-блоків є фундаментальним з точки зору розробки практичних конструкцій S-блоків, дослідження їх криптографічної якості та розуміння основних можливостей щодо її підвищення. На сьогоднішній день у відкритих літературних джерелах відсутні відомості щодо потужностей класів S-блоків, які володіли б заданим рівнем періодів повернення у вихідний стан.

Метою цієї роботи є дослідження потужностей класів S-блоків довжин $N = 8{,}16$, що володіють заданим періодом повернення S-блока у вихідний стан.

Одним з основних критеріїв криптографічної якості є критерій — повернення S-блоків у вихідний стан, який визначається як число ітерацій до повернення S-блоку в початковий стан, при тривалій вхідній дії. Для обчислення періоду повернення S-блока у вихідний стан, необхідно розкласти його на цикли, що визначаються як послідовності переходів елементів. Наприклад, для S-блока довжини $N = 8$

$$S = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ ? & ? & ? & ? & ? & ? & ? & ? \\ 6 & 7 & 3 & 2 & 0 & 1 & 4 & 5 \end{bmatrix}, \quad (1)$$

маємо наступні цикли

$$S = \{C_3(6,4,0),\ C_3(1,7,5),\ C_2(2,3)\}, \quad (2)$$

тоді період повернення S-блока у вихідний стан визначатиметься як

$$T = \text{НСК}(i_1, i_2 ...). \quad (3)$$

Відповідно до мети роботи сформуємо алгоритм експериментальних досліджень у вигляді конкретних кроків.

Крок 1. Сформувати вибірку досліджуваних S-блоків Ψ заданої довжини N та потужності $|\Psi|$.

Крок 2. Провести дослідження періодів повернення для кожного S-блока, який був сформований на *Кроці 1.*

Задля дослідження взаємозв'язку періодів повернення S-блоків у вихідний стан для значення довжини $N = 8$ може бути застосований метод повного перебору, тобто сформована вибірка Ψ, що вміщуватиме всі можливі варіанти S-блоків даної довжини, оскільки загальна множина даних S-блоків включає лише $|\Psi| = 40320$ елементів.

У табл. 1 представлено значення періодів повернення S-блоків довжини $N = 8$ у вихідний стан.

Таблиця 1 — Значення періодів повернення у вихідний стан та відповідні їм значення нелінійності для S-блоків довжини $N = 8$

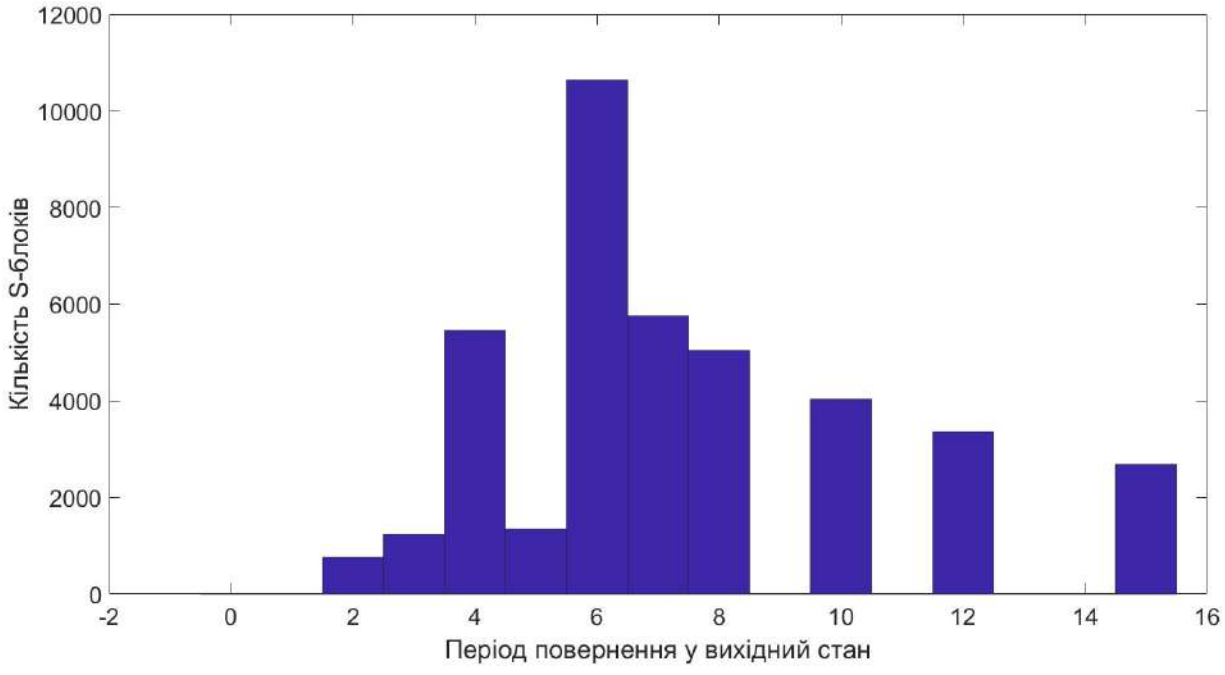
Період	1	2	3	4	5	6	7	8	10	12	15
Кількість	1	763	1232	5460	1344	10640	5760	5040	4032	3360	2688

Для дослідження S-блоків довжини $N = 16$ сформуємо вибірку з $|\Psi| = 1000000$ випадково згенерованих S-блоків, щодо яких проведемо дослідження, результати яких представлені у табл. 2.

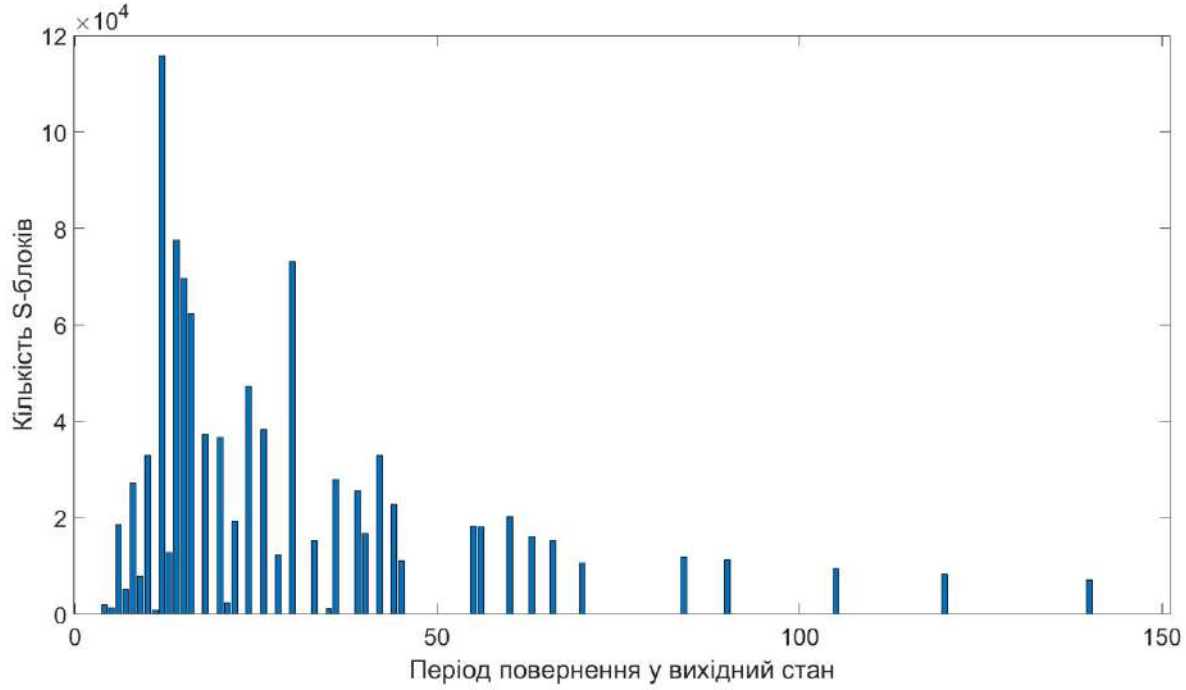
Таблиця 2 — Значення періодів повернення у вихідний стан та відповідні їм значення нелінійності для S-блоків довжини $N = 16$

Період	2	3	4	5	6	7	8
Кількість	1	52	1948	1440	18873	5034	27046
Період	9	10	11	12	13	14	15
Кількість	7580	32850	744	116719	12700	77251	69394
Період	16	18	20	21	22	24	26
Кількість	62387	37195	36889	2233	18684	47334	38474
Період	28	30	33	35	36	39	40
Кількість	12133	73450	15424	1172	27886	25781	16756
Період	42	44	45	55	56	60	63
Кількість	32804	23027	11089	18241	17764	19959	15831
Період	66	70	84	90	105	120	140
Кількість	15285	10714	11989	11031	9435	8145	7256

На рис. 1 показане графічне представлення кількостей S-блоків, що мають заданий період повернення у вихідний стан для значень довжини S-блоків $N = 8$ та $N = 16$.



а)



б)

Рис. 1 — Кількості S-блоків, що мають заданий період повернення у вихідний стан для значень довжини $N = 8$ *(а) та* $N = 16$ *(б).*

Аналіз даних, що представлені у табл. 1 та табл. 2, а також даних рис. 1 дозволяє дійти висновку, що зі збільшенням значення необхідного періоду повернення, кількість S-блоків, що володіють даним періодом істотно зменшується.

Висновки

Відзначимо основні результати проведених досліджень:

1. Проведено дослідження кількостей S-блоків, що володіють заданим рівнем періоду повернення у вихідний стан для практично цінних довжин $N = 8,16$.

2. Встановлено, що зі збільшенням значення періоду повернення S-блоків, кількість S-блоків, що володіють даним значенням періоду повернення, зменшується. Дана обставина означає, що випадково згенерований S-блок, з великою ймовірністю, не володітиме максимальним або близьким до максимального для даної довжини S-блоків значенням періодів повернення у вихідний стан. Означене диктує необхідність розробки регулярних методів синтезу множин S-блоків, які, зокрема, відповідають критерію максимізації періоду повернення у вихідний стан.

Список використаної літератури:

1. Shannon C. E. A Mathematical Theory of Cryptography. USA: Bell System Technical Memo, 1945. MM 45-110-02.
2. Соколов А. В. Новые методы синтеза нелинейных преобразований современных шифров. Lap Lambert Academic Publishing, Germany 2015. 100 с.
3. Sokolov A., Kazakova N., Kuzmenko L., Mahomedova M. Prerequisites for developing a methodology for estimating and increasing cryptographic strength based on many-valued logic functions. CEUR Workshop Proceedings, 2021. 2923. P. 107-116.
4. Maier W., Staffelbach O. Nonlinearity criteria for cryptographic functions. In Advances in Cryptology: Eurocrypt'89, 1990. Vol. 434, Lecture Notes in Computer Science, Springer-Verlag. P. 549-562.

Ключові слова: криптографія, S-блок, період повернення у вихідний стан.
Keywords: cryptography, S-box, the period of return to the initial state.

РОЗПОДІЛЕНІ МЕРЕЖІ ТА ЇХ РОЛЬ У БЛОКЧЕЙН-ТЕХНОЛОГІЯХ

Сметана Владислав

студент 2-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Технологія блокчейн стрімко розвивається в останні роки, впливаючи на різні галузі та сектори. Основним компонентом технології блокчейн є її залежність від розподілених мереж.

Розподілені мережі лежать в основі технології блокчейн. Розподілена мережа складається з групи взаємопов'язаних вузлів, які співпрацюють, щоб досягти загальної мети. Децентралізований характер цих мереж забезпечує відсутність єдиної контролюючої структури, забезпечуючи безпеку, прозорість та стійкість до відмов. В контексті технології блокчейн розподілені мережі є фундаментальним елементом. Децентралізація є ключовою характеристикою розподілених мереж. Технологія блокчейн може використовуватися для децентралізованого зберігання важливих даних, таких як медичні записи, ідентифікаційні документи та освітні сертифікати. В умовах війни, коли може виникнути ризик втрати або знищення документів, розподілена система зберігання даних може забезпечити доступ до необхідної інформації навіть у найскладніших умовах. В децентралізованій системі немає єдиного суб'єкта, що володіє абсолютним контролем. Це сприяє довірі та прозорості шляхом усунення центральних точок контролю. В контексті технології блокчейн це запобігає концентрації влади, що робить систему більш безпечною та стійкою.

Розподілені мережі складаються з учасників (вузлів), які можуть бути фізичними комп'ютерами, серверами або пристроями, підключеними до мережі. Кожен вузол виконує певні функції та може надсилати та приймати дані. Вузли в розподілених мережах взаємодіють безпосередньо один з одним. Ця взаємодія "peer-to-peer" забезпечує ефективне розповсюдження даних без посередників. Технологія блокчейн використовує взаємодію "peer-to-peer" для розповсюдження транзакцій та підтримки консенсусу в мережі. Дані в розподіленій мережі часто реплікуються на декількох вузлах. Ця резервованість підвищує стійкість до відмов та доступність даних. У випадку технології блокчейн кожен вузол зберігає копію всього обліку, забезпечуючи цілісність даних та стійкість. Блокчейн використовує специфічні протоколи зв'язку для обміну даними. Один із найвідоміших протоколів - це "Gossip Protocol", який використовується для розповсюдження інформації про нові транзакції та блоки в мережі [2]. Протокол розпочинається з того, що один або декілька вузлів в мережі ініціюють процес, надсилаючи інформацію або дані іншим вузлам. Ці вихідні вузли можуть бути вузлами, які створили нову транзакцію, блок чи іншу інформацію, яку вони хочуть поширити в мережі. Кожен вузол, який отримав інформацію, стає ініціатором та передає її іншим вузлам, які ще не отримали цю інформацію. Цей процес повторюється до того моменту, поки всі вузли в мережі не отримають інформацію.

Розподілені мережі використовують механізми консенсусу для того, щоб гарантувати узгодженість між всіма учасниками стосовно стану мережі та даних. Наприклад, блокчейн використовує різні механізми консенсусу, такі як доказ роботи (Proof of Work, PoW) та доказ володіння (Proof of Stake, PoS), для перевірки транзакцій та додавання нових блоків до ланцюжка [1].

У PoW учасники змагаються, щоб розв'язати складне завдання хешування, відоме як "доказ роботи". Це завдання полягає в пошуку спеціального числа (відомого як "nonce"), яке, разом з іншими даними блоку, створює хеш-значення (хеш блоку), що починається з певної кількості нулів. Учасникам потрібно багато ітерацій для знаходження правильного nonce, що вимагає значної обчислювальної потужності і, відповідно, електроенергії. Коли майнер знаходить правильне рішення, він додає блок до ланцюжка та транслює його по мережі. Усі інші учасники в мережі легко перевіряють, що рішення було виконано правильно, хешуючи блок за допомогою знайденого nonce. Якщо хеш блоку починається з необхідної кількості нулів, то рішення вважається правильним. Майнери, які успішно знаходять новий блок і додають його до блокчейну, отримують винагороду у вигляді нових видань криптовалютних токенів [1]. Ця винагорода називається блок-винагородою і представляє собою фіксовану кількість криптовалюти, яка створюється при ство-

ренні кожного нового блока. Крім того, майнери отримують комісії за транзакції, які користувачі мережі оплачують.

Проте механізми консенсусу, такі як PoW, які використовують деякі блокчейни, викликають обурення через споживання енергії. Процес майнінгу може вимагати багато ресурсів. Перехід до більш енергоефективних механізмів консенсусу, таких як PoS, є потенційним рішенням.

Розподілені мережі забезпечують надійну безпеку. Децентралізація та реплікація даних знижують вразливість, роблячи компрометацію системи зловмисниками дуже складною. Незмінність блокчейн-записів також сприяє безпеці зберіганих даних.

Розподілені мережі надають високий рівень прозорості. Всі учасники мережі можуть бачити та перевіряти історію транзакцій, що забезпечує довіру та відповідальність. У технології блокчейн ця прозорість є основою, особливо в застосуваннях, таких як управління постачанням і фінанси.

Реплікація даних на декількох вузлах забезпечує високу доступність. Навіть при збоях деяких вузлів мережа продовжує працювати, і дані залишаються доступними. Ця стійкість дуже важлива для застосувань блокчейн, які вимагають цілодобової доступності.

Відсутність потреби в довірі - унікальна перевага розподілених мереж в блокчейні. Учасники можуть взаємодіяти та проводити транзакції, не потребуючи довіри до центрального органу, такого як біржа. Замість цього вони довіряють базовій технології та правилам консенсусу мережі.

Масштабованість залишається значущою проблемою для розподілених мереж, включаючи блокчейн. Зі зростанням кількості учасників та транзакцій мережа може стикнутися з перевантаженням і зниженням продуктивності. Вивчаються різні рішення для масштабування, такі як протоколи другого рівня та шарування. Протоколи другого рівня - це рішення, які будуються над основною блокчейн-мережею (Layer 1) і призначені для збільшення масштабованості та покращення продуктивності мережі. Зазвичай вони вирішують проблеми, пов'язані з високою вартістю та затримкою транзакцій в основній мережі. Наприклад, для мережі Ethereum існують різні протоколи другого рівня, такі як Optimistic Rollups і zk-Rollups. Вони дозволяють стискувати транзакції та виконувати їх в більш ефективних та швидких середовищах, а потім зводити результати в основну блокчейн-мережу Ethereum. Зі свого боку, шарування дозволяє поділити мережу на кілька фрагментів (шардів), кожен з яких може обробляти свої власні транзакції та смарт-контракти [2]. Мережу розділяють на декілька шардів, і кожен шард має свій набір вузлів і базу даних для обробки транзакцій. Транзакції та дані розділяються між шардами таким чином, що кожен шард не обов'язково повинен знати про всі

транзакції та дані в мережі. Це зменшує навантаження на кожен шард і дозволяє обробляти багато транзакцій паралельно [3].

Криптовалюти, такі як Bitcoin і Ethereum, залежать від розподілених мереж для безпечних і недовірливих транзакцій. Ці мережі дозволяють емісію та передачу цифрових активів без посередників.

Смарт-контракти - це самовиконуючі контракти з умовами угоди, записаними безпосередньо в коді на спеціальних мовах програмування, таких як Solidity (для Ethereum), Vyper, Simplicity та інші, в залежності від блокчейн-платформи. Код смарт-контракту визначає умови, логіку та поведінку контракту. Розподілені мережі полегшують виконання смарт-контрактів, автоматизуючи різні процеси в прозорий і невразливий до втручання спосіб [2]. На початок червня 2023 сума пожертвувань Україні в криптовалютах перевищила 135 мільйонів доларів США [4]. Ця сума є вражаючою та свідчить про широку підтримку та допомогу зі сторони криптоспільноти світу. Пожертвування в криптовалютах може забезпечити більшу прозорість та ефективність в розподілі гуманітарної допомоги та фінансуванні важливих проектів. Ця інформація свідчить про роль криптовалют та розподілених мереж у сприянні глобальним гуманітарним ініціативам та реагуванню на кризи.

Рішення для управління ланцюгами постачання на основі блокчейн використовують розподілені мережі для відстеження переміщення товарів від місця походження до місця призначення. Це зменшує мошенництво і забезпечує аутентичність продукції.

Додатки децентралізованих фінансів використовують розподілені мережі для створення фінансових послуг без традиційних посередників. Ці платформи пропонують можливості для кредитування, запозичення, торгівлі та заробітку доходу, зберігаючи при цьому безпеку і прозорість.

Розподілені мережі довели свою фундаментальну важливість в технології блокчейн, забезпечуючи безпечні, прозорі та недовірливі системи. В умовах війни розподілені мережі та блокчейн можуть бути використані для створення безпечних систем електронного голосування, які можуть допомогти управлінню виборчими процесами в умовах кризи або обмежень на місцевості. В ситуаціях гуманітарних криз, блокчейн може допомогти відстежити розподілення гуманітарної допомоги та ресурсів. Кожна транзакція та поставка може бути записана у блокчейні, забезпечуючи прозорість та звітність використання ресурсів. У військових конфліктах або глобальних кризах може бути складно зберігати медичні історії та ідентифікаційні дані.

Незважаючи на численні переваги, існують виклики, такі як масштабованість, споживання енергії та управління. Проте постійні дослідження та інновації продовжують вирішувати ці проблеми. З розвитком механізмів консенсусу, засобів масштабування та моделей управління розподілені мережі,

ймовірно, будуть грати більш значущу роль у способах здійснення транзакцій та встановлення довіри в цифрову епоху.

Список використаних джерел:

1. Що таке блокчейн і як він працює? [Електронний ресурс]. URL: https://academy.binance.com/uk/articles/what-is-blockchain-and-how-does-it-work#.
2. Gossip Protocol. [Електронний ресурс]. URL: https://academy.binance.com/en/glossary/gossip-protocol.
3. Smart contract sharding with proof of execution. [Електронний ресурс]. URL: https://aait.od.ua/index.php/journal/article/view/122/172.
4. Україна отримала понад $100 млн криптовалютних пожертвувань. Куди вони йдуть? [Електронний ресурс]. URL: https://mind.ua/ru/publications/20247440-kripta-dlya-vsu-i-bezhencev-ukraina-poluchila-bolee-100-mln-kriptovalyutnyh-pozhertvovanij-kuda-oni-id.

Ключові слова: розподілені мережі, блокчейн, децентралізація.
Keywords: distributed Networks, blockchain, decentralization.

Науковий керівник: к.т.н., доцент Задерейко О. В.

ЧИСЛА, ЩО НЕ ПІДДАЮТЬСЯ НАУКОВОМУ ПОЯСНЕННЮ

Шляхтицький Дмитро

студент 2-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична Академія»

Сьогодні існує безліч цікавих чисел, які можуть бути більшими за нескінченність, меншими за нуль, але не від'ємними, нескінченно малими та інші.

Ці числа на перший погляд є нелогічними та навіть дурними, але такі числа не тільки не протирічать логіці науки, а навпаки, є важливою складовою сучасної математики та фізики.

Нескінченно великі числа використовуються в теорії множин та аналізі, де вони допомагають описувати складні структури та взаємодії між об'єктами.

Нескінченно малі числа допомагають описувати малий розмір об'єктів в фізиці та інженерії, а також використовуються в теорії чисел та інших галузях математики.

Багатовимірні числа, такі як уявні, комплексні, гіперкомплексні(кватерніони), дуальні та гіперболічні є важливими в геометрії та фізиці, де вони допомагають описувати складні просторові взаємодії між об'єктами.

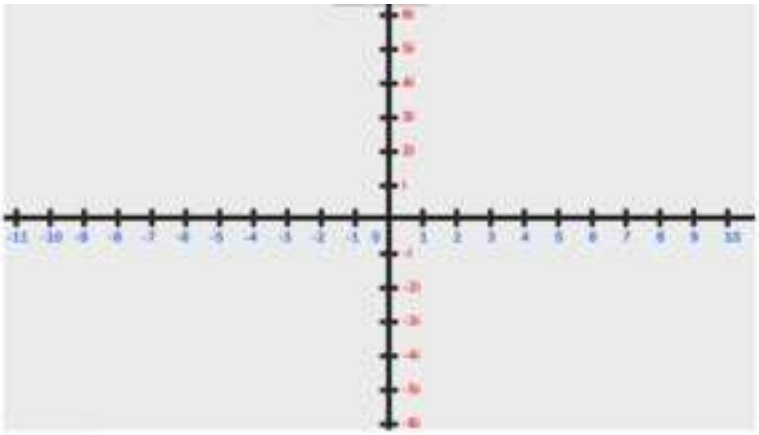
Знання про ці різноманітні числа може мати важливе застосування в різних галузях науки та технології, від фінансів до комп'ютерної графіки та машинного навчання.

Метою є те, що існування таких феноменів кидає нам виклик і спонукає зайнятися докладним вивченням тих форм, які Евклід відклав у бік через їхню «безформність» — дослідити, так би мовити, морфологію «аморфного».

З самого початку вивчення математики ми запитуємо себе: "Чому її так часто називають «холодною» та «сухою»?" Однією з причин є її нездатність описати форму хмари, гори, дерева або берегової лінії. Хмари не є сферами, гори — конусами, берегові лінії не можна зобразити за допомогою кіл, кору дерев не назвеш гладкою, а шлях блискавки — прямолінійним. У більш загальному вигляді можна заявити, що багато форм Природи настільки неправильні і фрагментовані, що в порівнянні з евклідовими фігурами (евклідовою в даній роботі ми називатимемо все, що відноситься до звичайної геометрії) Природа демонструє не просто більш високий ступінь, але зовсім інший рівень складності. Кількість різних масштабів довжини в природних формах можна вважати нескінченним для будь-яких практичних завдань.

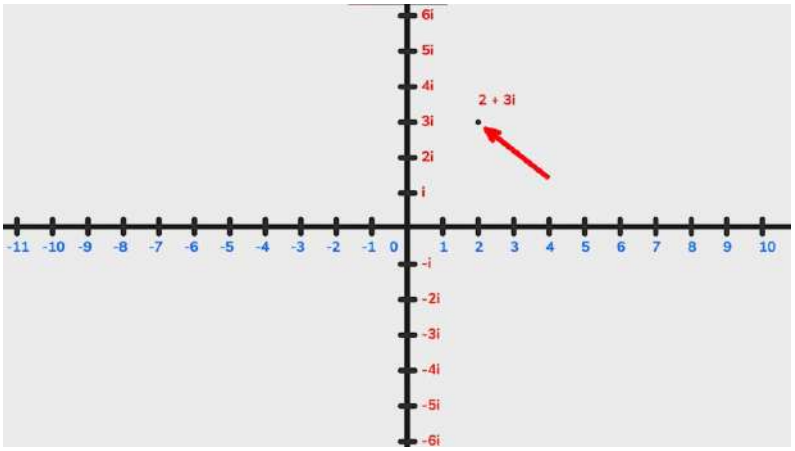
Уявні числа. Почнемо з класичного прикладу - уявних чисел. Уявні числа - це числа, які при множенні на себе дають негативний результат. Одним із прикладів такого числа є комплексне число .

Цікаво, що таке уявне число , яке не має місця на числовій прямій? Насправді, на звичайній числовій прямій немає чисел, які можуть бути помножені на себе, щоб отримати негативне число. У зв'язку з цим ми можемо створити нову числову пряму, де замість одиниці перебуватиме уявне число . Тепер ми можемо використовувати такі числа як , , і т.д. без порушення законів математики.



Комплексні числа. При додаванні уявного числа зі звичайним дійсним числом ми отримуємо комплексне число, яке складається з двох частин - дійсної та уявної. Деякі математики раніше схилялися до думки, що уявні числа є просто математичним трюком, який можна використовувати лише у

деяких випадках. Однак пізніше виявилося, що комплексні числа насправді мають низку важливих застосувань. Наприклад, вони використовуються для розрахунку поворотів на площині, а також електротехніки. У квантовій механіці комплексні числа відіграють фундаментальну роль і використовуються для опису багатьох процесів. Таким чином, уявні числа є важливим інструментом у математиці та її додатках.



Гіперкомплексні числа. Ми вже зрозуміли, що у фізиці використовуються числа, які виходять за рамки звичайної числової прямої, такі як комплексні числа. Але що, якщо ми розглянемо гіперкомплексні числа, які складаються не лише з двох, а із трьох і більше частин? Які властивості таких чисел і як їх можна застосовувати в науці?

Кватерніони (Уявне число j та k). Нове число складатиметься з 4 частин: однієї дійсної та трьох уявних. І кожна уявна кількість у квадраті дорівнює -1, але при цьому вони всі 3 нерівні один одному, плюс там ще є кілька важливих формул.

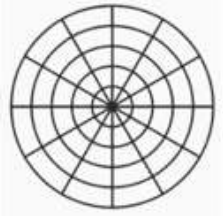
$$i^2 = -1 \qquad ij = -ji = k$$
$$j^2 = -1 \qquad jk = -kj = i$$
$$k^2 = -1 \qquad ki = -ik = j$$
$$ijk = -1$$

Виявляється, ними можна ефективно описувати повороти об'єктів у тривимірному просторі. Будь-який популярний 3-d ігровий движок, як, наприклад, Unity використовує кватерніони у своїх розрахунках.

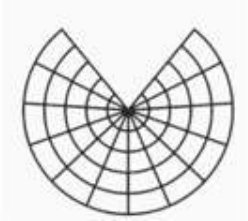
4-вимірний простір. Замість розгляду незвичайних чисел можна вивчати незвичайні геометричні простори. Як люди, ми постійно взаємодіємо з об'єктами у нашому оточенні та визначаємо їх становище у просторі. Однак, що станеться, якщо ми змінимо сам простір, де ці об'єкти знаходяться?

Одним із способів змінити простір є зміна кількості вимірів.

Інша кривизна. По-друге, ми можемо змінити кривизну простору. Якщо коротко, уявимо собі коло, не секрет, що в ньому 360 градусів.



Гіпер коло. А тепер візьмемо і буквально розсунемо простір, додавши туди ще градусів, щоб їх було, наприклад, 400. Тепер у нас з'явився величезний шматок нового простору.



Але ж ми не знаходимося в центрі простору, і він не розширюється саме з нашої точки. Виходить, що з кожної точки простору має йти шматок нового. І відповідно, геометрія і стереометрія такого простору дуже сильно змінить-ся. З'явиться більше сторін, до яких можна повернутись, і площа кожної з граней суттєво збільшиться.

Від'ємна кривизна. Прочитавши про від'ємну кривизну здається, що фігура виглядає як коло, але це не так. Це нескінченний простір, просто його неможливо спроектувати на нашу площину. Ось тому деякі ділянки малю-ються більшими, а інші дрібнішими при спробі візуалізувати простір з від'єм-ною кривизною. Ця тема заслуговує на окреме дослідження, але мова не про це зараз. Те, що ми отримали, називають Простором із негативною кривиз-ною.

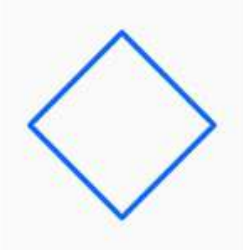
А що, якщо в такий спосіб не збільшити, а навпаки, зменшити простір? Як би вирізати з нього певний кут. Тоді ми матимемо простір із позитивною кривизною. Воно замкнеться саме у собі та утворює сферу. На цій картинці показані простори з +, - та 0 кривизною.

Метрика, метрика міських кварталів. Уявимо площину, де ми можемо ходити тільки вгору, вниз, вправо і вліво.

Якщо ми хочемо пройти від .A в .B, то краще піти по діагоналі.Але за умовою простору ми можемо ходити тільки вгору, вниз, ліворуч і праворуч.У такій геометрії у нас народжується безліч різних найкоротших шляхів.

Тоді, зміняться і характеристики простору. Цей спосіб зміни простору називають Метрикою. Метрика, де можна рухати вгору, вниз, ліворуч і праворуч називають Манхеттенською або Метрикою міських кварталів. Тобто розташовані будинки у вигляді сітки, і, відповідно, ми не можемо ходити крізь ці будинки.

Коло метрики міських кварталів. Цікаво те, що якщо розмістити всі 4 точки на однаковому відстані від нас, скажімо, в 100 метрів, то вид метрики набуде цього виду.



А тепер згадаємо рівняння кола для точок, що знаходяться на рівній відстані від центру. Тобто, в даній метриці, ромб вважається колом, адже в такому просторі ми не могли ходити по діагоналі, тому коло вийшло таким дивним. Розглянемо простір, де маємо можливість переміщатися по діагоналі. Більше того, крок по діагоналі рівносильний кроку по хрестоподібному напрямку. Прекрасним прикладом є король у шахах. Цю метрику називають Метрикою Чебишева.

Метрика Чебишева та коло. У цій метриці коло набуває такого вигляду, схожого з ромбом, але вже як квадрат.

У деяких комп'ютерних іграх розробники поєднують швидкість переміщення по осі x і осі y і, відповідно, швидкість по діагоналі буде набагато вищою, ніж рух по хрестоподібній. Тобто персонаж перебувати у своєрідній Метриці Чебишева. Якщо ж змінювати параметри метрики поступово, то з ромба ми з часом отримаємо коло, а з нього квадрат.

Гіперболічні числа. Але давайте повернемося до числа. Я вже розповів про комплексні числа, але що ми поговоримо про числа, квадрат яких дорівнює 1? Так, вже існує натуральне число, що дає нам 1 у квадраті, і це 1. Але візьмемо за аксіому те, що дане число не дорівнює одиниці, але в квадраті воно їй дорівнює. Так у нас з'являться чергові цікаві числа, такі числа ми

називаємо гіперболічними. Якщо в комплексних числах ми бачимо графік у вигляді банального кола, то графік кола гіперболічних чисел виглядатиме як гіпербола.

Дуальні числа. У дуальних числах, які є розширенням комплексних чисел, також можна визначити коло. Коло в дуальних числах - це множина точок, рівновіддалених від центру на однакову відстань, яка може бути визначена за допомогою дуальної алгебри.

Центр кола можна виразити у вигляді дуального числа, а радіус - у вигляді не- нульового дуального числа. Якщо дуальне число, що представляє радіус, є одиницею, то мова йде про одиничне коло.

Коло в дуальних числах має вигляд двох паралельних прямих.

Список використаних джерел:

1. Комплексне число. URL: https://uk.wikipedia.org/wiki/Комплексне число
2. Гіперкомплексне число. URL https://uk.wikipedia.org/wiki/Гіперкомплексні числа
3. Чотиривимірні гіперкомплексні числа. URL: https://uk.wikipedia.org/wiki/Чотиривимірні гіперкомплексні числа
4. Форма Всесвіту. URL: https://uk.wikipedia.org/wiki/Форма Всесвіту
5. Мангеттенська метрика. URL: https://uk.wikipedia.org/wiki/Мангеттенська метрика

Ключові слова: комплексні числа, метрика, кривизна, простір, дуальні та гіперболічні числа.
Keywords: complex numbers, metric, curvature, expanse, dual and hyperbolic numbers.

Науковий керівник: к. ф.-м. н., доцент Бакуніна О.В.

СУЧАСНІ МЕТОДИ ДОСЛІДЖЕННЯ ТА ОЦІНКИ DDoS-АТАК

Щербина Юрій

доцент кафедри інформаційних технологій
факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Казакова Надія

професор кафедри кібербезпеки
Факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Постановка проблеми

Протягом останнього десятиліття жертвами зловмисних осіб, що використовують комп'ютерні DDoS-атаки, стала велика кількість компаній, що працюють у сфері бізнесу та виробництва.

Під DDoS-атакою розуміється зловмисна спроба кількох систем зробити недоступними комп'ютерні або мережні ресурси для суб'єктів розподіленого обчислювального процесу, шляхом переривання або призупинення служб, підключених до Intrnet [1]. Проведені дослідження [2] показують, що об'єм трафіка таких атак експоненційно збільшується з року в рік. Зловмисники використовують для організації атак сучасні передові удосконалені методи, що дозволяють долати існуючи технічні засоби захисту.

Встановлено, що всі DDoS-атаки запускають з використанням, так званих, ботнетів [3]. Ботнетами вважаються безліч скомпрометованих комп'ютерів, що контролюються через сервер управління, який передає "жертві" атаки величезні об'єми даних [4].

Забезпечення ефективного захисту від DDoS-атак вимагає застосування сучасних методів дослідження і оцінки їх впливу на рівень безпеки інформаційних ресурсів на основі отриманих експериментальних даних.

Ціль дослідження

Переважна більшість дослідників DDoS-атак використовують загально доступні реальні дані для перевірки ефективності обраних методів захисту. Головною їх ціллю є вибір набору параметрів, який дозволяв би виявляти факти наявності атак із будь-якої суміші нормального інформаційного та атакуючого трафіку при будь-якому їх співвідношенні.

Перспективні методи дослідження DDoS-атак

Метод, що обирається або розроблюється для дослідження впливу DDoS-атак, передбачає організацію і проведення мережного експерименту та виконання на основі отриманих даних оцінки можливих наслідків від реалізації таких атак. На даний час розглядаються такі методи оцінки, як математичне моделювання, симуляція, емуляція та випробування в реальних умовах на реальних розподілених мережних обчислювальних системах.

Математичне моделювання, носить виключно теоретичний характер. В таких моделях розподілена обчислювальна система, її програмне забезпечення, платформа та умови середовища функціонування моделюються символічно і перевіряються математичними методами.

Симуляція, дозволяє виконувати статистичні мережні випробування з використанням комп'ютерних систем. Таке експериментальне моделювання є найбільш простим і найменш затратним, що дозволяє переглядати значну кількість способів протидії DDoS-атакам та визначати найбільш придатні з них у заданих умовах функціонування ще до початку їх практичної реалізації. Під час симуляції використовуються ключові функції операційної системи, механізми її ядра, віртуальні платформи та різні варіанти умов функціонування.

Емуляція передбачає комбінування моделювання з використанням випробувань на реальних системах. На відміну від моделювання, емуляція виконуються в реальному часі на реальній обчислювальній системі, а канали зв'язку, маршрутизатори та фоновий трафік і потоки атак реалізуються на основі побудованих математичних моделей. Недолік емуляції полягає в обмеженості "мережного простору", на якому виконується дослідження впливу DDoS-атак. Змоделювати топологію, яка за своїми розмірами, була б така сама, як і у інтернет-провайдера, неможливо.

Використання реальних розподілених мережних обчислювальних систем, програмного забезпечення і операційних систем, забезпечують реалістичні умови оцінки засобів протидії можливим DDoS-атакам. Втім, на використання реальних умов для дослідження, існують наступні обмеження:

– буд-які зміни в топології системи вимагають повторних досліджень в нових умовах;

– експериментальні дії з використанням вірусного програмного забезпечення є небезпечним через можливість їх виходу з під контролю експериментаторів;

– є можливість, що імітація DDoS-атаки на базі лавинної розсилки приведе до деградації мережних каналів розподіленої обчислювальної системи.

Таким чином, кожен із перелічених підходів до проведення дослідження і оцінки способів впливу DDoS-атак на безпеку розподілених обчислювальних систем має свої переваги і недоліки. А саме: математичні методи носять теоретичний характер і не враховують особливостей реального середовища функціонування систем, методи моделювання (симуляції) дозволяє виконувати апроксимацію тільки обмеженої кількості апаратних і програмних функцій, емуляція забезпечує хороший спосіб використання для досліджень реального обладнання та програмного забезпечення, однак її функціональність обмежена невеликою кількістю мережних вузлів, а також складністю налаштування та відтворення результатів проведених експериментів. Що стосується використання дослідження на реальних системах, то при всіх перевагах, їх використання обмежується їх складною природою.

В роботі [5] описано системний програмний стенд для випробування і оцінки DDoS-атак, побудований за рекомендаціями організації GENI (Global Environment for Network Innovations). Він уявляє собою спробу об'єднати всі існуючі методики в одну інтегровану платформу для проведення масштабних експериментів. В рамках цього проекту дослідники рік за роком працюють над рішенням проблем, пов'язаних із проведенням випробувань новітніх систем захисту. Найбільш перспективним підходом дослідники вважають використання програмно-керованих мереж (Software Defined Networking – SDN), описаних в [6], який дозволяє просте масштабування і програмування мереж.

Реальним набором даних, на основі якого виконується оцінка ефективності обраних засобів захисту від DDoS-атак, вважають дані, отримані в реальному часі з використанням реалістичних мережних умов, а також можливостей сучасного системного програмного забезпечення і платформ.

Альтернативним варіантом такого набору даних може бути набір, отриманий в лабораторному середовищі з використанням програмної реалізації таких методологій як NS3[7], Emulab[8], GENI[9] та ін. Такі засоби мають відповідати таким вимогам:

– точності – надійності і залежності від реальних мереж;

– повторюваності – можливості відтворення результатів в конкретних умовах довколишнього середовища;

– розширюваності – можливості масштабованості топології експериментів у порівнянні з Internet-середовищем.

Загальна тенденція досліджень у сфері боротьби з DDoS-атаками передбачає, що більшість теоретичних і технічних рішень, націлених на їх виявлення та запобігання впливу на ресурси системи, перевіряються шляхом організації і проведення експериментів описаними методиками, основаними на моделюванні, емуляції реальних систем та аналізі отриманих і доступних наборів даних.

Висновки

Кожен з поширених методів перевірки мережного трафіку має свої переваги та недоліки, але останнім часом, як альтернатива їм, широко використовуються реальні доступні набори даних, вже отримані дослідниками, DDoS-атак. На сьогодні існує дві проблеми. Перша – обмеження доступності дослідницькій спільноті результатів досліджень з міркувань безпеки. Друга – полягає в постійному ускладнені розподілених комп'ютерних мереж та інформаційних технологій, що в них реалізуються. Через це, тенденція дослідження DDoS-атак зміщується у бік реальних експериментів, які передбачають масштабування і дають можливість отримання реалістичних наборів даних, придатних для випробування нових засобів безпеки.

Список використаних джерел:

1. CERT. URL : https://cert.europa.eu/publications/security-advisories/2023. 2023.
2. Matias, P., Barbosa, P., Cardoso, T. N., Campos, D. M., Aranha, D. F.: NIZKCTF: A Non-interactive Zero-Knowledge Capture-the-Flag Platform. IEEE Security & Privacy, 16(6), 42-51 (2018) URL: https://doi.org/10.1109/MSEC.2018.2875324.
3. Wang, F., Wang, H., Wang, X., Su, J.. A new multistage approach to detect subtle ddos attacks. Mathematical and Computer Modelling 2012;55(1):198–213. URL: https://www.sciencedirect.com/science/article/pii/S0895717711001154

4. Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. 2012. URL: https://arxiv.org/ftp/arxiv/papers/1208/1208.0403.pdf.
5. Elliott, C.. Geni-global environment for network innovations. In: LCN. 2008, p. 8. URL: https://www.cct.lsu.edu/~kosar/csc7700-fall06/papers/NSF05.pdf.
6. Yeganeh, S.H., Tootoonchian, A., Ganjali, Y.. On scalability of software-defined networking. Communications Magazine, IEEE 2013; 51(2):136–141. URL: https://cs.brown.edu/courses/csci2950-u/s14/papers/yeganeh13SDNscalability.pdf.
7. NS3,. The network simulator 3. 2015. URL: http://www.nsnam.org/.
8. Emulab,. 2015. URL: The emulab network testbed http://www.emulab.net/.
9. Elliott, C. Geni-global environment for network innovations. In: LCN. 2008, p. 8. URL: https://www.researchgate.net/publication/221081032_GENI_-_global_environment_for_network_innovations

Ключові слова: DDoS-атаки, ботнет, атакуючий трафік, математичне моделювання, фоновий трафік.
Keywords: DDoS attacks, botnet, attacking traffic, mathematical modeling, background traffic.

МОЖЛИВОСТІ МОВИ C# ДЛЯ ОРГАНІЗАЦІЇ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ

Чикунов Павло

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Паралельне програмування – це метод програмування, в якому обчислення розподіляються між кількома обчислювальними ресурсами, такими як процесори, ядра процесорів або комп'ютери, з метою підвищення продуктивності та зменшення часу виконання завдань [1, 2]. Паралельне обчислення особливо корисне на звичайних багатоядерних системах, де можна використовувати кілька ядр або логічних процесорів для вирішення однієї задачі одночасно.

Microsoft Visual Studio – одне з найбільш популярних інтегрованих середовищ розробки (IDE) у світі, особливо в корпоративному і комерційному секторі. Visual Studio підтримує мови програмування C++, C#, Visual Basic .NET, Python, F#, JavaScript. Для організації та підтримки паралельного програмування Visual Studio пропонує розробникам декілька підходів.

1. Використання потоків (Threads) дозволяє виконувати різні частини програми паралельно. Це основний спосіб паралельного програмування в багатьох мовах програмування, включаючи C#, C++, Java та Python.

2. Використання завдань (Tasks) – це вищий рівень абстракції для паралельного програмування і зазвичай є більш зручними для створення та керування паралельними завданнями у асинхронному режимі.

3. Стандарт для розподіленого обчислення MPI (Message Passing Interface), який дозволяє обмінюватися повідомленнями між процесами на різних вузлах великих кластерів або суперкомп'ютерів [1]. Для підтримки MPI в Visual Studio потрібно встановити спеціальні розширення та бібліотеки.

4. OpenCL (Open Computing Language) – це відкритий стандарт для паралельного програмування обчислювальних пристроїв, таких як центральні процесори (CPU), графічні процесори (GPU), сопроцесори та інші.

5. OpenMP (Open Multi-Processing) – це стандарт для багатопоточного паралельного програмування в мовах програмування, що надає можливість створювати паралельні програми для багатоядерних систем [2].

6. GPGPU – можливість організації обчислень загального призначення на графічних процесорах. Одночасне використання декількох графічних чипів паралелізує природу обробки графіки. Звичайні дискретні відеокарти можна використовувати для організації паралельних обчислень у великій кількості областей, включаючи криптографію, машинне навчання і багато інших.

Усі ці фактори створюють унікальні можливості для розвитку технологій паралельних обчислень та дозволяють вирішувати складні завдання, які раніше були недосяжними. Розробники повинні володіти навичками паралельного програмування та здатністю використовувати сучасні апаратні засоби для досягнення оптимальної продуктивності додатків.

Вибір підходу до паралельного програмування залежить від конкретних потреб вашого проекту, доступних ресурсів і ваших знань у галузі паралельного програмування. Деякі підходи, зокрема MPI, OpenMP та OpenCL, обмежені використанням мови C або C++, тому далі не розглядаються.

Для платформі .NET поки що відсутня підтримка GPGPU, тому розробникам треба покладатися на сторонні рішення, зокрема бібліотеки Alea GPU, Atimesh Hybridizer, ILGPU, які можуть використовувати C# розробники.

CUDA (Compute Unified Device Architecture) – це пропрієтарна система корпорації Nvidia, що працює з графічними процесорами серії GeForce. Нажаль, API CUDA підтримує лише мови C та C++, але є можливість використовувати DLL-модулі CUDA в проєктах C# [3].

Корпорація AMD пропонує власну GPGPU-технологію під назвою ATI Stream – це набір вдосконалених апаратних і програмних технологій, які дозволяють графічним процесорам AMD, працюючи разом із CPU, прискорювати роботу додатків, окрім графічних. Інтерфейс програмування здійснюється через OpenCL, який нажаль не підтримує мову C#. Але розробникам доступ-

ний ATI Stream SDK Developer, який підтримує мови програмування C++, Java та C# [4].

Автором розроблено новий лабораторний практикум «Організація паралельних обчислень мовою C#», який акцентує увагу здобувачів на використанні класу Thread, синхронізації потоків засобами Mutex та Semaphore, бібліотеці підтримки паралельного програмування TPL, використанні завдань Task, паралельному шаблону обробки колекцій PLINQ (Parallel Language-Integrated Query) [5].

Parallel LINQ (PLINQ) є паралельною реалізацією шаблону LINQ (Language-Integrated Query), який підтримує уніфіковану модель для запитів до будь-якого джерела даних у пам'яті, наприклад з колекціями або масивами. PLINQ реалізує повний набір стандартних операторів запиту LINQ і має додаткові оператори для паралельних операцій.

Наприклад, для опанування здобувачем шаблону PLINQ потрібно написати паралельну версію програми мовою програмування C# з використанням методу AsParallel шаблону PLINQ, з блокуванням доступу до спільних ресурсів, на 10 тестових прогонах. Щоб не впливати на чистоту експерименту, значення елементів масиву не повинні змінюватися, розмірність масиву повинна бути підібрана експериментальним шляхом, щоб час виконання програми був не менш 500 мс.

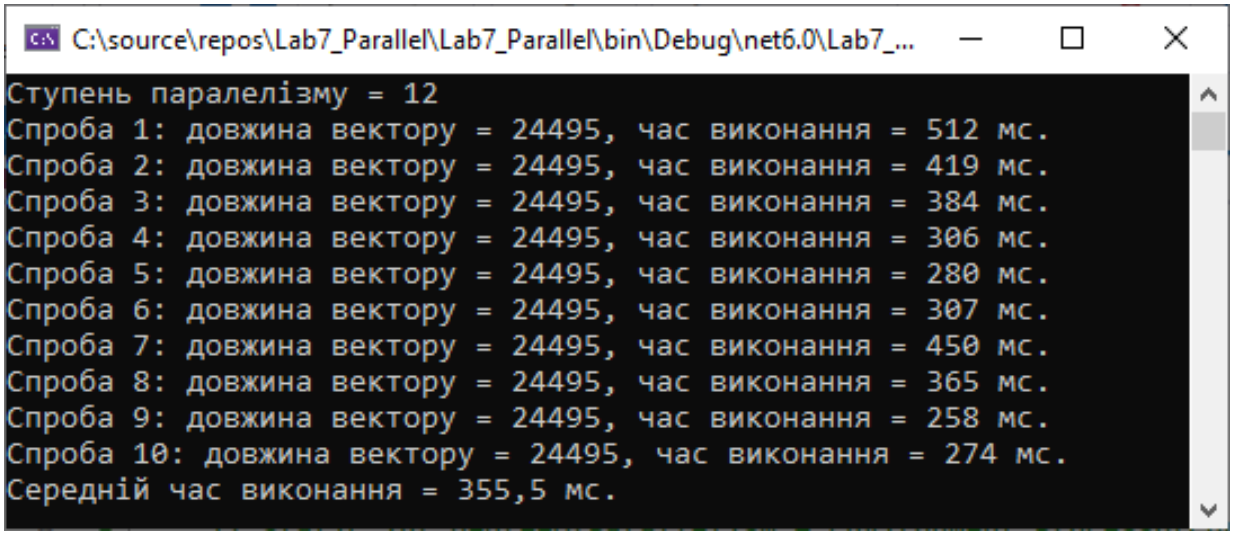


Рис. 1. Приклад виконання програми з обмеженням ступеня паралелізму 12

Окремо необхідно перевірити час виконання програми у режимі збереження порядку виконання запитів методом AsOrdered. Передбачити автоматичне або ручне обмеження ступеня паралелізму методом WithDegreeOfParallelism. При кожному тестовому запуску вимірюється час обчислення квадрату довжини вектору з використанням Stopwatch. Наприкінці програми виконано обчислення середнього часу виконання тестових запусків. Порів-

няти результати виконання програми при зменшенні кількості паралельних процесів. Обов'язково зробити висновок о рівні паралелізації реалізації алгоритму обчислення.

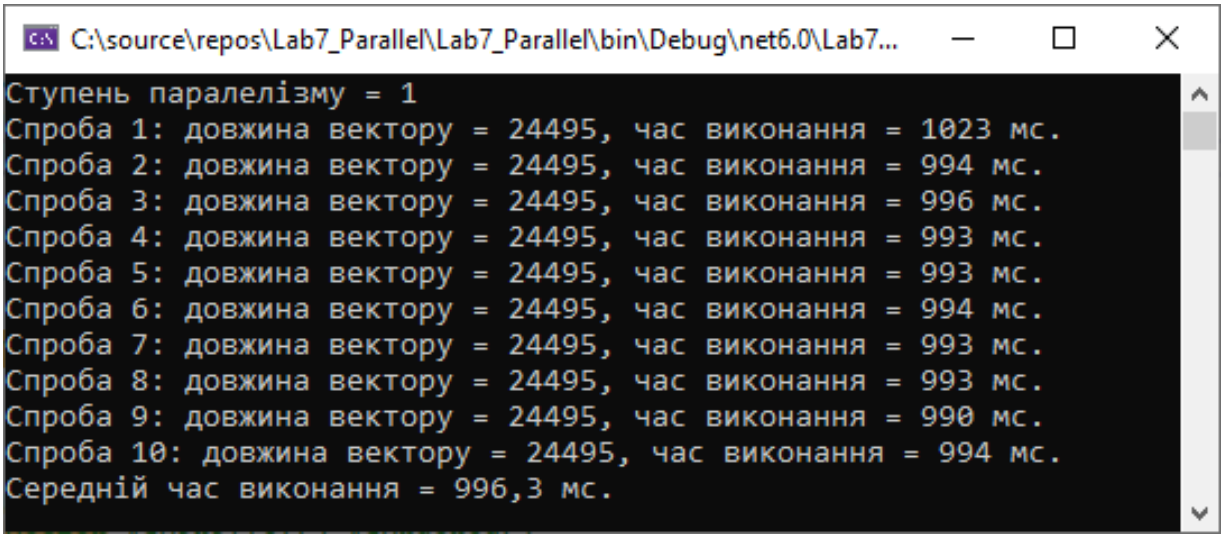


Рис. 2. Приклад виконання програми з обмеженням ступеня паралелізму 1

Список використаних джерел:

1. Гришанович Т. О. Лабораторний практикум із дисципліни "Паралельні та розподілені обчислення" [Електронний ресурс]; ВНУ імені Лесі Українки. Луцьк : ВНУ імені Лесі Українки, 2022. 50 с.
2. Минайленко Р. М. Паралельні та розподілені обчислення : навч. посіб. / Р. М. Минайленко ; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т. – Кропивницький : ЦНТУ, 2021. – 153 с.
3. CUDA Programming and Performance. URL: https://forums.developer.nvidia.com/c/accelerated-computing/cuda/cuda-programming-and-performance/7 (дата звернення: 01.11.2023).
4. ATI Stream SDK is now AMD Accelerated Parallel Processing. URL: https://community.amd.com/t5/archives-discussions/ati-stream-sdk-is-now-amd-accelerated-parallel-processing-app/m-p/93462 (дата звернення: 30.10.2023).
5. Онлайн-курс Udemy «Multithreading and Parallel Programming in C#». URL: https://www.udemy.com/course/parallel-csharp/ (дата звернення: 01.11.2023).

Ключові слова: паралельні обчислення, Visual Studio, C#, потоки, шаблон PLINQ.
Keywords: parallel computing, Visual Studio, C#, threads, PLINQ pattern.

ШТУЧНИЙ ІНТЕЛЕКТ У ВІЙСЬКОВІЙ СФЕРІ

Трофименко Олена

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат юридичних наук, доцент

Яремчук Максим

студент 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

На сьогодні засоби штучного інтелекту (ШІ) стрімко розвиваються і все частіше впроваджуються у програмно-апаратні системи для застосування у самих різних сферах життєдіяльності людини. Системи ШІ створені для навчання на досвіді, розпізнавання закономірностей і прийняття рішень на основі вхідних даних. Ці системи можна навчити виконувати певні завдання, як-от: розпізнавання зображень, розуміння природної мови тощо. Один з найцікавіших аспектів ШІ – це його здатність навчатися й адаптуватися, наслідуючи пізнавальні процеси людського мозку. Сфера ШІ охоплює широкий спектр методів, включаючи машинне навчання, оброблення природної мови, робототехніку, експертні системи тощо.

Наразі алгоритми ШІ продовжують розвиватися та автоматизувати різноманітні завдання у самих різних галузях: в інженерії – для оптимізації конструкції складних технічних систем задля покращення продуктивності та ефективності; у фінансовій сфері – для розробки торгових стратегій, які адаптуються до змінних ринкових умов і максимізують прибутки для інвесторів; в охороні здоров'я – для аналізу медичних зображень, що сприяє діагностиці хвороб та розробці персоналізованих планів лікування, а також для розробки лікарських молекул з певними властивостями, що прискорює процес відкриття ліків [1]; у підборі персоналу на роботу, щоб зменшити упередженість і підвищити ефективність; у секторі роздрібної торгівлі – як віртуальні помічники для безперебійної підтримки клієнтів, для впровадження ефективних автоматизованих систем оформлення замовлень, для оптимізації управління товарними запасами і прогнозування попиту на продукцію [2]; у сфері мистецтва – для створення новаторських, візуально привабливих дизайнів, розширюючи межі творчості [3].

Як інструмент аналізу даних за умов війни ШІ має значний вплив на військовий сектор. Він допомагає аналізувати значні обсяги інформації, яку генерують численні системи та ситуація на полі бою, та приймати ефективні рішення. Ця технологія покращує здатність оцінювати динаміку конфлікту, дозволяючи оперативно реагувати та адаптувати свої стратегії. Застосування передових технологій та концепції ШІ у військовій справі надає конкурент-

ну перевагу та сприяє загальній ефективності військових дій з різних позицій. Так, важливу роль відіграє інтеграція ШІ у військові системи розпізнавання цілей і об'єктів на супутникових зображеннях, для геолокації та аналізу відкритих даних у соціальних мережах задля ідентифікації солдатів або пересування їхніх підрозділів. Згідно з відкритими джерелами [4] нейронні мережі використовуються для поєднання фотографій на рівні землі, відеозйомки з численних дронів і БПЛА, а також супутникових зображень для забезпечення швидкого аналізу та оцінки розвідданих даних й отримання швидких та достовірних стратегічних і тактичних переваг у розвідці.

Точність. Застосування ШІ для підвищення точності зброї можливе шляхом впровадження алгоритмів машинного навчання та розпізнавання зображень. ШІ можна використовувати для навчання дронів самоідентифікації цілей і уникання втрат цивільних осіб. Це може істотно знизити ризики побічних пошкоджень і покращити точність зброї. Крім того, ШІ можна використовувати для покращення загальної продуктивності зброї шляхом аналізу даних і надання інформації для прийняття рішень. Завдяки ШІ зброю можна оптимізувати для різних сценаріїв і середовищ, що зробить її ефективнішою. Ба більше, ШІ може допомогти в розробці нової зброї та технологій, дозволяючи створювати передові складні системи.

Автономність. ШІ можна використовувати для підвищення автономності зброї, дозволяючи їй приймати рішення без втручання людини. Наприклад, ШІ може аналізувати та виявляти можливі загрози для завчасного чи то принаймні вчасного реагування на них. Ця здатність дозволяє зброї працювати незалежно та швидко реагувати на потенційну небезпеку. Завдяки впровадженню ШІ в системи озброєння, можна значно підвищити рівень автономності, зменшивши потребу в постійному нагляді та втручанні людини. Це не лише підвищує ефективність зброї, а й мінімізує ризики для операторів. Використання ШІ в цьому контексті є значним прогресом у військових технологіях, який дозволяє зброї адаптуватися та реагувати на зміни обставин у реальному часі.

Ефективність. ШІ можна використовувати для підвищення ефективності зброї шляхом автоматизації завдань, які зараз виконуються людьми. Наприклад, ШІ можна використовувати для керування складними системами зброї або аналізу даних бойових дій. Впроваджуючи технологію ШІ, можна значно підвищити швидкість і точність дій зі зброєю, що покращить ефективність і точність результатів на полі бою. Однією з переваг використання ШІ в системах зброї є його здатність автоматизувати завдання, які раніше вимагали втручання людини. Це не тільки зменшує навантаження на людей-операторів, а й мінімізує ймовірність людської помилки. ШІ може без втоми і сну обробляти величезні обсяги даних і приймати рішення в реальному часі, доз-

воляючи зброї адаптуватися і швидко реагувати на зміни обставин. Крім того, ШІ може аналізувати бойові дані для виявлення закономірностей і тенденцій, надаючи цінну інформацію для стратегічного планування та прийняття рішень. Використовуючи потужність ШІ, системи зброї можна оптимізувати для максимального використання їхнього потенціалу, що зрештою підвищує загальну ефективність роботи.

Приклади використання ШІ в сучасних системах озброєння:

– ШІ все частіше використовують, як для створення, так і для виявлення фейків. Оскільки ШІ дозволяє краще модерувати контент, то, з одного боку, його почали використовувати для створення ефективних алгоритмів розпізнавання дезінформації, з іншого — за рахунок формування ШІ відеодемонстрацій формувати реалістичні фейки та викликати помилкову реакцію ворога;

– ШІ може керувати безпілотними літальними апаратами (БПЛА) і контролювати групи дронів для проведення масових атак задля виснажування ворожих запасів бронетехніки та ракет ПВО на полі бою;

– ШІ, завдяки розпізнавання зображень та самоідентифікації цілей, надає важливу стратегічну інформацію про ворожі цілі, а також допомагає в орієнтуванні на місцевості, що відіграє важливу роль у проведенні тактичних боїв;

– ШІ можна використовувати для здійснення кібершпигунства та кібератак на інфраструктуру країни-ворога, що врешті негативно вплине і на її національну безпеку.

Наразі ШІ у війні в Україні використовується для:

– створення алгоритму розпізнавання російських військ за супутниковими знімками (ШІ-стартап Reface);

– розпізнавання облич для встановлення особистостей російських військових, боротьби з дезінформацією, ідентифікації загиблих та перевірки людей на контрольно-пропускних пунктах (технологія компанії Clearview AI);

– виявлення підозрілих осіб за допомогою системи розпізнавання облич у мобільному застосунку «ТиХто» (український YouControl спільно з компанією Artellence та за підтримки СБУ);

– створення інтерактивної онлайн-карти бойових дій в Україні, що допомагає більш точно та оперативно опрацьовувати й оновлювати дані (Deep State UA разом з Griselda);

– розмінування деокупованих територій України: робото-собаки Spot від Boston Dynamics допомагають знешкоджувати мінометні снаряди та касетні боєприпаси і тим самим зменшують ризик підриву людей [5].

З іншого боку, твердження про те, що ШІ обов'язково призведе до кращого захисту цивільного населення та дотримання норм міжнародного гуманітарного права внаслідок інтегрування алгоритмів штучного інтелекту і машинного навчання в процеси прийняття командних рішень, варто дуже критично оцінювати, беручи до уваги обмеження та вразливості програмних систем. Так, відомі приклади збоїв штучного інтелекту, навіть фатальні, коли оборонна система Patriot обстріляла літаки дружньої коаліції, оскільки відповідне програмне забезпечення класифікувало їх як атакуючі ракети [6]. Саме тому, вхідні дані та навчальні вибірки для ШІ мають бути перехресно перевірені декількома джерелами, щоб захиститися від упередженої або неточної інформації. Хоча подекуди за умов війни перевірити точність вхідних даних може бути надзвичайно складно, а подекуди і неможливо. Насамперед такі ризики пов'язані з навчальними наборами даних для ШІ. «Отруєння» такого набору даних зіпсує процес навчання та подальшу поведінку моделі. Це або знизить продуктивність систем ШІ та призведе до загальних неточностей і неефективності, або спричинить помилкову реакцію системи. З іншого боку, відомий приклад, коли 2021 року задля безпеки алгоритм ШІ націлювання ВПС навчався виключно на «синтетичних» наборах даних, згенерованих комп'ютером, і під час навчання розпізнавав об'єкти з точністю 90%, однак на практиці показники впали до 25% [7]. Тому готувати навчальні достовірні набори даних на етапі навчання ШІ треба дуже прискіпливо, включаючи шифрування даних, аудит безпеки та цілісності даних, а також готувати способи виправлення, якщо набір даних буде скомпрометовано.

Після розгортання моделі ШІ проблеми не зникають, адже вони можуть бути сприйнятливі до агресивних атак, навіть якщо зловмисник має лише доступ запитів до моделі. Вже відома категорія атак проти моделей штучного інтелекту, які називають фізичними змагальними атаками [7], що можуть змусити ШІ неправильно інтерпретувати або неправильно класифікувати дані через збурення невеликої величини, додані до вхідних даних, як-от: замасковані обличчя, розставлені хибні мітки тощо. Такі приклади показують, наскільки крихкими можуть бути системи ШІ і формують скептичність щодо їх продуктивності. Є непідставна думка про те, що замість того, щоб зробити війну зрозумілішою та чистішою, системи ШІ з такою ж вірогідністю можуть зробити її безладнішою і спричинити більше плутанини та складнощів для тих, хто приймає рішення.

Наразі побоювання того, що ШІ буде інтегрований у сферу війни вже втратила свою актуальність, адже військові системи із підтримкою ШІ вже функціонують і вдосконалюються в режимі реального часу на полі бою. Системи з автономними можливостями ШІ розгортаються на передовій як українськими, так і російськими силами, зокрема у формі безпілотників і боє-

припасів, що перебувають у режимі вільного часу. Важливо зважати на ризики при прийнятті рішень на їх основі щодо життя та смерті на полі бою та максимально мінімізувати їх.

Список використаних джерел:

1. Artificial Intelligence Revolutionizes the Retail Landscape. URL: https://ts2.space/en/artificial-intelligence-revolutionizes-the-retail-landscape/
2. Accelerating Drug Development: Unlocking the Potential of AI. URL: https://ts2.space/en/accelerating-drug-development-unlocking-the-potential-of-ai/
3. Can anyone create AI art? URL: https://ts2.space/en/can-anyone-create-ai-art/
4. Bendett S. Roles and Implications of AI in the Russian-Ukrainian Conflict. URL: https://www.cnas.org/publications/commentary/roles-and-implications-of-ai-in-the-russian-ukrainian-conflict
5. Левченко Д. Тенденції розвитку штучного інтелекту в Україні та світі. URL: https://gwaramedia.com/tendenczii-rozvitku-shtuchnogo-intelektu-v-ukraini-ta-sviti/
6. Stewart R., Hinds G. Algorithms of war: The use of artificial intelligence in decision making in armed conflict. URL: https://blogs.icrc.org/law-and-policy/2023/10/24/algorithms-of-war-use-of-artificial-intelligence-decision-making-armed-conflict/
7. Reynolds I., Cetin O. War is messy. AI can't handle it. URL: https://thebulletin.org/2023/08/war-is-messy-ai-cant-handle-it/

Ключові слова: штучний інтелект, ШІ, машине навчання, нейронні мережі.
Keywords: artificial intelligence, AI, machine learning, neural networks.

АЛГОРИТМИ У BACK-END ЗАСОБАМИ JAVA

Старіков Ігор

студент 2-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Трофименко Олена

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат юридичних наук, доцент

Задачами розробника back-end є створення, розвиток та підтримка серверної сторони програмного забезпечення. Саме від цього фахівця залежить надійність та продуктивність програмних рішень, оскільки він керує створенням та роботою з базами даних для ефективного обміну інформацією між клієнтом та сервером, обробленням запитів від інтерфейсу користувача або front-end, а також забезпеченням безпеки, продуктивності і стабільності програмних систем [1].

До інструментарію сучасного бекенд-розробника нині входять різні продуктивні алгоритми сортування, фільтрування та пошуку. У найбільш по-

ширеній для back-end мові програмування Java використання цих алгоритмів має свою специфіку:

```
private void updateValuesInContracts(
  final AbstractAdditionalField fieldForUpdate,
  final List<AdditionalFieldValueDefinition> values,
  final String contractUUID) {
    String newValue = values
      .stream()
      .filter(newValues -> contractValuesIdsForFilter.contains(newValues.getValueUuid()))
      .filter(newValues -> !newValues.isLogicalDeleted())
      .map(newValues -> String.valueOf(newValues.getValue()))
      .collect(Collectors.joining(",","));
}
```

Тут List<AdditionalFieldValueDefinition> values проходить дві фільтрації:

```
1) filter(newValues -> contractValuesIdsForFilter.contains(newValues.getValueUuid()))
2) filter(newValues -> !newValues.isLogicalDeleted())
```

А далі відбувається перетворення кожного елемента на об'єкт типу String:

```
map(newValues -> String.valueOf(newValues.getValue()))
```

У Java роботу з алгоритмами у колекціях можна виконувати за допомогою потоків (стрімів – Stream API). Наприклад, пошук потрібен при визначенні елементів, які підпадають під певні критерії бізнес-логіки. При цьому усталено стріми використовують алгоритм лінійного пошуку. Варто зауважити, в промисловій розробці не прийнято використовувати алгоритми пошуку/сортування, написані розробником для розв'язання тої чи іншої задачі. Замість цього повсюдно використовуються імплементовані інструменті чи то стороні бібліотеки, наприклад, Apache Commons Collections від Apache Foundation.

Також у Java для сортування при використанні Stream API переважно використовується усталений (default) алгоритм сортування, який вибирається JVM автоматично, залежно від даних та контексту [2]. Так, метод sorted() автоматично вибирає найбільш оптимальний алгоритм сортування для оброблюваних даних. Для малих наборів даних stream може використовувати алгоритм швидкого сортування (QuickSort) чи то алгоритм сортування злиттям (MergeSort), залежно від реалізації Java та контексту виконання. Ці алгоритми зазвичай працюють із часовою складністю O(n *log(n)), де n – кількість сортованих елементів.

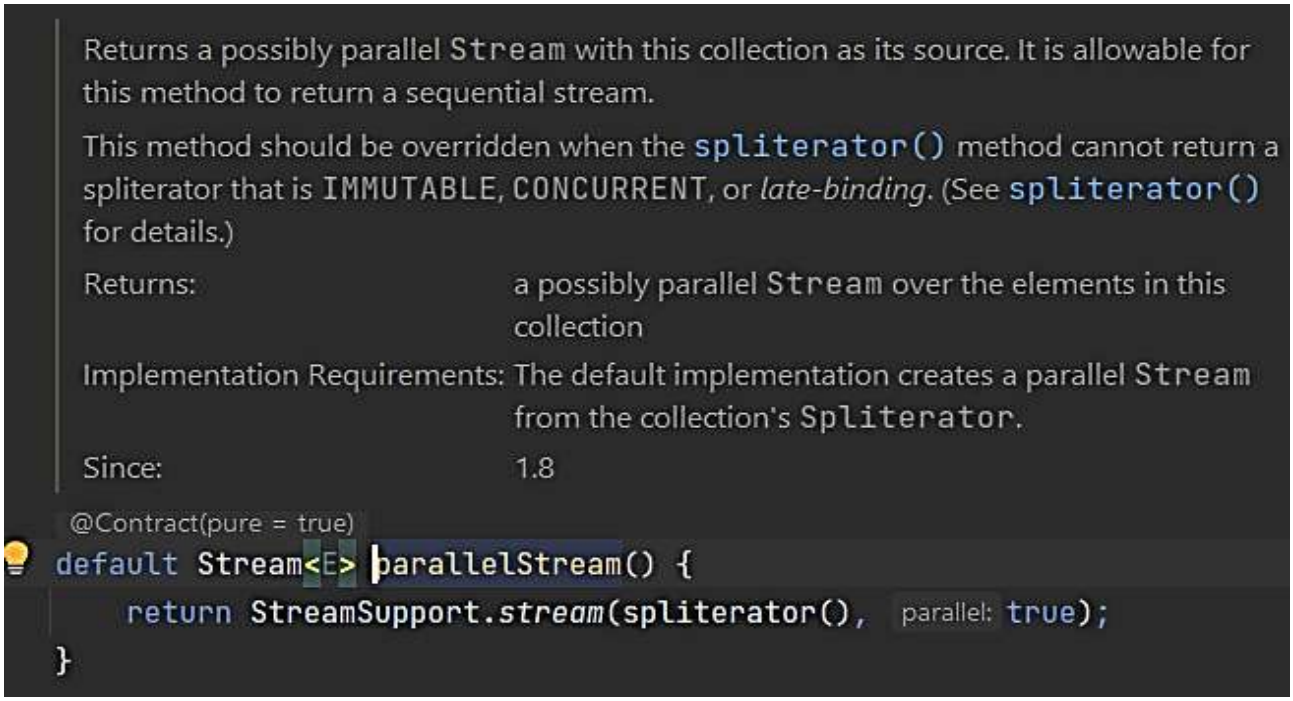
Приклад сортування колекції за допомогою потоку:

```
List<Person> sortedList = people.stream()
        .sorted(Comparator.comparingInt(Person::getAge))
        .toList();
```

Однак для великих колекцій, які не містяться в пам'яті, стріми можуть використовувати алгоритм зовнішнього сортування, який розбиває дані на частини, сортує їх частини в пам'яті, а потім об'єднує їх. Цей алгоритм є більш ефективним для великих наборів даних, але потребує більше операцій введення-виведення. Важливо, що Java Stream API абстрагує деталі алгоритмів сортування від програміста, що спрощує роботу над даними та дозволяє фокусуватися на більш високорівневих операціях.

Якщо потрібно вказати тип сортування, можна скористатися класом Arrays, в якому є метод для Dual-Pivot Quicksort. Основна відмінність цього методу від класичного швидкого сортування полягає в тому, що замість однієї опорної точки (півота), як у класичній версії, він використовує дві опорні точки (подвійний півот). Ці опорні точки розбивають масив на три частини: елементи, менші за першу опорну точку, елементи між опорними точками та елементи, більші за другу опорну точку. Далі кожна з цих частин рекурсивно сортується. Переваги Dual-Pivot Quicksort полягають у більш ефективному поділі масиву на підмасиви, більш швидкому виконанні «в середньому випадку», а також у стабільній поведінці для певних типів даних. Хоча, з іншого боку, Dual-Pivot Quicksort не завжди є оптимальним вибором і може бути програшним для деяких типів даних та для малих розмірів масивів. У таких випадках для кращої продуктивності варто використовувати інші алгоритми сортування, наприклад, сортування злиттям (Merge Sort) або сортування вставками (Insertion Sort). Отже, Stream API вибирає найліпший варіант алгоритму сортування в тій чи інший ситуації.

На практиці вважається переважним використання сортування та інших операції стріму в одному потоці. Хоча для певних задач, коли точно відомо, що будуть оброблятися великі масиви даних, доцільно використовувати паралельні стріми. Це надасть суттєві переваги, однак їх доцільно використовувати лише для великих наборів даних, інакше ефект буде протилежний:



Щодо алгоритмів пошуку, то бінарний пошук (binarySearch), який у Java надається методом Arrays.binarySearch(), працює лише, якщо колекція, в якій шукається певний елемент, відсортована. Якщо колекція не відсортована, результат бінарного пошуку може бути неправильним. Тобто, бінарний пошук виконується завжди з припущенням, що елементи впорядковані.

Інший метод пошуку findFirst() з Java Stream API використовується для роботи з довільними колекціями, не вимагаючи їхнього попереднього впорядкування. findFirst() для пошуку елемента у послідовності не виконує сортування елементів, а лише повертає перший елемент з урахуванням умов, заданих у лямбда-виразі, наприклад:

```
if (!evaluationResults.isEmpty()) {
   // look up the first unevaluated KPI
   EvaluationResult firstUnevaluatedEvaluationResult = evaluationResults.stream()
       .filter(evaluationResult -> evaluationResult.getScoreValue() == null)
       .findFirst()
       .orElse(evaluationResults.get(DEFAULT_EVALUATION_RESULT_TO_SHOW));
}
```

Час виконання findFirst() для List близький до часової складності O(n), де n – кількість елементів колекції. Метод findFirst() перебирає елементи по порядку і повертає перший елемент, який задовільнить заданій умові. Якщо такий елемент є на початку колекції, метод завершить роботу швидко. Однак, якщо відповідний елемент розташований наприкінці колекції або взагалі відсутній, метод працюватиме значно довше. Тобто швидкість виконання findFirst() для List в однопотоковому режимі залежить від розташування відповідного елемента в колекції.

Суттєво, що до версії Java 8 розробники часто вдавалися до циклів і умовних операторів для реалізації алгоритмів фільтрації, перетворення або агрегації даних. Цей підхід вимагав великого обсягу коду, був складночитаним і схильним до помилок. Впровадження Stream API забезпечило функціональний стиль роботи з даними, компактний, виразний і читабельний код, а також полегшило паралельне виконання операцій.

Загалом Stream API є потужним інструментом Java для оброблення великих наборів даних, проте не є універсальним, адже має свою специфіку. Якщо завдання не відповідає шаблону "джерело – перетворення – збір", краще скористатися іншими алгоритмами та інструментами Java. Розуміння та вміння використовувати доречні алгоритми сортування, хешування і пошуку є важливою навичкою для кожного бекенд-розробника для створення оптимізованого коду, організації ефективного обміну інформацією між клієнтом та сервером, забезпечення продуктивності та покращення якості програм.

Список використаних джерел:

1. Трофименко О.Г., Козін О.Б., Задерейко О.В., Плачінда О.Є. Веб-технології та веб-дизайн: навч. посібник. Одеса: Фенікс, 2019. 278 с. URL: http://dspace.onua.edu.ua/handle/11300/11777
2. Stream in Java. URL: https://www.geeksforgeeks.org/stream-in-java/

Ключові слова: розробнка back-end, Stream API, алгоритми сортування, алгоритми пошуку.
Keywords: back-end development, Stream API, sorting algorithms, search algorithms.

ПРОГРАМНІ ЗАСОБИ ДЛЯ ARDUINO

Усатенко Ярослав

студент 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Наразі платформи Arduino мають велику популярність і широко використовуються в охоронних системах (кодових замках для дверей, сейфах), пристроях для запуску приладів в зазначений час (світлофорах, автоматичних системах поливу, настільних годинниках, плеєрах з можливістю завантажувати різні типи файлів), приладах для вимірювання та контролю фізичних величин (міні метеостанціях, механізмах контролю рівня води, газу тощо), мульти-тестерах та контролерах управління приладами (роботами, іграшками), системах «Розумний будинок» і навіть квадрокоптерах. Модуль Arduino поєднує комп'ютерне середовище, мову програмування та спеціальні плати з незалежно програмованими інструментами. Плата Arduino є таким собі мікроконтролером, який приймає сигнали із зовнішнього середовища та передає

їх на безпосередньо задіяні програмовані пристрої. При цьому до дрібниць продуманого корпусу включено все необхідне для роботи мікропроцесора Arduino.

Роботу апаратної частини Arduino забезпечує її програмна частина, яка може бути реалізована засобами того чи іншого інтегрованого середовища розробки (Integrated Development Environment, IDE). Програмний код (скетч) формує характер поведінки певного програмованого модуля (набору елементів на макетній платі). Arduino працює з різними операційними системами і здебільшого використовує для розробки мову програмування C [1]. Найбільш поширеними програмними засобами для Arduino нині є середовища PlatformIO, Arduino IDE, Visual Studio Code, Mbed OS.

Arduino IDE є кросплатформним інтегрованим середовищем розробки з відкритим кодом, яке офіційно пропонується компанією Arduino (https://www.arduino.cc/en/software) як редактор коду, компілятор і модуль передачі прошивки в плату. Це IDE використовується для написання та завантаження програм на Arduino-сумісні плати, але може використовуватися і з ядрами сторонніх виробників для створення плат розробки інших виробників. Програми, написані засобами Arduino IDE, називають скетчами і зберігають з розширенням .ino. Arduino IDE підтримує мови C і C++, використовуючи спеціальні правила структурування коду. Код, написаний користувачем, поєднує дві основні програмні складові для виконання скетчу: void setup() та основний цикл програми void loop() [2]. По суті, це IDE виглядає як простий текстовий редактор, що зручно і зрозуміло для новачків у програмуванні [3].

PlatformIO – ще український проєкт, якмй підтримує не тільки Arduino, а й інші мікроконтролерні платформи [4]. Це популярне IDE надає широкі можливості для роботи з бібліотеками та іншими інструментами розробки. Порівняно з Arduino IDE, безкоштовна версія PlatformIO має численні переваги, серед яких:

- зручна робота з файловою структурою проєкту;
- сучасний, інтелектуальний редактор коду;
- можливість використання широкого набору плагінів для базової IDE, наприклад, плагін для GIT чи то інших систем контролю версій;
- зручна робота з проєктами загалом: можна відкривати водночас кілька проєктів в одному workspace;
- набагато зручніший і функціональніший менеджер бібліотек;
- зручний оброблювач помилок компіляції, в якому перехід до потрібних файлів і рядків відбувається в один клік.

Visual Studio Code – популярний текстовий редактор від Microsoft, який можна використовувати для роботи з Arduino через відповідне розширення. Це сучасний редактор коду з широким функціоналом [5]:

- IntelliSense та підсвічування синтаксису у скетчах Arduino;
- перевірка і завантаження скетчів у Visual Studio Code;
- вбудований менеджер плати та бібліотеки;
- вбудований список прикладів;
- вбудований серійний монітор;
- сніпети скетчів;
- автоматичний скаффолдинг проєктів Arduino;
- об'єднання часто використовуваних команд Command Palette (F1);
- інтегроване налагодження Arduino.

Зрештою, не має значення, яку IDE використовувати, адже код Arduino працюватиме однаково. Вибір IDE залежить від уподобань розробника щодо інтерфейсу програмування Arduino. Важливо, що основна мова залишається незмінною, все програмне забезпечення, необхідне для програмування в Arduino, надається Arduino безкоштовно і воно з відкритим кодом. Завдяки цьому Arduino відкриває доступ до мікроконтролерної розробки для початківців. Платформа Arduino надає можливість навчати програмуванню та робототехніці, створювати різноманітні пристрої та системи. Arduino використовується в освіті, наукових дослідженнях, робототехніці, IoT проєктах та багатьох інших галузях. Завдяки активній спільноті і великій кількості розширень та бібліотек, Arduino надає широкі можливості для створення різноманітних проєктів. Нині платформа продовжує залучати нових користувачів і сприяти інноваціям в світі електроніки та програмування.

Список використаних джерел:

1. Arduino Software. URL: https://www.arduino.cc/en/software.
2. Деміен А. Arduino IDE, встановіть це середовище розробки для роботи з Arduino. URL: https://ubunlog.com/uk/Середовище-розробки-arduino-ide-для-роботи-з-arduino/#google_vignette.
3. Which Arduino IDE Should I Use? URL: https://www.programmingelectronics.com/arduino-ides/
4. PlatformIO. Frameworks. Arduino. URL: https://docs.platformio.org/en/stable/frameworks/arduino.html
5. Visual Studio Code extension for Arduino. URL: https://marketplace.visualstudio.com/items?itemName=vsciot-vscode.vscode-arduino

Ключові слова: Arduino, PlatformIO, Arduino IDE.
Keywords: Arduino, PlatformIO, Arduino IDE.

Науковий керівник: к. ю. н., доцент Трофименко О.Г.

ПРОЕКТИ ОБРОБКИ ВІЗУАЛЬНИХ ДАНИХ

Пучков Владислав

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Кібербезпека в сучасному світі – це не лише питання захисту від кібератак, але й забезпечення конфіденційності інформації. Технології обробки візуальних даних виявляються невід'ємною складовою цього завдання. З їхньою допомогою розпізнавання облич, аналізу сцен та класифікації візуального контенту, можемо удосконалити моніторинг і виявлення загроз.

Проекти обробки візуальних даних мають широкий спектр застосувань. Вони допомагають автоматизувати процеси, підвищують безпеку, збагачують користувацький досвід та знаходять застосування в військової справі, медицині, науці, медіа, рекламі та багатьох інших галузях. Автоматичне розпізнавання об'єктів, аналіз сцен та класифікація зображень відкривають нові горизонти для інновацій та поліпшень.

Таки проекти обробки візуальних даних часто ґрунтуються на технологіях машинного та глибокого навчання. Глибокі нейронні мережі, такі як згорткові нейронні мережі (CNN), рекурентні нейронні мережі (RNN) та трансформери, стали важливими інструментами для аналізу та класифікації візуального контенту. Навчання моделей відбувається на величезних наборах даних, де алгоритми навчаються виявляти унікальні ознаки та закономірності.

Існує багато технологій в обробці візуальних даних. Найбільш поширеними є:

Глибоке навчання (Deep Learning):

Глибоке навчання є підгалуззю машинного навчання, яка використовує глибокі нейронні мережі для автоматичного вивчення представлень в даних. Для обробки візуальних даних, зазвичай використовуються сверточні нейронні мережі (CNN), які ефективно розпізнають взори та особливості на зображеннях. Глибоке навчання використовується для виявлення аномалій на візуальних даних, враховуючи складність структури та контексту відображення.[1]

Аналіз облич (Facial Recognition):

Аналіз облич полягає в розпізнаванні та ідентифікації осіб на зображеннях або відео. Для цього використовуються алгоритми глибокого навчання, які вивчають унікальні риси обличчя та структури для точного визначення особи. Аналіз обличчя використовується для контролю доступу, виявлення недозволених осіб та відслідковування осіб на відео чи зображеннях [2].

Класифікація зображень (Image Classification):

Це процес призначення зображенню або виділеним об'єктам на зображенні відповідної категорії чи класу. Глибокі нейронні мережі використовуються для вивчення різних патернів та ознак для ефективної класифікації. Класифікація зображень використовується для визначення небезпечних об'єктів або аномалій на візуальних даних, що сприяє ефективному виявленню потенційних загроз [3].

На основі розглянутих технологій обробки візуальних даних за допомогою методів машинного навчання створено багато проектів, як то:

OneDrive:

Мета проекту: Автоматизована класифікація та організація фотографій для поліпшеного пошуку та управління контентом.

Метод машинного навчання: Проект використовує глибокі нейронні мережі для навчання моделі, здатної розпізнавати об'єкти та сцени на зображеннях. Мережі навчаються на величезних наборах даних, які містять різноманітні зображення з мітками для навчання класифікації. OneDrive дозволяє автоматично присвоювати теги та категорії фотографіям, спрощуючи процес організації та управління вмістом для кінцевого користувача.

Apple Photos:

Мета проекту: Інтелектуальна організація фотоархіву, автоматичне розпізнавання об'єктів та облич.

Метод машинного навчання: У проекті використовуються згорткові нейронні мережі (CNN) для навчання моделі на великому обсязі даних, що включають фотографії з різними об'єктами, людьми та сценами. Навчання базується на мінімізації функції втрат, що дозволяє мережам виявляти унікальні ознаки. Apple Photos використовує цю модель для автоматичного розпізнавання облич, місць та об'єктів на фотографіях, підвищуючи зручність користувацького досвіду та забезпечуючи ефективну організацію фотоколекції.

Amazon Rekognition:

Мета проекту: Аналіз зображень та відео для розпізнавання об'єктів, сцен, облич і тексту.

Метод машинного навчання: Amazon Rekognition використовує глибокі нейронні мережі та методи навчання на мітках для класифікації об'єктів. Навчання проводиться на різноманітних наборах даних, що дозволяє моделі узагальнювати та ефективно працювати з різними типами візуального контенту. Система надає розробникам та бізнесам можливість створювати додатки, які можуть автоматично аналізувати та розуміти візуальний контент, що широко застосовується в рекламі, безпеці та інших областях.

Google Vision API:

Мета проекту: Аналіз зображень та відео для розпізнавання об'єктів, сцен, облич і тексту за допомогою інноваційних технологій від Google.

Метод машинного навчання: Google Vision API використовує глибокі нейронні мережі для розпізнавання та класифікації візуального контенту. Модель навчається на великому обсязі різноманітних даних, що дозволяє їй ефективно виявляти обличчя, об'єкти та інші елементи зображень.

Зачем це потрібно: Google Vision API дозволяє розробникам та підприємствам легко інтегрувати розширені можливості розпізнавання візуального контенту у свої додатки. Це широко використовується в рекламі, безпеці, медіа та інших галузях, щоб автоматизувати обробку зображень та поліпшити користувацький досвід.[4]

OpenCV (Open Source Computer Vision):

Мета проекту: Розробка відкритої та доступної бібліотеки для комп'ютерного зору з метою обробки та аналізу зображень та відео.

Застосування машинного навчання: OpenCV використовується для великого спектру завдань, від простого виявлення обличчя до більш складних задач, таких як відстеження об'єктів. Використання традиційних методів комп'ютерного зору та машинного навчання робить його універсальним інструментом для великої кількості додатків.

OpenCV дозволяє розробникам і дослідникам легко використовувати відкритий інструментарій для створення програм, які взаємодіють з візуальним контентом. Це включає в себе розпізнавання обличчя, виявлення об'єктів та реалізацію різноманітних алгоритмів комп'ютерного зору.

OpenCV відкриває можливості для реалізації проектів у сферах робототехніки, медицини, безпеки та багатьох інших галузях, де обробка візуальної інформації є важливою складовою [5].

Отже, у світі швидко зростаючих кіберзагроз та кількісного збільшення візуальних даних важливо розуміти, що технології обробки візуальної інформації стають помітною ланкою в забезпеченні кібербезпеки. Впровадження проектів, що використовують глибоке навчання для розпізнавання об'єктів, аналізу облич і класифікації зображень, дозволяє забезпечити не лише реактивний захист від потенційних загроз, але й активно виявляти аномалії та підвищувати загальний рівень кібербезпеки.

Проекти, такі як Google Vision API та OpenCV, є важливими кроками у напрямку розвитку інтелектуальних систем обробки візуальних даних. Їхнє використання дозволяє автоматизувати процеси аналізу, розпізнавання та класифікації, забезпечуючи ефективний захист від сучасних кіберзагроз.

З врахуванням тенденції зростання кількості візуальної інформації у всіх сферах, важливо продовжувати вдосконалювати та розвивати технології обробки візуальних даних. Це допоможе не лише ефективно захищати від

потенційних загроз, але й впроваджувати інновації, що полегшують повсякденне функціонування і підвищують рівень безпеки в цифровому світі.

Список використаних джерел:

1. Goodfellow, I., Bengio, Y., Courville, A. Deep Learning. MIT Press. URL: http://surl.li/nejgd
2. Можливості Face ID: ідентифікація облич за фото. URL: https://evergreens.com.ua/ua/articles/digital-facial-recognition.html
3. Deng, J., Dong, W., Socher, R., Li, L. J., Li, K., Li, F. F. ImageNet Large Scale Visual Recognition Challenge. URL: https://ieeexplore.ieee.org/document/5206848
4. Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., ... & Rabinovich, A. Going deeper with convolutions. In Proceedings of the IEEE conference on computer vision and pattern recognition. URL: https://ieeexplore.ieee.org/document/7298594
5. Google Cloud. Google Cloud Vision API. URL: https://cloud.google.com/vision
6. OpenCV. Open Source Computer Vision Library. URL: https://opencv.org/

Ключові слова: Технології обробки візуальних даних, кібербезпека, розпізнавання облич, глибоке навчання, класифікація зображень
Keywords: Visual data processing technologies, cyber security, face recognition, deep learning, image classification

Науковий керівник: к.пед.н., доцент Логінова Н.І.

РОЛЬ СИСТЕМНОГО АНАЛІЗУ В РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Ревацький Олександр

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Системний аналіз – це процес вивчення, розуміння і оцінки складних систем з метою розробки або поліпшення цих систем. Він використовується в багатьох галузях, включаючи інженерію, менеджмент, інформаційні технології та інші, для розгляду систем з різних точок зору і забезпечення їхнього оптимального функціонування [1, 2].

Саме системний аналіз відіграє ключову роль у визначенні мети та обсягу програмного забезпечення (ПЗ), визначаючи, що система повинна виконувати та які функції на неї покладаються. Це допомагає визначити, що ПЗ відповідає потребам користувачів. Системний аналіз визначає мету та обсяг ПЗ. Мета ПЗ визначає його загальні цілі, як то автоматизація певних процесів, поліпшення ефективності роботи, забезпечення точної інформації або зростання прибутків. Обсяг ПЗ визначається його функціональними можливостями і функціями. Він охоплює всі модулі, компоненти та функції, які вхо-

дять до складу програми. Вибір обсягу ПЗ може залежати від розміру проекту, доступних ресурсів, часових обмежень та інших факторів. Розробка ПЗ включає наступні етапи [3]:

- збір та аналіз вимог;
- визначення мети та цілей;
- створення специфікацій;
- обговорення з партнерами;
- уточнення ітерацій.

Збір і аналіз вимог ПЗ – це важливий процес у розробці програм, який передбачає визначення, збір та детальний аналіз потреб користувачів для розробки програмного продукту, який відповідає їхнім очікуванням та вимогам. Цей процес можна розділити:

1. Збір вимог:
- ідентифікація зацікавлених сторін;
- спільна робота з користувачами;
- опис вимог;
- визначення пріоритетів.

2. Аналіз вимог:
- специфікація вимог;
- визначення ризиків;
- затвердження вимог;
- управління змінами;
- завдання та планування розробки;
- валідація вимог;
- оновлення документації вимог.

Загалом, збір та аналіз вимог вважається фундаментальним етапом у розробці ПЗ, адже від правильності та повноти визначених вимог залежить успіх проекту.

Визначення мети та цілей ПЗ допомагають чітко визначити для чого створюється ПЗ та які завдання воно має вирішити. Мета визначає загальний напрямок розробки та використання ПЗ. Це може бути покращення ефективності бізнес-процесів, полегшення роботи користувачів, автоматизація конкретних функцій тощо. Цілі часто формуються конкретно та мають критерії оцінки, які дозволяють визначити, чи були вони досягнуті. Для правильного визначення мети та цілей ПЗ, важливо взяти до уваги потреби користувачів, бізнес-вимоги та інші фактори, які впливають на проект.

Специфікації визначають вимоги до програмного продукту, архітектурні особливості, функціональність, інтерфейси та інші характеристики. Це дозволяє уточнити, що саме має бути розроблено та забезпечити зрозумілість

для всіх клієнтів, розробників, тестувальників тощо. Даний етап складається з підетапів:

- технічна специфікація;
- функціональна специфікація;
- вимоги користувача;
- вимоги до продуктивності;
- безпека та захист;
- вимоги до документації.

Створення специфікацій допомагає забезпечити чіткість і цілісність вимог, полегшує співпрацю між різними командами та допомагає визначити, чи були вимоги виконані під час розробки та тестування.

Обговорення з партнерами – це вид процесу, при якому, обговорюються усі цілі партнерів щодо їхнього загального проекту, він має такі аспекти:

- уточнення вимог;
- узгодження плану проекту;
- звітність та зворотний зв'язок;
- управління ризиками;
- зміни в процесі;
- контроль якості;
- спільні цілі та інтереси;
- документування.

Забезпечення ефективного обговорення з партнерами допомагає створити взаєморозуміння, зменшити ризики та покращити результати проекту. Комунікація та співпраця з партнерами є ключовими елементами успішної розробки ПЗ.

Ітерації представляють собою короткі цикли розробки, під час яких створюється, тестується та вдосконалюється функціональність програмного продукту. Уточнення ітерацій включає в себе наступні етапи:

- планування ітерації;
- оцінка завдань;
- складання плану ітерації;
- обговорення та затвердження;
- виконання ітерації;
- тестування та перевірка;
- демонстрація та оцінка;
- відгук і вдосконалення.

Уточнення ітерацій допомагає підвищити продуктивність та якість розробки, роблячи її більш прозорою та ефективною. Регулярні ітерації дозволяють швидко адаптуватися до змін у вимогах та вимагають активної комунікації в команді розробників і зі партнерами.

Отже, системний аналіз є фундаментом для успішного процесу розробки ПЗ. Він допомагає розробникам розуміти потреби партнерів, визначати мету та цілі, створювати специфікації та проектувати систему таким чином, щоб задовольняти вимогам якості та надійності. Управління процесом розробки та збір вимог є ключовими елементами системного аналізу, які сприяють створенню високоякісного програмного продукту, що буде відповідати потребам користувачів.

Список використаних джерел:

1. Прокопенко Т.О. Теорія систем і системний аналіз: навч. посіб. [Електронний ресурс] / Т.О.Прокопенко; М-во освіти і науки України: Черкас. держ. технол. ун-т. Черкаси: ЧДТУ, 2019. 139 с.
2. Проектування інформаційних систем: Загальні питання теорії проектування ІС (конспект лекцій) [Електронний ресурс]: навч. посіб. для студ. спеціальності 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського; уклад.: О. С. Коваленко, Л. М. Добровська. Електронні текстові дані (1 файл: 2,02 Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2020. 192с.
3. Цибульник С.О., Барандич К.С. Технології розроблення програмного забезпечення. Частина 1. Життєвий цикл програмного забезпечення: підручник. Київ : КПІ ім. Ігоря Сікорського, 2022. 270 с.

Ключові слова: системний аналіз, програмне забезпечення, етапи розробки, аналіз вимог
Keywords: system analysis, software, development stages, requirements analysis

Науковий керівник: к.пед.н., доцент Логінова Н.І.

ДИСТАНЦІЙНИЙ КОНТРОЛЬ СИСТЕМ ЕНЕРГОЗАБЕЗПЕЧЕННЯ СЕРВЕРНОГО ОБЛАДНАННЯ ЗА УМОВ ЗБОЇВ ЕНЕРГОПОСТАЧАННЯ

Пшеничний Євгеній

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Внаслідок бойових дій Україна зіткнулася з проблемою планових та позапланових відключень електроенергії. Досвід зими 2022 показує, що навіть планові відключення не завжди відбуваються за графіком і завжди є ймовірність непередбачуваного заздалегідь відключення електроенергії. Це може призвести до проблем у роботі комп'ютерних мереж і окремих робочих станцій організацій. Особливо гостро ця проблема стоїть для корпоративного обладнання, яке часто встановлюється в труднодоступних місцях.

Перебої у постачанні електроенергії ускладняють його обслуговування та контроль. Найбільш поширеними проблемами, пов'язаними з відключеннями електроенергії, є:

- Втрата даних: при раптовому вимкненні електроенергії сервер може не встигнути зберегти важливі дані.
- Пошкодження обладнання: тривала робота без електроенергії може призвести до пошкодження серверного обладнання.
- Порушення роботи мережі: відключення електроенергії може призвести до збоїв у роботі комп'ютерної мережі.

Ця проблема частково вирішується використанням блоків безперебійного живлення, стабілізаторів напруги, автономних джерел живлення та генераторів тощо. Однак, у більшості випадків контроль та робота такого обладнання здійснюється вручну. При цьому, як було зазначено вище, якщо для індивідуальних користувачів це цілком доступне рішення, то для промислового та корпоративного обладнання може бути проблема, оскільки зазвичай доводиться здійснювати нагляд та обслуговування великого парку обладнання. При цьому зазвичай фізичний доступ до цього парку ускладнений через його територіальну розподіленість, а найчастіше і фізичну важкодоступність. Також слід взяти до уваги, що перераховане вище обладнання через інтенсивну експлуатацію зазвичай втрачає свої штатні характеристики (наприклад, ємність та режими розрядки акумуляторів), що додає невизначеності в режими його експлуатації.

Сучасні пристрої безперебійного живлення (ПБЖ) мають можливість дистанційного керування. Ця можливість реалізується за допомогою протоколів RS-232, USB, Ethernet тощо. На рис. 1 показана задня панель ПБЖ Mustek PowerMust 600 USB, на якій видно інтерфейси USB (зайнятий сірим кабелем) та RS-232, які можуть використовуватися для керування та моніторингу ПБЖ. Ці інтерфейси вимагають використання спеціального програмного забезпечення (з'єднувальні кабелі та ПЗ зазвичай йдуть у комплекті), однак це завдання може бути вирішене використанням універсальних бібліотек мови Python.

Рис. 1 — Загальний вигляд інтерфейсів ПБЖ Mustek

Також сучасні комп'ютери мають ACPI-інтерфейс, який дозволяє отримувати інформацію про стан системи живлення. Ці можливості дозволяють розробити програмне забезпечення для дистанційного контролю систем енергозабезпечення серверного обладнання, що має суттєво полегшити та спростити контроль та обслуговування парку обладнання.

Запропонований програмний прототип для дистанційного контролю систем енергозабезпечення серверного обладнання реалізує наступні функції:

- Отримання інформації про стан батареї: відсоток заряду, час роботи від батареї, стан роботи (заряджається чи працює від мережі).
- Вмикання і вимикання приладів котрі живляться через ПБЖ.

Програма написана на мові Python і реалізована з використанням інтерфейсу командного рядка, при цьому дозволяє вбудувати її в існуючи системи керування парком або додатково реалізувати GUI або web-інтерфейси.

Програма дозволяє дистанційно контролювати стан доступного обладнання, а також включати та вимикати системи, які працюють від автономних джерел живлення. У перспективі існує можливість реалізації програми, що відстежує стан автономного джерела живлення та штатно відключає обладнання за низького рівня заряду батареї. Штатне відключення в критичних ситуаціях дозволить зберегти цілісність даних, уникнути збоїв і втрат інформації в роботі операційної системи та програмного забезпечення користувача і продовжить термін експлуатації апаратного забезпечення за рахунок штатного відключення та включення системи.

Таким чином використання технології EVM дозволить покращити та підвищити ефективність та безпеку технологій аналізу ШПЗ.

Список використаних джерел:

1. psutil · PyPI [Електронний ресурс]. – Режим доступу : https://pypi.org/project/psutil/ – Назва з екрана.
2. wakeonlan · PyPI [Електронний ресурс]. – Режим доступу : https://pypi.org/project/wakeonlan/ – Назва з екрана.
3. Wake-on-LAN protocol - Scaler Topics [Електронний ресурс]. – Режим доступу : https://www.scaler.com/topics/wake-on-lAN-protocol/ – Назва з екрана.

Ключові слова: відкрите програмне забезпечення, відкриті формати даних, відкриті протоколи взаємодії, загрози і ризики.
Keywords: open software, open data formats, open communication protocols, threats and risks.

Науковий керівник: к.т.н., доцент Бойко В.Д.

ЦИФРОВА ТРАНСФОРМАЦІЯ ОСВІТНЬОГО ПРОЦЕСУ В ЗВО ПІД ЧАС ВІЙНИ

Кульбабський Анатолій

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Реалії та виклики сьогодення зумовлюють об'єктивні зміни в сучасній українській освіті. За повномасштабної війни постало завдання мінімізувати вплив новітніх чинників і загроз, до яких належать повітряні тривоги, необхідність перебувати в укриттях, переорієнтація деяких ЗВО на пункти соціально-гуманітарної допомоги для внутрішньо переміщених осіб, специфічний психологічний стан людини під час війни, евакуація/міграція частини студентів і викладачів, мобілізація роботодавців, активне волонтерство учасників освітнього процесу тощо. Саме тому «функціонування системи освіти в умовах воєнного стану характеризується інтенсивним пошуком нових підходів до навчання, інноваційних форм організації освітнього процесу, ефективних педагогічних та інформаційних технологій» [5, с. 8].

Україні під час воєнного стану потрібно зреалізувати План дій із цифрової освіти, який затвердила Європейська комісія на 2021–2027 роки. У документі визначено два першочергові напрями діяльності: прискорення розвитку ефективних цифрових освітніх екосистем, що передбачає стратегічне планування цифрового потенціалу (інфраструктури, сучасних організаційних можливостей, створення інструментів і безпечних платформ (у т. ч. для учасників освітнього процесу з особливими потребами)); виформування цифрових умінь і компетентностей науково-педагогічних працівників і студентів [7]. У цьому аспекті активне впровадження інформаційно-комунікаційних технологій (далі – ІКТ) дає змогу вживати заходи щодо забезпечення життєдіяльності учасників освітнього процесу, а також уможливлює створення особливих умов навчання для тих бакалаврів/магістрантів, які перебувають у лавах ЗСУ або в підрозділах тероборони, займаються волонтерською діяльністю, тимчасово перебувають за кордоном (серед таких умов – узгодження індивідуального графіка навчання, надання академічної відпустки, продовження терміну складання сесії тощо). І найголовніше – ІКТ «забезпечують рівний доступ до навчання, створюють передумови для утримання студентів і педагогів у сфері впливу української системи освіти» [3, с. 17]. З цією метою МОН України з перших днів війни рекомендувало викладачам кафедр здійснювати дистанційне навчання здобувачів вищої освіти за допомогою засобів комунікації, вбудованих до системи управління навчанням, електронну пошту, месенджери (Viber, Telegram та ін.), форуми, чати, електронні відеоконференції (MS Teams, ZOOM, Google Meet, Skype та ін.), що засновані на викори-

станні засобів телекомунікації по аудіоканалах, відеоканалах і комп'ютерних мережах тощо [4]. Отож віртуальне освітнє середовище як сукупність засобів ІКТ супроводжує навчальний процес в очному, дистанційному або змішаному форматах за рішенням обласних військових адміністрацій.

Для створення віртуальної освітньої платформи (вона може бути частиною інформаційно-аналітичної системи – ІАС) необхідні такі компоненти: система управління навчанням; система дистанційного консультування здобувачів освіти; електронний навчальний контент; система контролю знань осіб, які навчаються; інституційний репозитарій наукової та навчально-методичної літератури. Використання в навчанні сучасних ІКТ є засобом, що дозволяє забезпечити індивідуалізацію навчання: здобувач не лише отримує нову інформацію, але також активно занурюється у контекст виконання поставлених завдань. ІКТ допомагають автоматизувати навчально-методичну діяльність, створити бази даних із дидактичним матеріалом.

Найважливішими складниками персоналізації навчання у вищій школі є обрання теми кваліфікаційного дослідження, наукового керівника, а також навчальних дисциплін вільного вибору студентів. Забезпечити право здобувачів освіти на індивідуальну освітню траєкторію можливо лише із застосуванням автоматизації цих процесів, з-поміж яких традиційними є: відправлення списку тем наукових робіт/назв вибіркових дисциплін у форматі PDF-файлів у месенджери Viber, Telegram, а також на персональну електронну адресу студента або використання Google Таблиць. Утім, на нашу думку, найефективнішим способом автоматизації обрання теми наукового дослідження та дисциплін вільного вибору є спеціалізований розділ на вебпорталі університету, факультету або кафедри.

Універсальним і найпоширенішим засобом для розв'язання навчальних і адміністративних завдань є застосунки Microsoft Office 365 – сукупність інформаційних технологій, що їх призначено для автоматизації діловодства (опрацювання текстових і табличних даних, офісної графіки, баз даних тощо), розміщення навчально-методичних комплексів дисциплін, методичних інструкцій, відеозаписів лекцій тощо. За допомогою корпоративного хмарного сервісу Microsoft Office 365 проводять ректорські наради, засідання Вченої та науково-технічної рад, засідання кафедр, відкриті лекції, захисти кваліфікаційних робіт і результатів виробничих практик, тестування та оцінювання знань і умінь студентів.

До електронних освітніх ресурсів уналежнюють комп'ютерні навчальні програми й автоматизовані освітні компоненти. Наприклад, у більшості українських ЗВО успішно функціонує сервер інформаційної підтримки освітніх компонент ОПП, створений на ґрунті вільно поширюваної системи дистанційного навчання Moodle (Modular Object-Oriented Dynamic Learning Environment)

– це безкоштовне «модульне об'єктно-орієнтоване динамічне навчальне середовище, яке називають також системою управління навчанням, системою управління курсами, віртуальним навчальним середовищем або платформою для навчання, яка надає викладачам, студентам та адміністраторам великий набір інструментів для комп'ютеризованого навчання, у тому числі дистанційного» [2]. Система підтримує основні стандарти електронного навчання: MS, AICC і SCORM. Підтримка xAPI (Tin-Can) здійснюється через плагін Logstore API. Важливо, що в Moodle можна створювати текстовий навчальний контент, завантажувати інтерактивні презентації, графічні зображення, відео- та аудіофайли, які були створені в інших застосунках, вести електронні журнали оцінювання навчальних досягнень студентів і відвідування занять. Для застосування інтерактивних матеріалів можна додавати навчальний контент із вебсервісу H5P [6], а також гіперпосилання, вбудовувати мультимедійні фрагменти. Окрім платформи Moodle, у навчальному процесі використовують також інші Web-орієнтовані системи для організації електронного навчання, наприклад, OLAT, Open Elms, ATutor, Dokeos, eFront, Tovuti, CourseLab та ін., які різняться функціональними можливостями, технічними параметрами, вартістю тощо.

Потужним інформаційно-цифровим інструментом є офіційний вебсайт ЗВО як «регламентований засіб комунікації, оскільки відправник контролює зміст повідомлень, які надають одержувачам. З іншого боку – сайт є своєрідним електронним довідником ЗВО, відкритою інформаційною системою, оскільки йому притаманні всі ознаки такої системи в класичному розумінні: наявність певного масиву документів, засобів інформаційного пошуку, техніко-технологічних засобів фіксування, зберігання та представлення інформації» [1, с. 34]. Зауважимо: нині є багато платформ і систем для створення освітніх вебпорталів, у т. ч. системи управління контентом (CMS) та фреймворки для веброзробки. Наприклад, офіційний вебсайт Національного університету «Одеська юридична академія» (далі – НУ «ОЮА») [https://www.onua.edu.ua/ua/] використовує систему CMS Joomla!, а його контент розміщений на умовах ліцензії Creative Commons Attribution 4.0 International. Інтерфейс відрізняється лаконічною структурою, зручною навігацією, оригінальним дизайном. Вебсайт, по-перше, уможливлює панорамне висвітлення діяльності ЗВО як українською, так і англійською мовами, групуючи інформаційні блоки у вигляді dropdown меню: «Про нас», «Наука», «Навчання», «Міжнародне співробітництво», «Вступнику», «Новини»; по-друге, створює для внутрішньої та зовнішньої цільової авдиторії умови для зворотного спілкування через оприлюднену контактну інформацію та соціальні мережі «Facebook», «Telegram», «Instagram» і на Youtube; по-третє, адаптована мобільна версія сайту робить його зручнішим і дієвішим: юзабіліті призводить як

до збільшення часу перебування користувачів на сайті, так і уважнішого перегляду ними інформації, завантаження файлів та стимулювання повторних відвідувань. В умовах війни вебсайт НУ «ОЮА» став особливо важливим інформаційним ресурсом та платформою для підтримки іміджу. Він не лише забезпечує неперервність освітнього процесу в режимах офлайн та онлайн, але також містить обширні колекції наукової та науково-методичної літератури в зручному електронному форматі (локальний репозитарій). Крім того, сприяє взаємодії між абітурієнтами, адміністрацією, викладачами і студентами в періоди, коли фізичний контакт обмежений або й неможливий. Визначальну місію в забезпеченні функціонування ІАС в умовах гібридної війни покладено на Центр кібербезпеки та інформаційних технологій НУ «ОЮА».

Список використаних джерел:

1. Божук Л. Сучасні інтернет-технології у формуванні іміджу закладів вищої освіти. Society. Document. Communication. 2019. Ed. 8. A series of «Historical science». P. 30–54. URL: https://bit.ly/4728v3X
2. Організація дистанційного навчання в Moodle. Освіта UA. URL: https://bit.ly/3ujzhGm
3. Освіта України в умовах воєнного стану : інформаційно-аналітичний збірник / МОНУ; Ін-т освітньої аналітики. К., 2022. 358 с. URL: https://bit.ly/3SIifMn
4. Рекомендації щодо організації поточного, семестрового контролю та атестації здобувачів освіти із застосуванням дистанційних технологій : Лист МОН України від 14.05.2020 р. № 1/9-249 URL: https://bit.ly/3QVJiT1
5. Рогова В. Інноваційна експериментальна діяльність у системі освіти України в умовах воєнного стану. Освіта України в умовах воєнного стану. Інноваційна та проєктна діяльність : наук. зб. К.-Чернівці : Букрек, 2022. 140 с.
6. Система управління навчанням Moodle. URL: www.moodle.org
7. Стратегія розвитку вищої освіти в Україні на 2022–2032 роки. URL: https://bit.ly/3z0mIie

Ключові слова: цифровізація, автоматизація, заклад вищої освіти, навчальний процес, інформаційно-комунікаційні технології.
Keywords: digitization, automation, higher education institution, educational process, information and communication technologies.

Науковий керівник: к.пед.н., доцент Логінова Н.І.

ЗАСТОСУВАННЯ МАТЕМАТИКИ В ПРОГРАМУВАННІ

Ковальський Олександр

студент 2-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Багатьом відомо, що математика грає ключову роль у розвитку та застосуванні програмування. Але мало з цих людей можуть одразу ж навести конкретні приклади застосування математики в програмуванні, коли їх про це питають. У спробі вирішити дану проблему був створений цей доклад.

Одним з популярних застосувань математики у програмуванні є функції активації в нейронних мережах. Ось приклади деяких з функцій та візуалізація їх роботи.

Припустимо, що:

s = [-2, 1, 6, 7, -3] - вектор вхідних сигналів

w = [-1, 3, -4, 4, 5] - вектор ваг

Обчислимо значення вихідного сигналу, а потім знайдемо значення функції активації цього сигналу.

$$\sum_{i=0} s_i * w_i = -2*(-1) + 1*3 + 6*(-4) + 7*4 + (-3)*5 = -8$$

1) ReLU (Rectified Linear Unit)

Формула функції: ReLU(x) = max(0, x)

ReLU(-8) = max(0, -8) = 0

Візуалізуємо отриманий результат.

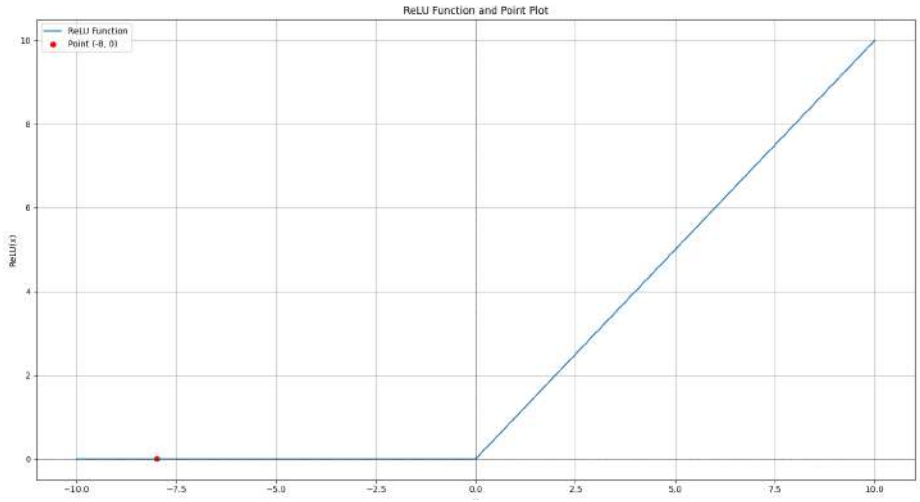


Рис. 1. Графік ReLU з точкою (-8, 0)

2) Сигмоїда

Формула функції: сигмоїда(x) = 1 / (1 + e-x)

сигмоїда(-8) = 1 / (1 + e-(-8)) ≈ 0.000335

Візуалізуємо отриманий результат:

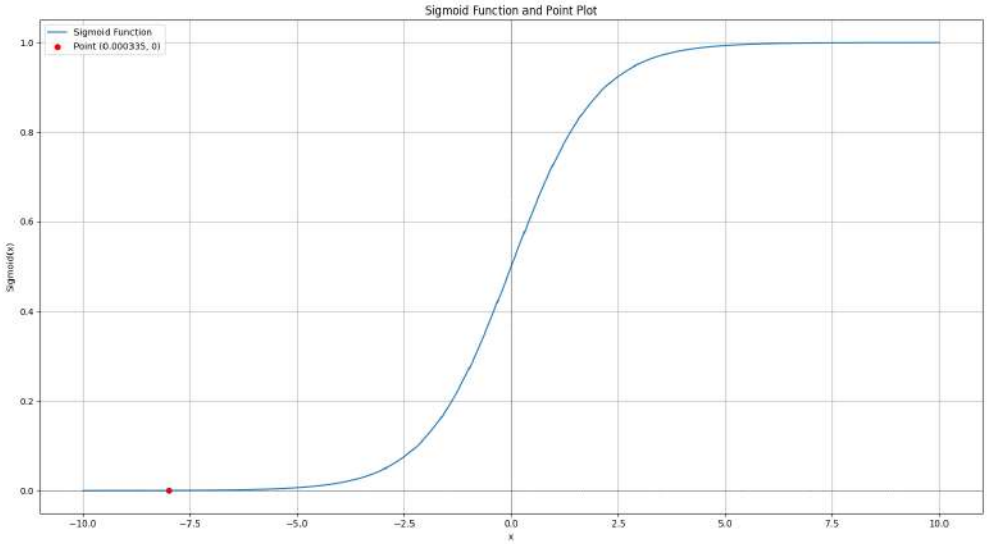


Рис. 2. Графік сигмоїди з точкою (-8, 0.000335)

3) tanh (Гіперболічний тангенс)

Формула функції: tanh(x) = (ex – e-x) / (ex + e-x)

tanh(-8) = (e-8 – e-(-8)) / (e-8 + e-(-8)) ≈ -0.99999977493

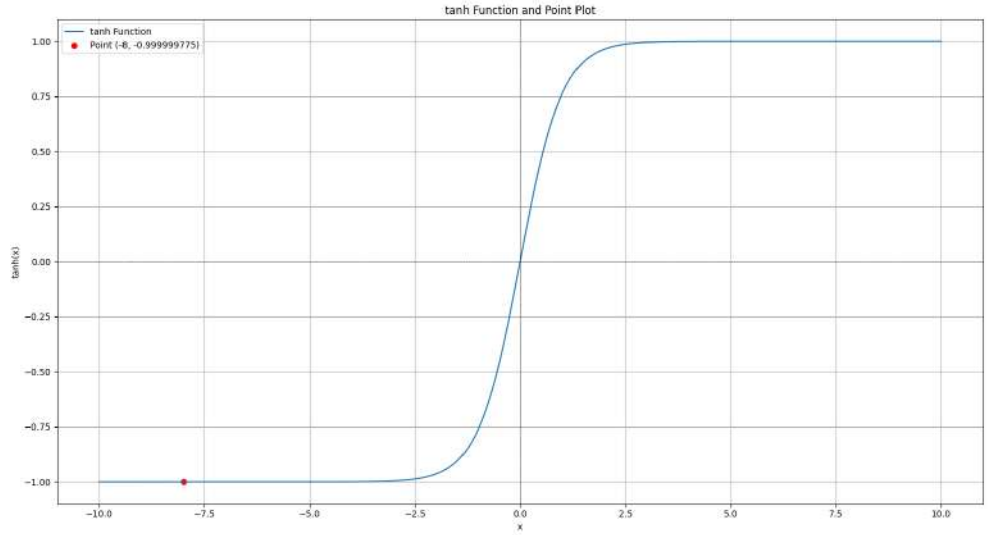


Рис. 3. Графік гіперболічного тангенсу з точкою (-8, -0.99999977493)

Окрім функцій активації математика також використовується у методі випадкових гіперплощин - один із способів локально-чутливого хешування. В цьому методі визначається певна кількість гіперплощин за допомогою нормальних векторів. Для хешування даних, які подають у вигляді координат точки у n-мірному, проводять скалярний добуток точки з кожним з наявних нормальних векторів.

Формульно це можна подати так:

(v, n), де (,) - операція скалярного добутку, v - радіус-вектор точки, що хешують, n - нормальний вектор площини.

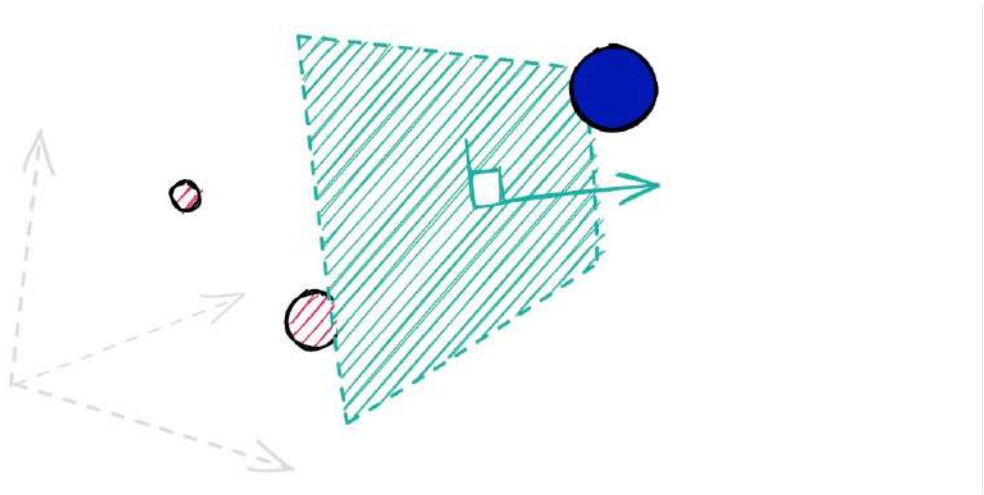


Рис. 4. Ілюстрація хешування випадковими гіперплощинами. Узято з джерела[1]

Висновок: Наведено конкретні приклади застосування математики в програмуванні, приклади супроводжено ілюстраціями та формулами з поясненням кожного елементу.

Список використаних джерел:

1. https://www.pinecone.io/learn/series/faiss/locality-sensitive-hashing-random-projection/

Ключові слова: функції активації, ReLU, сигмоїда, гіперболічний тангенс, нейронні мережі, хешування, локальність, гіперплощини
Keywords: activation functions, ReLU, sigmoid, hyberbolic tangent, neural networks, hashing, locality, hyperplanes

Науковий керівник: старший викладач Баландіна Н.М.

СТВОРЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗА ДОПОМОГОЮ AGILE

Гурін Євген

студент 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Одну з провідних ланок у методах сучасної розробки програмного забезпечення (ПЗ) займає метод Agile. Це підхід до розробки ПЗ, що базується на співпраці між командою розробників та клієнтом і ітеративному підході до процесу, тобто натомість довгого та неперервного процесу – циклічне поліпшення та доповнення вже готової окремої частини кінцевого проекту, який у процесі додається до інших таких частин [1]. Такі дії повторюються для усіх компонентів ПЗ, результатом яких є оновлення функціоналу продукту. Цей

підхід є одним із найпопулярніших у сучасному IT середовищі. Серед прихильників Agile знаходяться такі гіганти бізнесу, як Honda, Amazon, Google, Tesla та інші. Ці компанії розраховують на постійне оновлення та підтримку випущеного продукту, оцінку споживачів, циклічне тестування. Такий підхід обмежує жорсткий контроль та бюрократію у цьому питанні [2].

У аналогії з розробкою ПЗ, Agile має свої методології: SCRUM, Kanban, XP (Extreme Programming) та ін. Вони є найпопулярнішими у Agile.

Основна ідея методології SCRUM - це управління створенням будь-якого проекту поетапно одною, або декількома групами. Оптимальна кількість групи – від 5 до 8 розробників (у залежності від складності проекту). За весь процес створення, підтримки та адаптації продукту відповідають саме групи. Кожна частина проекту розробляється спринтами – ітерації фіксованого проміжку часу, які складають, у середньому, від 1 до 2 тижнів (у деяких випадках до 1 місяця). Головна ціль групи – реліз готової частини ПЗ у кожній такій ітерації. Процес не є лінійним, тому суворої послідовності розробки можна уникнути, і, у випадку необхідності, переходити до наступної частини, навіть якщо попередня ще не є завершеною [3].

Методологія Kanban представляє принцип еволюції розвитку процесу розробки шляхом багатьох невеликих поступових кроків, натомість одному великому. Такий підхід мінімізує ризик виникнення будь-яких небажаних ситуацій у проєкті. Найголовнішим кроком тут є візуалізація усіх складових проєкту: задачі, робочого процесу, проблеми та їх вирішення. Це зроблено у формі дошки, яка, умовно, складається з простої дощечки, карток, нотаток. Кожна картка представляє якусь задачу, причому вона може знаходитись у будь-якому стані: виконана, не виконана, у процесі, на опрацюванні тощо. Такий крок здається примітивним, але може вирішити багато важливих питань, наприклад – розподілення роботи, прозорість процесу, чітке представлення усього проекту. Після цього максимально зменшується кількість паралельних завдань, при цьому уся команда виконує одне завдання. Це зменшує багатозадачність, але кожна частина проекту виконується набагато швидше [4].

Методологія Extreme Programming є дещо складнішою, але не менш ефективною методика розробки. Екстремальне програмування ґрунтується на чотирьох базових процесах: кодуванні, тестуванні, дизайні та взаєморозумінні. Найбільша увага у Extreme Programming приділяється командній роботі та комунікації між розробниками і замовниками. Цій методиці властива філософія чіткості та прямолінійності, тобто визначаються чіткі побажання та завдання, відкидаються по максимуму усі їх розмитості, а якщо не вдається, то хоча б їх конкретизувати. Коли вже задачі точно описані, а документація го-

това, тоді клієнт дає згоду на початок роботи, у іншому випадку умови уточнюються [5].

Вибір методології треба обґрунтовувати на таких складових:

- бюджет;
- завдання, що поставлено групі;
- обсяг за об'ємом роботи проєкту;
- строки розробки та релізу.

Методологія SCRUM підходить для малого, або середнього за обсягом проєкту, який треба розробити з нуля швидко і без зайвих витрат, випускаючи окремі частини регулярно, орієнтовно раз в місяць. Але є одна деталь - кошти можуть бути невеликими за обсягом, але обов'язково мають надходити регулярно. Найкращим варіантом є фінансування кожної частини проекту, як окремої роботи.

Методологія Kanban підходить для малих, або середніх за обсягом проєктів, але вже не для розробки з нуля, а швидкого та ефективного вдосконалення готового або напівготового продукту. Ця методологія може бути використана для початкового етапу розробки.

Методологія Extreme Programming доцільно використовувати в проектах середнього та великого об'єму, які необхідно розробити з «повного нуля». У цьому випадку релізи відбуваються регулярно і не раніше за 2 місяця, але не більше за 6 місяців. Extreme Programming орієнтована на більш велике фінансування, не обов'язково регулярне, адже розробка займає багато часу, під час якого вона виконується поступово. Важливою деталлю є те, що Extreme Programming підходить тільки для галузі інформаційних технологій, що відрізняє цю методику від інших, що походить від Agile.

Висновки

У питанні строків виконання SCRUM та Kanban дещо схожі: чим швидше, тим краще, але не виходячи за межі оптимального часу. Обидві методики орієнтуються на неперервність випуску продукту. Методологія Extreme Programming більш м'яка у питанні часу: немає такого гострого принципу «чим швидше, тим краще», але терміни виконання від цього аж ніскільки не стають менш значимими. Такої гострої необхідності у регулярному фінансуванні, як у методології SCRUM та Kanban не передбачається, але його нестача може погано відобразитись на етапах розробки. Extreme Programming у свою чергу зберігає золоту середину у питанні фінансування, але з важливою умовою: замовник не має просто оплатити проект, та чекати на його реліз; він має стати повноцінним членом команди, який, за необхідності, має консультувати команду розробників у вимогах та приймати участь у проектуванні самого ПЗ.

Метод Agile швидко витіснив традиційний «метод водоспаду» через свою практичність та ефективність, але є декілька нюансів під час розробки саме за допомогою Agile. Його не слід використовувати у проектах, де вимагається сувора підзвітність: точно встановити кінцеві строки виконання проекту та необхідний бюджет, використовуючи Agile, - неможливо. Але для проектів малого та середнього розміру Agile буде найкращим варіантом, навіть у найгіршому випадку розвитку подій. Водночас із цього випливає недолік: чим більше проект, тим менше клієнт буде зацікавлений у фінансуванні та очікуванні. При цьому точних строків виконання та необхідних коштів замовнику розробники не зможуть визначити. Також серед недоліків можна виокремити те, що сам клієнт, або його представник, має контактувати з групою розробників [6].

Важливо зазначити, що метод Agile не зможе на 100% підійти для теперішніх умов в Україні. Це обумовлене тим, що майже 40% компаній є аутсорсинговими. Це у свою чергу дуже ускладнює роботу в команді, а тим більше комунікацію безпосередньо із замовником. Також від цього страждає прозорість усього процесу, адже виявити недоліки буде складніше, а приховати їх несумлінним розробникам ПЗ значно легше [7].

Список використаних джерел:

1. Ітеративна модель розробки. [Електронний ресурс]. URL: :https://dou.ua/lenta/articles/iterative-development-model/.
2. Agile в дії. [Електронний ресурс]. URL: https://mind.ua/publications/20178767.
3. Скрам. [Електронний ресурс]. URL: https://brainrain.com.ua/uk/scrum-upravlinnya-proektom/.
4. Канбан. [Електронний ресурс]. URL: https://www.ukraine.com.ua/blog/interesting/chto-takoe-kanban.html.
5. XP. [Електронний ресурс]. URL: https://worksection.com/ua/blog/extreme-programming.html.
6. Переваги та недоліки Agile. [Електронний ресурс]. URL: https://uk.itpedia.nl/2018/05/03/voor-en-nadelen-van-8-bekende-project-management-methodes/.
7. Ситуація в Україні. [Електронний ресурс]. URL: https://dou.ua/lenta/articles/specifics-of-product-companies-2023/.

Ключові слова: Agile, SCRUM, Kanban, XP.
Keywords: Agile, SCRUM, Kanban, XP.

Науковий керівник: к.т.н., доцент Задерейко О.В.

ШТУЧНИЙ ІНТЕЛЕКТ У ВЕБРОЗРОБЦІ: РЕВОЛЮЦІЯ ПЕРСОНАЛІЗАЦІЇ КОРИСТУВАЧА

Дика Анастасія

асистент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Максименко Артем

студент 2-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Штучний інтелект (ШІ) наразі все ширше використовують для поліпшення функціональності та користувацького досвіду в інтернет-просторі. Ця технологія революціонізує спосіб класичної веброзробки щодо проєктування та підтримки вебсайтів та вебзастосунків. ШІ грає важливу роль у покращенні користувацького досвіду на вебсайтах та додатках.

Досвід користування (User Experience, UX) – це те, що відчуває користувач, коли він підключається, наприклад, до вебсайту, програми чи то гаджета. Згідно з дослідженням компанії Imaginovation [1] практично 88% користувачів мають меншу ймовірність повернутися на сайт після свого поганого досвіду. Відтак UX є важливим показником, хоча при цьому багато хто його недооцінює.

Через швидкий розвиток ШІ та інновацій у галузі веброзробки постійно з'являються нові підходи до формування чудового UX. Алгоритми машинного навчання можуть аналізувати дані про користувачів та надавати їм персоналізований контент і таргетовану рекламу. Наприклад, інтернет-магазини використовують ШІ для рекомендацій товарів, на основі історії покупок певного користувача та аналізі його попередньої взаємодії із сайтом. Такий підхід покращує рівень задоволеності користувачів і підвищують рівень конверсії. Так, система рекомендацій Amazon аналізує історію покупок користувачів і вебперегляду, щоб надати покупцям персоналізовані пропозиції товарів. Потокові сервіси (наприклад, Spotify) теж видають рекомендації на основі їхніх попередніх дій. Такі інструменти, як Drift і Netflix, використовують ШІ для кращого обслуговування клієнтів, формування пропозицій та рекомендацій на базі запитів користувачів, їхніх уподобань і відгуків [2].

Персоналізований досвід користувача можна формувати для сотень тисяч окремих користувачів, використовуючи динамічну персоналізацію вмісту засобами ШІ. Опираючись на дані з різних джерел, штучний інтелект може визначати, де перебуває потенційний споживач, дізнаватися його поведінку та розробляти маркетингові стратегії з персоналізованим вмістом [3]. Наприклад, платформа для залучення клієнтів Braze, покладаючись на ШІ, допомагає веброзробникам створювати взаємодію, орієнтовану на користу-

вача, що сприяє розширенню цільової аудиторії. Інструменти Crystal, завдяки ШІ, аналізують дані користувачів через їхні профілі у соціальних мереж, електронну пошту та інші джерела для створення точних і детальних персонажів. Це дає змогу створювати персоналізовані, ефективні підходи до залучення і взаємодії з потенційним клієнтом. Інструменти Hotjar та Google Analytics за допомогою алгоритмів ШІ аналізують дані поведінки користувачів задля виявлення проблемних місць вебінтерфейсу та закономірностей, які можуть стати базисом для прийняття дизайнерських рішень.

Для численних інтернет-груп, розділених по регіонах і особистісних уподобаннях, процес персоналізації є нетривіальною задачею. Застосування алгоритмів ШІ дозволяє мінімально можливими зусиллями для розв'язання таких складних задач персоналізувати вигляд вебсторінки інтернет-магазину для різних груп покупців, використовуючи їхню геолокацію і відстеження їхніх купівельних звичок, пропонуючи інтерфейс, який з великою ймовірністю сподобається користувачеві. Це не лише сприяє популяризації сайту (самооптимізації), а й підвищує коефіцієнт конверсії вебмагазину (CRO) та формує стійку ідентичність бренду на ринку. Так, один з найбільших виробників брендового одягу та косметики Asos з'ясував, що 43% покупців використовують функцію збережених товарів у категорії «обране» і в такий спосіб зберігають від 50 до 500 позицій у своєму профілі як потенційні покупки. Бренд організував сортування та розподіл цих товарів по категоріях, додавши функцію Boards (дошки). Тим самим виробник бачить товари, які найбільш цікавлять потенційних покупців.

Розробка персоналізованих вебсайтів за допомогою ШІ є актуальним інноваційним напрямком у сфері веброзробки. Цей підхід дозволяє створювати вебсайти, які індивідуально відповідають потребам та очікуванням кожного користувача. ШІ має потенціал для значного покращення досвіду користувача. Наприклад, у майбутньому ШІ може бути використаний для прогнозування потреб користувачів, щоб завчасно пропонувати їм контент та функціонал, ще до усвідомлення ними своїх бажань. ШІ може використовуватися для генерації різнорідного контенту: тексту, зображень, відео [4]. Усе це разом може призвести до створення більш персоналізованих, ефективних та інтуїтивних вебдосвідів для користувачів. З розвитком ШІ вебсайти матимуть змогу адаптуватися до потреб кожного, щоб краще задовольняти очікування.

Однак, разом розширенням можливостей ШІ, все гостріше постають етичні питання щодо порушення приватності користувачів, забезпечення безпеки та конфіденційності персональних даних, які використовуються при створенні персоналізованого досвіду. Іншою проблемою є «бульбашка фільтрів», коли алгоритми створюють персоналізовані контентові фільтри, які обмежують доступ користувачів до всебічної інформації. Це може призвести

до формування обмеженого сприйняття світу та збільшення ехокамер, де користувачі бачать лише те, що відповідає їхнім власним поглядам. Для подолання подібних проблем важливо розвивати ефективні алгоритми регулювання та контролю користувачами того, якою інформацією вони свідомо діляться із системою. Транспарентність та відкритість використання ШІ можуть забезпечити більше довіри з боку користувачів.

Список використаних джерел:

1. 27 Eye-Opening Statistics About User Experience, Website First Impressions, and Website Design That You Should Be Taking Very Seriously. URL: https://www.sweor.com/firstimpressions.
2. How Artificial Intelligence is Impacting the Web Development? URL: https://cutt.ly/xwTJfjZp.
3. Li J., Cao H., Lin L., Hou Y., Zhu R., Ali A. User Experience Design Professionals' Perceptions of Generative Artificial Intelligence. 2023. Vol. 1. P. 1-25. DOI: 10.48550/arXiv.2309.15237. URL: https://arxiv.org/ftp/arxiv/papers/2309/2309.15237.pdf
4. Wu S., Yang W., Amin M., Kang B., Xu G. Assessment of the Influence of Interaction and Recommendation Approaches on the Formation of Information Filter Bubbles. Knowledge Management and Acquisition for Intelligent Systems. 2023. Vol. 14317. P. 98-110. DOI: 10.1007/978-981-99-7855-7_8.

Ключові слова: штучний інтелект, веброзробка, персоналізація користувача, досвід користувача.
Keywords: artificial intelligence, web development, user personalization, user experience.

Науковий керівник: к.т.н., доцент Трофименко О. Г.

РЕАЛІЗАЦІЯ АЛГОРИТМІВ MACHINE LEARNING У БАЗАХ ДАНИХ СІМЕЙСТВА NOSQL

Лобода Юлія

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат педагогічних наук, доцент

Бази даних NoSQL набули значного поширення в додатках машинного навчання та обробки даних завдяки своїй здатності обробляти великі обсяги різноманітних та неструктурованих даних. Ось кілька ключових випадків використання баз даних NoSQL.

1. Аналітика в реальному часі. Бази даних NoSQL використовуються для обробки потокових даних у реальному часі, що дозволяє практично миттєво аналізувати та приймати рішення у таких додатках, як виявлення шахрайства, обробка даних датчиків та аналіз потоку відвідувань.

2. Зберігання даних машинного навчання. Бази даних NoSQL надають масштабоване та гнучке рішення для зберігання даних навчання та виведення у робочих процесах машинного навчання. Вони можуть обробляти великі набори даних, підтримувати паралельну обробку та легко інтегруватися з популярними платформами машинного навчання.

3. Обробка природної мови. Програми обробки природної мови працюють з неструктурованими текстовими даними, такими як повідомлення в соціальних мережах, статті та відгуки клієнтів. Сховища документів NoSQL забезпечують ефективне зберігання, вилучення та індексацію текстових даних, полегшуючи виконання завдань, таких як аналіз настроїв, розпізнавання сутностей та тематичне моделювання.

4. Інтернет речей (IoT). Інтернет речей генерує величезні обсяги даних датчиків, часто у форматі часових рядів. Бази даних NoSQL, особливо сховища сімейств стовпців, добре підходять для зберігання, запиту та аналізу даних часових рядів, забезпечуючи ефективне керування даними Інтернету речей та моніторинг у реальному часі.

5. Рекомендаційні системи. Графові бази даних підходять для моделювання та аналізу складних взаємозв'язків, що робить їх ідеальними для рекомендаційних систем. Вони можуть ефективно представляти взаємодію користувача з елементами, обчислювати показники подібності та генерувати персональні рекомендації.

Одним із прикладів реалізації алгоритмів машинного навчання у базах даних сімейства Nosql є база даних Redis, яка забезпечує швидке створення, навчання і розгортання моделей машинного навчання. Redis – це сховище структур даних у пам'яті з відкритим вихідним кодом, що використовується як база даних, кеш, брокер повідомлень і механізм потокової передачі. Однією з основних особливостей Redis є підтримка різних структур даних, таких як рядки, відсортовані набори, растрові зображення, геопросторові індекси, гіперлоги та багато іншого [1].

У Redis також є вбудована реплікація, транзакції та різні рівні збереження на диску. Для досягнення максимальної продуктивності Redis працює із набором даних у пам'яті. Залежно від варіанта використання Redis може зберігати ваші дані шляхом періодичного скидання набору даних на диск, або шляхом додавання кожної команди в дисковий журнал.

Ось деякі з основних переваг Redis:

– автоматичний процес аварійного перемикання;

– Redis-ML – модуль, що реалізує різні моделі машинного навчання у вигляді вбудованих типів даних Redis;

– різноманітність структур даних, таких як рядки, списки, набори, хеші, растрові зображення, потоки та багато іншого;

– спрощує написання складного коду з меншою кількістю простих рядків.

RedisML – це модуль Redis, що реалізує кілька моделей машинного навчання як типів даних Redis. Збережені моделі повністю працездатні та підтримують процес прогнозування та оцінки. RedisML це готове рішення для використання моделей машинного навчання у виробничому середовищі [2].

Основні моделі машинного навчання RedisML модуля Redis: класифікація та регресія ансамблів дерева рішень (випадкові ліси); лінійна регресія; логістична регресія; матричні операції.

Деякі матричні операції в інтерфейсі командного рядка Redis мають такий вигляд:

– множення матриць - ML.MATRIX.MULTIPLY matrix1 matrix2 product;
– додавання матриць - ML.MATRIX.ADD matrix1 matrix2 sum;
– масштабування матриці шляхом множення її елементів на скаляр - ML.MATRIX.SCALE key scalar.

Для швидкої обробки величезних обсягів різноманітних даних, що передаються на великій швидкості, та автоматизування прийнятих рішень, сучасним додаткам, керованим даними, потрібне машинне навчання. Виявлення шахрайства в іграх, у фінансових сервісах, торги в режимі реального часу, сфера реклами, підбір пар на сайтах знайомств, пошук попутників та багато іншого, здатність обробляти дані в режимі реального часу та прийняття рішень протягом кількох десятків мілісекунд має першорядне значення.

Машинне навчання у базі даних – це практика розробки та виконання завдань машинного навчання: дослідження та підготовка даних; алгоритми навчання; моделі оцінки, збереження та управління версіями; та обслуговування цих моделей – усередині бази даних, що містить дані.

Список використаних джерел:

1. Introduction to Redis. URL: https://redis.io/docs/about/
2. Amazon ElastiCache for Redis. URL: https://aws.amazon.com/elasticache/redis
3. Celesti A., Galletta A., Fazio M., "Improving Machine Learning Algorithm Processing Time in Tele-Rehabilization Through a NoSQL Graph Database Approach: A Preliminary Study,"2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 2020, p. 1-6, DOI: 10.1109/ISCC50000.2020.9219700.
4. Dive into Deep Learning. Aston Zhang, Zachary C. Lipton, Mu Li, Alexander J. Smola. Cambridge University Press; 1st edition (December 7, 2023), 574 p. URL: http://preview.d2l.ai/d2l-en.
5. NoSQL Data Modeling Patterns in Redis. URL: https://developer.redis.com/ebooks/8-nosql-data-modeling-patterns/

Ключові слова: машинне навчання, дані, бази даних, NoSQL, Redis, моделі.
Keywords: machine learning, data, databases, NoSQL, Redis, models.

ХАРАКТЕРИСТИКА ФРЕЙМВОРКІВ ДЛЯ КРОСПЛАТФОРМНОЇ РОЗРОБКИ

Касян Павло

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Кросплатформна розробка – це підхід у програмуванні, який дозволяє розробникам створювати додатки, сумісні з декількома операційними системами, використовуючи один і той же код. Цей метод розробки набирає популярності через свою ефективність та економію часу, оскільки він знижує необхідність писати окремий код для кожної платформи, таких як Android і iOS.

Однією з головних переваг кросплатформної розробки є зменшення витрат і ресурсів. Замість того, щоб мати окремі команди для розробки на різних платформах, компанії можуть скористатися однією командою, яка працює над єдиним кодовим базисом. Це також сприяє більшій консистенції та єдності досвіду користувачів на різних пристроях.

Ще однією ключовою перевагою є швидкість виходу на ринок. Завдяки тому, що розробники можуть одночасно розробляти додатки для різних платформ, час виходу продукту на ринок істотно скорочується. Це особливо важливо в сучасному світі, де швидкість реагування на ринкові зміни та потреби користувачів може мати значний вплив на успіх продукту.

Втім, існують певні виклики, пов'язані з кросплатформною розробкою. Один із них - це обмеження функціональності: не всі нативні можливості операційних систем можуть бути доступними або легко інтегрованими через кросплатформні технології. Також, додатки, розроблені з використанням цього підходу, іноді можуть поступатися в продуктивності нативним додаткам, які спеціально оптимізовані для кожної платформи.

З огляду на ці фактори, вибір між кросплатформною та нативною розробкою часто залежить від специфічних потреб та цілей проекту. Однак, з розвитком технологій, інструментів та фреймворків для кросплатформної розробки, якісний розрив між кросплатформними та нативними додатками зменшується, роблячи цей підхід все більш привабливим для широкого спектру проектів.

Продовжуючи розгляд теми кросплатформної розробки, важливо виділити роль JavaScript та фреймворку React Native у цій сфері. JavaScript, будучи однією з найпопулярніших мов програмування, відіграє ключову роль у розвитку кросплатформних технологій. Його гнучкість, широке використання та активна спільнота розробників забезпечують солідну базу для створення ефективних та інтерактивних додатків.

React Native, створений Facebook, є одним із провідних фреймворків у світі кросплатформної розробки. Використовуючи JavaScript, цей фреймворк дозволяє розробникам писати додатки, що надають майже нативний досвід користувачам на обох основних мобільних платформах - Android та iOS. React Native використовує декларативний підхід до програмування, який робить код більш зрозумілим та легким для тестування.

Однією з унікальних особливостей React Native є його можливість "гарячої" перезавантаження (hot reloading), яка дозволяє розробникам миттєво побачити зміни, внесені у код, без необхідності перезавантаження всього додатку. Це не тільки підвищує продуктивність розробки, але й значно спрощує процес тестування та налагодження.

React Native також сприяє модульності та повторному використанню коду. Компоненти, розроблені для одного проекту, можуть бути легко перенесені та адаптовані до іншого, зменшуючи загальні витрати часу та ресурсів на розробку. Це робить фреймворк ідеальним рішенням для стартапів та компаній, які прагнуть швидко вивести свій продукт на ринок.

Тим не менш, не можна ігнорувати певні виклики, пов'язані з React Native. Наприклад, хоча він пропонує широкі можливості для кросплатформної розробки, існують випадки, коли потрібно використовувати нативний код для оптимізації додатку під конкретну платформу. Це може вимагати додаткових знань в області нативної мобільної розробки.

Окрім того, важливо враховувати, що хоча React Native постійно розвивається, він все ще може зазнавати обмежень у порівнянні з чисто нативною розробкою, особливо у випадках, коли необхідно використовувати складні функції апаратного забезпечення або останні можливості платформи. Це вимагає від розробників постійно оновлювати свої знання та навички, щоб використовувати потенціал фреймворку на повну.

У підсумку, React Native відіграє значну роль у розвитку кросплатформної розробки, пропонуючи ефективний баланс між продуктивністю, якістю додатку та швидкістю виходу на ринок. Однак, як і будь-який інструмент, він має свої особливості та обмеження, які слід враховувати при виборі підходу до розробки конкретного додатку.

Прогресуючи у вивченні інструментів кросплатформної розробки, варто звернути увагу на інші значущі фреймворки та технології, які розширюють можливості розробників у цій сфері.

Flutter, розроблений Google, є ще одним популярним фреймворком для створення кросплатформних додатків. Він використовує мову програмування Dart, яка забезпечує високу продуктивність та ефективність. Особливістю Flutter є його використання власного віджет-базованого двигуна, що дозво-

ляє створювати дуже гладкі та візуально привабливі інтерфейси користувача.

Flutter пропонує високий рівень нативної інтеграції, забезпечуючи доступ до великої кількості функцій операційних систем. Це робить його привабливим для розробників, які прагнуть максимально наблизити досвід користувача кросплатформного додатку до нативного. Flutter також має активну спільноту і багатий набір готових компонентів, що значно спрощує процес розробки.

Xamarin, від Microsoft, є ще одним важливим гравцем у сфері кросплатформної розробки. Xamarin використовує C# та .NET для створення додатків для Android, iOS та Windows. Особливістю Xamarin є його здатність використовувати велику частину коду між платформами, що значно знижує час та зусилля, необхідні для розробки.

Xamarin забезпечує доступ до нативних API і інструментів кожної платформи, що дозволяє розробникам створювати високопродуктивні та нативно виглядаючи додатки. Він також інтегрований з Microsoft Visual Studio, що забезпечує розробникам потужне середовище для розробки.

Apache Cordova є відкритим фреймворком, який дозволяє розробникам створювати мобільні додатки, використовуючи HTML, CSS та JavaScript. Це відмінний вибір для веб-розробників, які хочуть перейти до мобільної розробки, використовуючи знайомі технології. Хоча додатки, створені за допомогою Cordova, можуть не завжди мати таку ж продуктивність, як нативні або інші кросплатформні рішення, вони забезпечують швидкий спосіб розробки для менш вимогливих додатків.

Кожен із цих фреймворків має свої унікальні переваги та обмеження, і вибір між ними залежить від конкретних потреб та вимог проекту. Важливо також розуміти, що ландшафт кросплатформної розробки постійно розвивається, тому розробникам слід залишатися в курсі останніх тенденцій та оновлень у цій галузі.

Список використаних джерел:

1. Огляд React Native для кросплатформної розробки. URL: https://reactnative.dev/docs/getting-started
2. Flutter: Повний посібник з кросплатформної розробки. URL: https://flutter.dev/docs
3. Розробка мобільних додатків з Xamarin. URL: https://docs.microsoft.com/en-us/xamarin/
4. Використання Apache Cordova для створення кросплатформних додатків. URL: https://cordova.apache.org/docs/en/latest/

Ключові слова: кросплатформна розробка, React Native, Flutter, Xamarin, Apache Cordova, мобільна розробка, вибір фреймворку, веб-технології.
Keywords: cross-platform development, React Native, Flutter, Xamarin, Apache Cordova, mobile development, framework selection, web technologies.

Науковий керівник: к.пед.н., доцент Лобода Ю.Г.

ВИКОРИСТАННЯ КОЛЕКЦІЇ TIDYVERSE В АНАЛІЗІ ДАНИХ

Сітько Анастасія

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Для аналізу даних в мові R використовується велика кількість пакетів, які розширюють функціонал. Один з них – tidyverse. Це набір пакетів з відкритим кодом, представлений Хедлі Вікхемом, які роблять аналіз даних більш ефективним, простим та зрозумілим [1]. Дана колекція пакетів працює лише з так званими “охайними даними” (tidy data). Концепція охайних даних передбачає зберігання даних в форматі, в якому:

- кожна змінна повинна міститись в окремому стовпчику;
- кожне спостереження повинне міститись в окремому рядку;
- кожне значення повинне міститись в окремій комірці [2].

Tidyverse складається з двох частин: ключові (ядро) та побічні пакети, які додатково розширюють функціонал мови R.

Ядро tidyverse складається з наступних пакетів:

- ggplot2 (використовується для візуалізації даних за допомогою графіків);
- dplyr (використовується для маніпуляцій з даними; наприклад, фільтрувати дані за певним критерієм, використовуючи функцію filter);
- tidyr (використовується для приведення даних до “охайного” вигляду);
- readr (використовується для зчитування та записування даних);
- purr (використовується для функціонального програмування);
- tibble (використовується для роботи з даними у вигляді tibble (розширена версія стандартного дата фрейму));
- stringr (використовується для роботи з текстом);
- forcats (використовується для роботи з факторами (тип даних для роботи з категоріальними змінними – змінними, які можуть приймати обмежену кількість значень і вказують на певну характеристику)).

Окрім ядра до tidyverse входять наступні пакети:

- vroom (швидке завантаження даних);

- DBI (робота з базами даних);
- haven (для SAS, Stata та SSPS даних);
- httr (робота з API) та інші.

Щоб встановити бібліотеку, потрібно ввести наступний код: *install.packeges("tideverse")*.

Для підключення даної бібліотеки використовується наступна команда: *library("tidyverse")*.

Tidyverse додає багато корисного та зрозумілого функціоналу в мову R. Підключення пакету дає можливість завантажувати файли з даними, які мають розширення .csv, .xls, .xslx та .tsv.

Файли типу .csv можна завантажити за допомогою стандартної команди read.csv(), але для великого об'єму даних краще використовувати команду read_csv() пакету readr, який є частиною ядра tidyverse. Для завантаження файлу можна використовувати шлях до локального файлу на комп'ютері або прямі посилання для завантаження:

```
#Завантаження файлу з робочої директорії
file1 <–read_csv("file.csv")
#Завантаження файлу за URL
file2 <– read_csv("https://github.com/tacookson/master/sakura-modern.csv")
```

Головна відмінність цієї команди від стандартної в тому, що read_csv записує дані відразу в формат tibble. Також аналогічною командою є vroom з однойменного пакету, яка виділяється значно вищою швидкістю завантаження даних:

```
#Завантаження файлу з робочої директорії
file1 <–vroom("file.csv")
#Завантаження файлу за URL
file2 <– vroom ("https://github.com/tacookson/master/sakura-modern.csv")
```

Також існує структура для завантаження відразу декількох файлів однакового формату. Команда dir(pattern =) отримує назви всіх файлів в даній директорії, які відповідають певному шаблону (pattern) [2]:

```
#Завантаження всіх .csv файлів в робочій директорії
files <dir(paterrn = "\\.csv$")
all_files <– vroom(files)
```

Також за допомогою пакету можна відкривати файли Excel. Для цього використовується пакет readxl та команда read_excel:

```
#Отримання всіх листів файлу
exel_sheets("file.xlsx")
#Зчитування даних з потрібного листа
file_data <–read_excel("file.xlsx , sheet = "SheetName"")
```

Для різноманітних маніпуляцій з даними використовується пакет dplyr. Приклад функцій пакету:

- glimpse(name) – перегляд структури тібблу name;
- filter(name, pattern) – фільтрація (відбір) значень тібблу name за критерієм pattern;
- slice(first:last) – відбір (зріз) значень від first елемента до last (наприклад, name %>% slice(4:9) – відбір з тібблу name рядків даних з четвертого до дев'ятого);
- arrange(colname) – відсортування даних тібблу за значеннями стовпця colname. За замовчуванням дані сортуються в зростаючому порядку (наприклад, name %>% arrange(desc(sum)) – сортування даних тібблу name за даними стовпця sum в спадаючому порядку);
- select(names) – відбір потрібних змінних датасету (наприклад, name %>% select(first, sum) – з тібблу name обираються тільки змінні (стовпці) first і sum);
- rename() – зміна назви змінної (наприклад, name %>% rename(f = first) – змінюємо назву змінної first тібблу name на f);
- mutate() – створення нового стовпчика та запис даних в нього (наприклад, name %>% mutate(newcol = first*second) – в тібблі name створюємо новий стовпець newcol, в який записуємо добуток значень стовпців first і second);
- group_by() – групування даних за змінною;
- summarise() – агрегація даних;
- count(col) – підрахунок кількості значень в стовпці (наприклад, name %>% count(first) – підраховуємо кількість значень в стовпці first тібблу name).

За допомогою пакету ggplot2 можна створювати різні графіки для візуалізації потрібних даних. Приклад функцій пакету [3, 4]:

- основні функції – ggplot, gplot та plot – всі три функції використовуються для побудови графіку, але відрізняються набором аргументів та даних;
- geom() – дана функція використовується для нанесення рисунків різних типів на графік (наприклад, geom_jitter – точкова діаграма, geom_boxplot – діаграма з боксплотами (ящики з вусами), geom_violin() – скрипкова діаграма);
- theme – дана функція відповідає за тему діаграми (тобто її зовнішній вигляд);
- ggtitle – дана функція відповідає за додавання написів для діаграми;
- color – зміна кольору діаграми або її частини.

Список використаних джерел

1. Tidyverse – Wikipedia. URL: https://en.wikipedia.org/wiki/Tidyverse .
2. Маніпуляція з даними за допомогою dplyr і не тільки r_econometricks.knit. URL: https://aranaur.github.io/r_econometrics/dplyr.html .
3. Create Elegant Data Visualisations Using the Grammar of Graphics ggplot2. URL: https://ggplot2.tidyverse.org/ .
4. Plot function – R Documentation. URL: https://www.rdocumentation.org/packages/graphics/versions/3.6.2/topics/plot .

Ключові слова: пакет, tidyverse, функція, датасет, тіббл.
Keywords: tidy data, package, tidyverse, function, dataset, tibble.

Науковий керівник: к.пед.н., доцент Лобода Ю.Г.

ВЕБРОЗРОБКА ЗАСОБАМИ ASP.NET CORE

Солом'яний Олексій

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Наразі веброзробка засобами стека технологій .NET набуває популярності у секторі високонавантажених застосунків для бізнес-сектору. З кожним роком вимоги користувачів до сайтів зростають, тим самим збільшується навантаження на сайти за кількістю запитів. Чим більше бізнес, тим швидше компанія стикається з проблемою великого навантаження на її вебресурси. Для розв'язування такого роду проблем варто або збільшувати ресурси сайту, або при розробці сайту використовувати технології, які дозволяють ефективно та гнучко проєктувати сервіси з великим навантаженням.

ASP.NET Core – технологія для розробки вебсайтів та вебзастосунків з великим навантаженням. З перших версій ця технологія проєктувалася під великі навантаження, тому весь код пишеться засобами асинхронного програмування [1].

Більшість застосунків на ASP.NET Core працюють за шаблоном MVC (Model-View-Controller) [2]. За цією моделлю кожен запит користувача проходить через 3 етапи: 1) етап Model формує дані, які користувач відправляє на бізнес-логіку сайту, а контролер передає їх далі на відображення; 2) View – це відображення інформації на сторінці, яку сайт обробив; 3) Controller – це етап оброблення даних, які надав користувач для взаємодії, далі вони переходять до моделі. Після цих етапів користувач отримує результат запиту, будь-то перехід за посиланням чи то заповнення форми замовлення або керування панеллю адміністратора на сайті. Поділ на три основні групи компо-

нентів (моделі, подання та контролери) дозволяє реалізувати принципи поділу завдань.

Перевагами ASP.NET Core є:

- кросплатформність: безперешкодне розгортання застосунків на різних операційних системах (Windows, Linux, MacOS) з оптимізацією та прямою підтримкою;
- висока швидкість та продуктивність забезпечується різними технологіями: JIT-компіляція дозволяє прискорити завантаження і виконання програми; кешування даних скорочує час доступу до них та покращує продуктивність програм; механізми оптимізації запитів до бази даних зменшують кількість звернень до бази даних та прискорюють виконання запитів; асинхронні операції обробки запитів ефективно впливають на використання ресурсів сервера і дозволяють обробляти запити одночасно; збирач сміття оптимізує і дозволяє знизити навантаження на систему, тим самим покращити продуктивність [3];
- можливість створення застосунків під різні патерни та архітектури: розробка проєкту створена за модульною системою, що дозволяє використовувати лише необхідні компоненти;
- вбудована система Dependency Injection: ця технологія спрощує роботи з залежностями у різних частинах коду та робить їх більш незалежними;
- сучасна архітектура та підтримка SignalR робить з'єднання клієнтської та серверної частини простішим, SignalR виступає обгорткою, яка забезпечує усі стандарти зв'язку server-client та сама вибирає, за яким стандартом буде здійснено зв'язок за мінімальний час та мінімальною кількістю ресурсів;
- масштабованість: у випадку, коли застосунок не справляється з навантаженням, то в ньому є можливість збільшення ресурсів. ASP.NET Core має інтегровану підтримку розробки API та мікросервісних програм, що дозволяє розробникам створювати масштабовані проєкти;
- тестування: для детальної перевірки коду за допомогою unit-тестів необхідно багато часу та ресурсів. Платформа ASP.NET Core підтримує інтеграційне тестування з використанням платформ модульного тестування та вбудованого вебсервера тестування (TestServer), який можна використовувати для обробки запитів без навантаження на мережу. Це дозволяє виконувати тести швидше, ніж під час роботи з реальними вебсерверами.

З іншого боку, сучасний фреймворк ASP.NET Core із багатьма новітніми концепціями та функціями може видатись складним для розробників, які не знайомі з ним. Розробка вебзастосунків засобами ASP.NET Core вимагає високого рівня кваліфікації програміста. Тому до певних недоліків ASP.NET Core

можна віднести: круту криву навчання, обмежену підтримку бібліотек, накладні витрати на продуктивність, складне розгортання, проблеми сумісності, обмежену підтримку Windows. До того ж хоча ASP.NET Core є безплатним з відкритим кодом, використання його у робочому середовищі може вимагати додаткових витрат на інструменти, інфраструктуру та інші ресурси [4].

Зважаючи на численні переваги та враховуючи певну специфіку розробки, можна сказати що ASP.NET Core має все необхідне для створення сучасних вебзастосунків з великим навантаженням. На сьогодні ASP.NET Core – це універсальна система веброзробки, яка має гарну підтримку спільноти розробників (https://github.com/aspnet, https://www.facebook.com/groups/2128178990740761/, https://github.com/dotnetcore, https://devblogs.microsoft.com/dotnet, https://dev.to/t/dotnet), яка постійно оновлює та покращує систему та підходи до розробки.

Список використаних джерел:

1. Overview of ASP.NET Core. URL: https://learn.microsoft.com/en-us/aspnet/core/introduction-to-aspnet-core?view=aspnetcore-8.0.
2. Overview of ASP.NET Core MVC. URL: https://learn.microsoft.com/en-us/aspnet/core/mvc/overview?view=aspnetcore-7.0.
3. Бондаренко С. Що таке ASP.NET? Принцип функціонування та моделі розробки. URL: https://highload.today/uk/shho-take-asp-net-printsip-funktsionuvannya-ta-modeli-rozrobki/
4. What are the disadvantages of ASP.NET Core?. URL: https://www.quora.com/What-are-the-disadvantages-of-ASP-NET-Core

Ключові слова: веброзробка, кросплатформність, ASP.NET Core, MVC.
Keywords: web development, cross-platform, ASP.NET Core, MVC.

Науковий керівник: к. ю. н., доцент Трофименко О.Г.

АНАЛІЗ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ УПРАВЛІННЯ

Фомічов Дмитро

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Ефективність роботи фахівців у різних галузях залежить від багатьох факторів, в тому числі й від автоматизації їхньої діяльності. Будь яка управлінська діяльність пов'язана з прийняттям рішень, яке складається зі збором, обробкою та накопиченням великих обсягів інформації, вивченням, селекцією та оцінкою даних. Ці значні обсяги інформації неможливо обробити без

сучасних інформаційних технологій, до яких відносяться інформаційно-аналітичні системи та системи підтримки прийняття рішень [1].

Інформаційно-аналітична система (АІС) – це автоматизована організаційно-технічна система, що реалізує технології накопичення, зберігання та обробки інформації з використанням технічних засобів обробки, програмного забезпечення, а також відповідних методів і процедур.

Основне призначення ІАС – забезпечення кращого доступу до інформації для прийняття рішень.

Функціями ІАС є:

- отримання даних з різних джерел, їх перетворення та завантаження;
- зберігання даних;
- оперативний та інтелектуальний аналіз даних;
- підготовка результатів аналізу даних для ефективного прийняття рішень користувачами.

Компоненти ІАС – апаратне та програмне забезпечення, бази даних, засоби зв'язку та інтернет, персонал та різні процедури.

До складу ІАС входять:

- сховища даних (Data Warehouse);
- вітрини даних (Data Marts);
- технологія OLTP (Online Transaction Processing), яка орієнтована на обробку транзакцій інформації та деталізовані дані;
- технологія OLAP (Online Analytical Processing), яка здійснює інтерактивну аналітичну обробку та орієнтована на роботу з агрегованими даними;
- технології Query and Reporting tools для створення запитів та звітів;
- технологія інтелектуальної обробки даних (Data Mining) для вирішення задач пошуку закономірностей у масивах даних.

Сховища даних – це великі загально корпоративні бази даних, які містять певну інформацію та забезпечують її оперативне представлення у формі, зручній для користувача або для подальшої обробки іншими аналітичними системами. Сховища даних побудовані з урахуванням структури та діяльності організації. Однак дані, що містяться в сховищах, як правило, недостатньо доступні для обробки в реальному часі, особливо при великих обсягах. Ця проблема вирішується на наступних рівнях ієрархії – на рівнях вітрин даних і OLAP-систем.

Вітрини даних є структурованими інформаційними масивами, але їхня відмінність від сховищ даних у тому, що вони більш предметно орієнтовані. Як правило, вітрини даних містять інформацію, пов'язану з певною предметною областю та особливостями діяльності організації. Тому інформація в вітринах даних зберігається в спеціальному вигляді, який найбільше підходить для ви-

рішення конкретних аналітичних завдань або обробки запитів певної групи аналітиків [2].

OLTP-системи – це системи операційної обробки даних. Їх структура розроблена для швидкого та ефективного виконання елементарних дій, з яких складаються різні операції. Таки системи працюють з оперативними (поточними) даними. OLTP-системи спрямовані на швидку обробку.

OLAP-системи – системи аналітичної обробки даних у реальному часі. Таки системи можуть забезпечувати вирішення багатьох аналітичних завдань, наприклад, аналіз ключових показників ефективності, маркетинговий, фінансово-економічний аналіз, сценарний аналіз, моделювання, прогнозування тощо. Вони можуть працювати з усіма необхідними даними, незалежно від характеристик інформаційна інфраструктура компанії. Особливістю OLAP-систем є багатовимірність зберігання даних (на відміну від реляційних таблиць), а також попередній розрахунок агрегованих значень. Це дає користувачеві можливість будувати оперативні спеціальні запити даних, використовуючи кілька аналітичних напрямків. Крім того, для OLAP-систем характерна предметно-орієнтована (а не технічна) структура інформації, що дозволяє користувачеві оперувати звичними категоріями та поняттями [3].

Інструменти запитів і звітів забезпечують побудову запитів до ІАС з можливою інтеграцією даних з різних джерел, а також перегляд інформації з можливістю її деталізації та агрегації, формування та друку звітів. Зазвичай модулі, що містять функції генерації запитів і генерації звітів, є частиною багатьох OLAP-систем, хоча існують окремі програмні продукти цього класу.

Технологія інтелектуальної обробки даних дозволяє виявляти закономірності в даних і на цій основі отримувати якісно нову інформацію. Така інформація може явно не міститися в джерелі даних, отже, в цьому випадку формування знань базується на даних.

Аналіз складових ІАС показує, що таки системи використовують єдину інформаційну базу, тобто містять інформацію для виконання аналітичної обробки та управління. Побудовані за принципом мінімізації введення та виведення інформації, адже постійне внесення в систему нових обсягів даних, приводить до формування ірраціональної структури бази даних, в яких складно знаходити потрібну інформацію. Для спрощення роботи з великими даними масиви інформації в ІАС розподілені на банки даних в залежності від відомостей, які в них знаходяться. Принцип мінімізації введення та виведення інформації сприяє скороченню кількості помилок, які виникають на ключових етапах роботи з даними: в процесі введення, коли будь-яка погрішність приводить до генерації невірного результату, та в процесі виводу, коли помилка порушує всі попередні етапи обробки інформації. Надання можливості введення змін пов'язаний з тим, що фіксувати нові дані в базі даних ІАС по-

трібно тільки тоді, коли нова інформація може привести до змін вже записаних відомостей або їх інтерпретації.

ІАС створюють єдиний інформаційний простір і надають доступ до потрібної інформації на всіх етапах управління в процесі прийняття рішень. ІАС будуються на основі оперативних даних, які поступають у систему в режимі реального часу з різних джерел даних і використовуються при прийнятті управлінських рішень.

Список використаних джерел:

1. Ніколаєв І.В., Вишневська В.А., Жовновач Р.І. Підходи до розробки інформаційно-аналітичної системи для прийняття управлінських рішень на підприємстві. Центральноукраїнський науковий вісник. Економічні науки. 2019. Вип. 2(35). С. 159-168.
2. Data mart vs. data warehouse vs. data lake. URL: https://www.ibm.com/topics/data-mart
3. Data Engineering – OLTP vs OLAP. URL: http://surl.li/nizuu.

Ключові слова: системний аналіз, програмне забезпечення, етапи розробки, аналіз вимог
Keywords: system analysis, software, development stages, requirements analysis

Науковий керівник: к.пед.н., доцент Логінова Н.І.

РОЗРОБКА ЧАТ-БОТА ДЛЯ ПОШУКУ НЕРУХОМОСТІ

Петрушенко Мілєна

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Ефективне використання цифрових технологій на сучасному ринку нерухомості є важливим фактором успіху агентств нерухомості та їхніх працівників. Створення ефективного та інтуїтивно зрозумілого телеграм-бота для отримання актуальної інформації про об'єкти нерухомості, доступні на ринку, підвищить ефективність та зручність роботи агентів з нерухомості.

Для розробки чат-бота Property Searcher було використано мову програмування Java, фреймворк Maven (Apache Maven), Telegram Bot API для взаємодії з платформою Telegram та реалізації функціоналу бота. Залучення бібліотек Jsoup (https://jsoup.org/) відіграло важливу роль щодо забезпечення функціональності та оброблення даних з платформ типу OLX.ua для формування актуальних оголошень (рис. 1, 2).

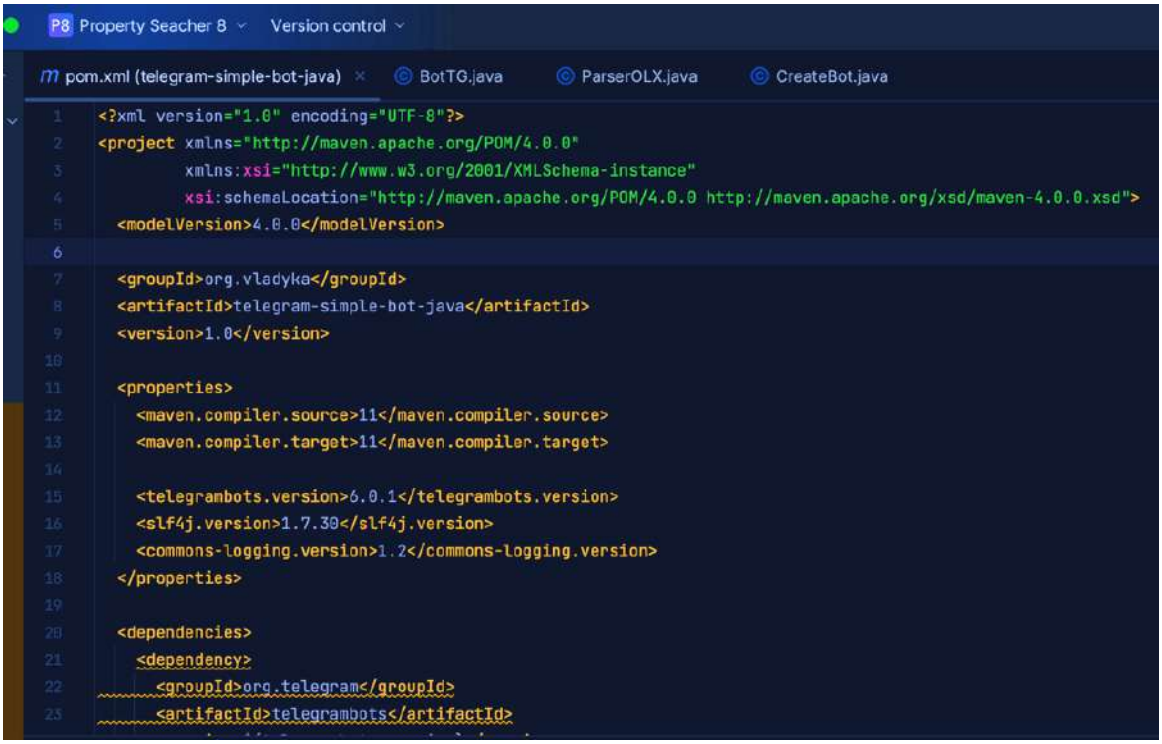
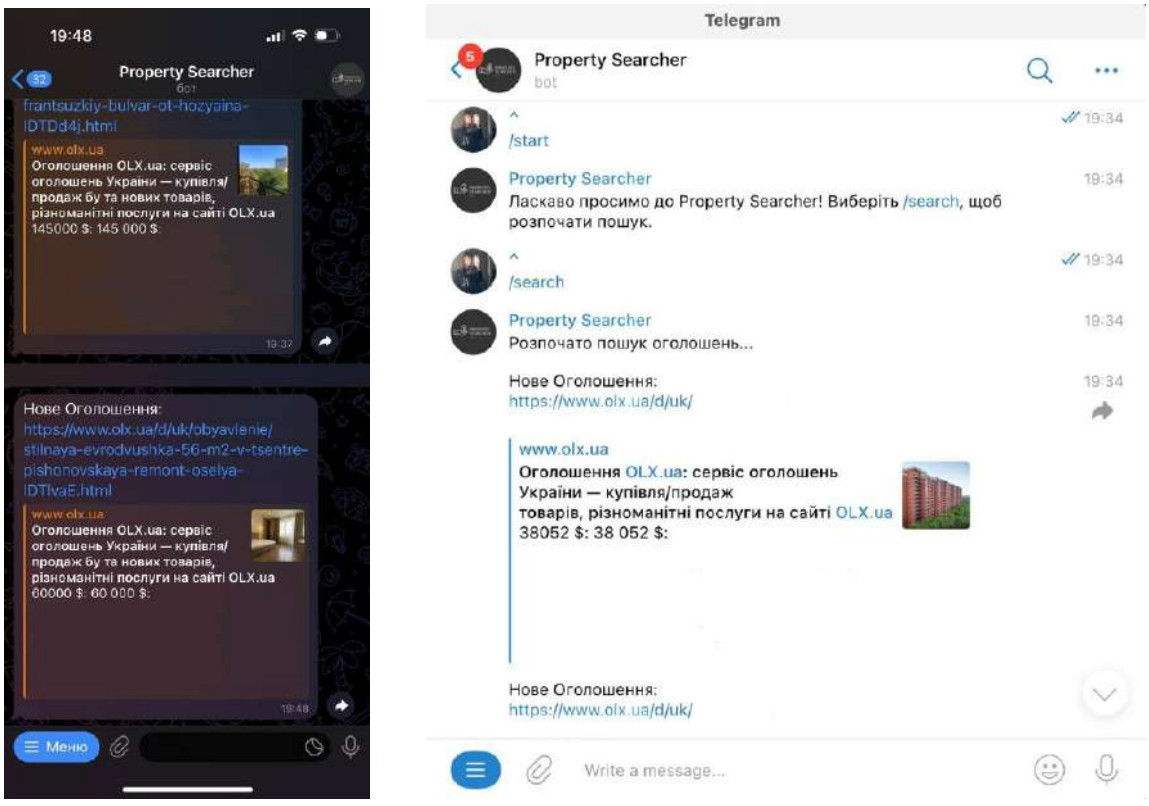


Рис. 1. Фрагмент .xml-файлу, в якому прописані залежності



а) *б)*

Рис. 2. Вигляд роботи чат-бота: а) на телефоні; б) на комп'ютері

Складність розроблення такого чат-бота полягала в тому, що взаємодія з платформами, з яких беруться оголошення, ускладнена через постійні

оновлення та зміни в структурі сайтів. Через це треба регулярно адаптувати парсер до змін для забезпечення стабільної роботи застосунку, тобто бот потребує постійного супроводу та підтримки. Крім того, виникла потреба використання багатопоточності в боті, по-перше, щоб одночасно обробляти запити користувачів та здійснювати парсинг або оброблення даних з різних джерел, а, по-друге, щоб підвищити загальну продуктивність й уникнути затримки виконання завдань, особливо при обробленні великих обсягів даних та при запитах до різних ресурсів.

Розроблений чат-бот Property Searcher є зручним і продуктивним інструментом для моніторингу доступних об'єктів нерухомості. Він швидко відбирає і надсилає користувачам найновіші оголошення у вибраній категорії. Розроблений бот може слугувати відповідним рішенням для широкого кола користувачів, які шукають доступну нерухомість.

Список використаних джерел:

1. Trofymenko O., Prokop Y., Loginova N., Zadereyko A. Taxonomy of Chatbots. International Scientific and Practical Conference «Intellectual Systems and Information Technologies» (ISIT2021). September 13-19, 2021, Odesa, Ukraine. P. 181-185. ISBN 978-966-186-161-8.
2. Трофименко О. Г. Сфери застосування чат-ботів. Інформаційне суспільство: проблеми та перспективи : матер. VII всеукр. наук.-практ. конф. (20 травня 2022). Одеса, 2022. С. 68-71. https://doi.org/10.32837/11300.17736.

Ключові слова: чат-бот, Telegram bot API, Jsoup.
Keywords: chat bot, Telegram bot API, Jsoup.

Науковий керівник: к. ю. н., доцент Трофименко О.Г.

Секція 3. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ КІБЕРПРОСТОРУ

ЩОДО ОБОВ'ЯЗКОВОСТІ РЕЄСТРАЦІЇ ЮРИДИЧНИХ ОСІБ ПРИВАТНОГО ПРАВА В ЕЛЕКТРОННОМУ СУДУ

Купенко Артем

студент 3-го курсу факультету прокуратури та слідства Національного університету «Одеська юридична академія»

У зв'язку із швидкими темпами колосального розвитку сучасних технологій, зокрема цифровізації всеможливого документообігу в нашій країні, постало й питання створення Єдиної судової інформаційно-телекомунікаційної системи, однієї з ключових підсистем якої є електронний суд. «Електронний суд» – це підсистема, яка прямо забезпечує здійснення обміну процесуальними документами між учасниками судового процесу та судом, як один з одним так і загалом.

Процесуальним законодавством України прямо зазначається обов'язковість реєстрації електронних адрес таких суб'єктів як: державні органи, нотаріуси, адвокати, судові експерти, суб'єкти господарювання комунального та державного секторів економіки та інших в Єдиній судовій інформаційно-телекомунікаційній системі (далі - ЄСІТС) [1]. Усі суб'єкти, які офіційно зареєстрували свою адресу в ЄСІТС, будуть отримувати усю документацію виключно в електронному варіанті на свою електронну адресу, та матимуть змогу надсилати документацію за умовою обов'язкового використання електронного підпису використовуючи цю систему. Загалом, свій початок ЄСІТС бере з 01 грудня 2018 року, коли Державна судова адміністрація України оголосила про її створення. Починаючи з 05 жовтня 2021 року офіційно почали функціонувати такі підсистеми ЄСІТС як Електронний суд, Електронний кабінет та підсистема відеоконференцзв'язку.

Основна мета такої цифровізації суду – це відхід від паперового документообороту, що становив і, на жаль, поки що ставить надмірний тягар для роботи суду, до більш сучасного та зручного способу комунікації – електронного: адже подання позовних заяв, скарг, заяв і клопотань тощо, участь в судових засіданнях в режимі відеоконференції лише за допомогою вашої електронної пошти та попередньої реєстрації в ЄСІТС значно спрощує багато бізнес процесів. У зв'язку з цим нещодавно, а саме 18 жовтня 2023 року, набрали чинності зміни до Господарського процесуального кодексу України, які прямо передбачають обов'язкову реєстрацію юридичних осіб приватного права в ЄСІТС (п.6 ст. 6 ГПК України) [2]. Зазначені зміни викликали хвилю

як обурення, так і схвалення зі сторони бізнесу. Так, нові зміни у законодавстві фактично позбавляють права юридичних осіб приватного права подавати до суду документи у формі, відмінній від електронної. Це нововведення стосується не лише тих, хто планував звернутися до суду з метою вирішення певного господарського спору, а й тих, хто вже безпосередньо бере участь у судовому процесі. У Державній судовій адміністрації пояснюють, що подвійна реєстрація необхідна, оскільки у разі звільнення штатного працівника юридичної особи, який здійснює представництво інтересів компанії, документи з суду мають надходити саме до такої юридичної особи, а не в особистий кабінет системи ЄСІТС звільненого представника. Аналогічну паралель проводять і з представництвом адвокатами в суді [3]. У разі, якщо адвокат припиняє надавати правничу допомогу своєму клієнту за договором та відповідно здійснювати його представництво у суді, то в такому випадку юридична особа не залишиться поза інформаційним полем.

Звичайно, за порушення норми щодо обов'язкової реєстрації в підсистемі Електронний Суд законодавцем передбачено й негативні процесуальні наслідки – повернення документів заявникові або залишення їх без розгляду. З огляду на викладене, та враховуючи сьогоденні умови (запроваджений на території України воєнний стан, активні бойові дії в частині регіонів нашої держави, відсутність технічних засобів, інтернету тощо) юридичні особи приватного права будуть фактично позбавлені права на захист. На практиці, це матиме й інші негативні наслідки. Так, суд не зможе прийняти та долучити до матеріалів справи чисельні заяви, скарги, клопотання від юридичних осіб, які не зареєструвалися в ЄСІТС, а отже, це впливатиме й на вирішення судового спору, повноту і всебічність судового розгляду, обґрунтованість прийнятого рішення. Серед іншого, такі процесуальні причини як не реєстрації в ЄСІТС негативно вплинуть на суть вирішення спору та строки розгляду справ. Фактично, обґрунтованість та об'єктивність прийняття судового рішення в господарського процесі будуть поставлені в залежність від дотримання судом процесуальної норми щодо їх прийняття з огляду на наявність чи відсутність реєстрації в Електронному Суді [4].

Крім того, для реєстрації в ЄСІТС як фізичні, так і юридичні особи мають вказати свою офіційну електронну адресу. Проте, законодавчого закріплення вказаного терміну й досі немає, незважаючи на чисельність слушних законодавчих ініціатив щодо врегулювання цього питання, принаймні, для державних органів, органів місцевого самоврядування, юридичних осіб. Такі прогалини у законодавстві, в свою чергу, призведуть до масового оскарження дій суду: як у поверненні позовних заяв, залишення позовних заяв, скарг тощо без розгляду, так і в оскарженні необґрунтованих і необ'єктивних рі-

шень – не лише на національному рівні, а й до Європейського суду з прав людини.

З метою недопущення створення штучних перешкод у доступі до правосуддя, вважаємо, що законодавцем мають вчинені відповідні заходи, які направлені на забезпечення процесуальної рівності всіх учасників судового процесу.

Список використаних джерел:

1. Єдина судова інформаційно-телекомунікаційна система (ЄСІТС). «Електронний суд»: URL: https://wiki.legalaid.gov.ua/index.php/
2. Господарський процесуальний кодекс України : Закон України від 06.11.1991 року №1798-XII. URL: https://zakon.rada.gov.ua/laws/show/1798-12#n1525
3. Мамченко Н. Навіщо підприємствам реєструватися в Електронному суді паралельно зі своїми адвокатами. 25.10. 2023. : URL https://sud.ua/uk/news/publication/
4. Мамченко Н. Як обов'язкова реєстрація Електронних кабінетів може перетворитися у проблему для українських підприємців та судів. 24.10. 2023. URL: https://sud.ua/uk/news/

Ключові слова: електронний суд, документообіг, судовий розгляд, правова відповідальність

Keywords: electronic court, document management, legal proceedings, legal responsibility

Науковий керівник: к.ю.н., доцент Добровольська В.В.

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ В ПРОЦЕСІ МЕДІАЦІЇ

Блатін Стівен

студент 4-го курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Сучасний досвід багатьох розвинутих країн показує, що медіація є ефективним, фінансово заощадливим і своєчасним способом досягнення консенсусу, вирішення конфлікту порівняно з вирішенням спору в судовому порядку. При чому компроміс і врегулювання можуть бути досягнуті не тільки у спірних питаннях, що виникають у сімейних, цивільних, господарських, корпоративних відносинах, але й навіть у певних кримінальних провадженнях.

В результаті довготривалої законотворчої роботи Верховної Радою України 16 листопада 2021 року було прийнято Закон про медіацію [1]. З метою подальшого створення законодавчого механізму для успішного становлення медіації в Україні діяльність законодавців, науковців та професійних громадських організацій має бути спрямована на розробку та прийняття від-

повідних підзаконних нормативно правових актів та пошук шляхів для повноцінного запровадження інституту медіації як альтернативного інструменту вирішення трудових спорів.

Запровадження в Україні медіації, як одне із нагальних питань в межах правової доктрини досліджується й обговорюється вже багато років. Аналізуючи національне законодавство, потрібно зазначити, що про необхідність запровадження процедур примирення за участю посередника (медіатора) вказувалось ще у Законі України «Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу» в якому визначено що медіація надається як переговори за участі нейтрального посередника, добровільний і конфіденційний процес, в якому нейтральна третя сторона допомагає конфліктуючим сторонам досягти взаємоприйнятої угоди, як метод, за яким сторони управляють і володіють як самим процесом так і його результатом – угодою.

Сучасний розвиток інформаційних технологій та воєнний стан роблять актуальними питання використання цифрових технологій для захисту прав, включаючи сферу медіації.

Інтенсивний розвиток інформаційно-комунікаційних технологій та процеси глобалізації роблять обмін інформацією більш доступним на всіх рівнях взаємовідносин людей, включаючи публічне управління та адміністрування. Однак технології не завжди можуть повністю вирішити або усунути проблеми, що виникають в цьому контексті.

Сучасні дослідники закликають використовувати альтернативні методи для вирішення конфліктів [2, с. 66]. Одним з таких методів є медіація, яка, хоча не є новою ідеєю, залишається недостатньо дослідженою. Останнім часом медіація виходить за рамки звичайного методу вирішення конфліктів і застосовується в багатьох сферах суспільного життя.

Цифрові технології відіграють значну роль в процесі медіації, роблячи її більш доступною та ефективною. Інтернет та цифрові комунікаційні засоби дозволяють учасникам конфлікту взаємодіяти з віддаленими медіаторами. Це особливо корисно в ситуаціях, коли сторони знаходяться в різних географічних регіонах або коли участь в зустрічі особисто неможлива, наприклад, через пандемію. Цифрові платформи для медіації можуть забезпечити вищий рівень конфіденційності, оскільки забезпечують безпеку обміну інформацією між сторонами та медіатором.

Цифрові засоби дозволяють зберігати всю необхідну документацію та записи засідань медіації в електронному форматі [3, с. 93]. Це полегшує процес архівування та доступ до інформації для всіх учасників. Цифрові платформи можуть надавати інструменти для вирішення конфліктів, наприклад, онлайн-дошки для створення спільних документів, веб-камери для візуально-

го спілкування та системи голосового чату для обговорення питань. Використання цифрових технологій може зменшити витрати на проведення медіації, так як не потребує фізичної присутності сторін або медіаторів у спеціальних приміщеннях. Цифрові платформи можуть надавати інструменти для автоматизації певних аспектів процесу медіації, таких як нагадування про зустрічі, створення звітів і планів дій.

Таким чином, запровадження медіації в Україні має багато позитивних аспектів. Це сприяє полегшенню доступу до вирішення конфліктів, зменшенню витрат, і надає можливість вирішувати спори без відвідування суду. З огляду на інтенсивний розвиток інформаційних технологій, цифрові засоби можуть використовуватися для поліпшення процесу медіації. Медіація, підсилена цифровими інструментами, може стати дієвим засобом вирішення конфліктів, забезпечуючи більш зручний та доступний процес для всіх учасників.

Варто констатувати той факт, що цифрові технології полегшують доступ до медіації, допомагають сторонам ефективно вирішувати конфлікти та забезпечують більш швидкий та зручний процес.

Список використаних джерел:

1. Про медіацію: Закон України Закон України від 16.11.2021 р №1875- IX. Голос України 15 грудня 2021 року.
2. Бородін Є. Є. Механізм медіації в системі публічного управління: дис. … канд. наук держ. упр. Дніпро, 2019. 245 с.
3. Мазаракі М. Медіація в Україні: проблеми теорії та практики. Зовнішня торгівля: економіка, фінанси, право. 2016. № 1. С. 92–100.

Ключові слова: медіація, медіатор, принципи медіації, альтернативне вирішення спору, спір (конфлікт).
Keywords: mediation, mediator, principles of mediation, alternative dispute resolution, dispute (conflict).

Науковий керівник: к.ю.н., доцент Добровольська В.В.

ІНФОРМАЦІЙНА ПОСЛУГА У СФЕРІ ГОСПОДАРЮВАННЯ: ПОНЯТТЯ ТА ОЗНАКИ

Деренюк Ангеліна

студентка 3-го курсу факультету прокуратури та слідства Національного університету «Одеська юридична академія»

Загальна Декларація прав людини, ухвалена у 1948 році, історично стала першим міжнародним актом, що провозголосив право на свободу отримання та поширення інформації незалежно від кордонів конкретних країн та способів. Подальше розширення цього права відбулося з ухваленням Між-

народного пакту про громадянські та політичні права в 1966 році, де конкретизовано, що воно включає свободу пошуку, одержання та поширення інформації через будь-які доступні засоби, незалежно від національних кордонів, чи то усно, письмово, друкованою продукцією, мистецтвом або іншими обраними способами. Конституція України також гарантує право на інформацію, визначаючи, що "кожен громадянин має право вільно збирати, зберігати, використовувати та розповсюджувати інформацію у будь-якій формі — усно, письмово, друкованою продукцією, в образотворчому мистецтві чи іншими доступними способами відповідно до закону." [1]

У Законі України "Про інформацію" законодавець визначив інформацію як будь-які відомості та/або дані, які можуть зберігатися на матеріальних носіях або подаватися в електронному вигляді. Це закріплення в законодавстві сприяє розумінню широкого спектру інформаційних прав та свобод у сучасному інформаційному суспільстві. Проте, законодавство не надає точного визначення для понять "дані" та "відомості", і не розглядає різницю між ними. Це породжує питання стосовно того, що може бути вважено даними або відомостями, і чи можуть жести або думки людини увійти в ці категорії. Відсутність конкретного визначення може призвести до недорозумінь щодо того, коли інформація стає інформацією, а коли лише даними.

Закон також не містить обов'язкових вимог до змісту, значення та сенсу відомостей і даних, які вважаються інформацією. Це створює питання стосовно того, коли інформація вважається інформацією, а коли лише даними.

У юридичній науці спостерігається багато різних підходів до трактування поняття "інформація". У доктрині цивільного права, інформація може розглядатися як об'єкт цивільних прав, а також як особисте немайнове благо, об'єкт виключних прав інтелектуальної власності, об'єкт правочинів (інформаційний продукт, товар, послуга).

Згідно з Цивільним кодексом України, інформацію може бути визнано об'єктом права власності та наділено ознаками правового режиму речі (майна). Це означає, що інформація як об'єкт права власності може існувати у матеріалізованій товарній формі. У зв'язку із розвитком ринку інформаційних товарів і послуг, інформація стає важливою у підприємницькій діяльності. Її характер може варіюватися в залежності від господарських відносин і може виступати у різних формах. Господарська діяльність, спрямована на досягнення економічних та соціальних результатів з метою отримання прибутку, визнається підприємництвом, і її суб'єкти вважаються підприємцями. Господарські відносини охоплюють господарсько-виробничі, організаційно-господарські та внутрішньогосподарські відносини. Проте інформація, яка виступає як об'єкт договірних відносин, може бути актуальною лише в галузі господарсько-виробничої діяльності суб'єктів господарювання, тобто в разі без-

посереднього виконання господарської діяльності з метою виробництва продукції, надання послуг та виконання робіт.

Саме у межах цих господарських правовідносин інформація набуває форми товару, який створено для обміну або продажу, а не для особистого споживання. Інформація набуває таких характеристик, як корисність та ринкова вартість.

Для того, щоб інформація стала об'єктом комерційного інтересу для суб'єктів господарської діяльності, вона має відповідати кільком критеріям. По-перше, інформація повинна мати цінність, тобто містити дані, які є корисними і необхідними для замовника, і він готовий заплатити за них. По-друге, ця інформація не повинна бути загальнодоступною, що створює потребу звертатися до постачальника інформаційних послуг. По-третє, такі відомості повинні задовольняти інформаційні потреби споживача, оскільки в іншому випадку відносини втрачають сенс. Крім того, професійна підготовка, спеціальні знання та дозволи можуть бути обов'язковими умовами для суб'єктів, які надають інформаційні послуги. З урахуванням цих умов, інформація як об'єкт господарської діяльності - це відомості і/або дані, які містяться на матеріальних або віртуальних носіях і передаються суб'єктами в процесі здійснення господарської діяльності.

Щоб інформація стала повноцінним об'єктом відносин у сфері надання інформаційних послуг, вона повинна мати певну форму. Наприклад, Закон України "Про національну програму інформатизації" визначає поняття інформаційної послуги як дії суб'єктів, спрямовані на забезпечення споживачів інформаційними продуктами. Однак термін "інформаційний продукт" в цьому законі визначено занадто стисло і неповно. Згідно з наказом Державного комітету зв'язку та інформатизації № 97 від 06.06.2003, інформаційний продукт - це цифрові дані, призначені для задоволення інформаційних потреб користувача, включаючи програмний продукт. Закон України "Про інформацію" має більш широке визначення інформаційної продукції, яка визначається як матеріалізований результат інформаційної діяльності, призначений для задоволення потреб суб'єктів інформаційних відносин. [1]

Справді, законодавство України має різні інтерпретації та визначення понять, пов'язаних із сферою інформаційних послуг та продуктів. Ця ситуація може виникнути через різні часи ухвалення різних нормативних актів, їх обмежену чи суперечливу дефініцію.

Погляди на відношення між інформаційними продуктами і послугами можуть варіюватися в залежності від контексту та трактування понять. Олександр Теряник виділив кілька ознак, які він вважає характерними для інформаційних продуктів, і такі ознаки відзначають їх від інформаційних послуг, наприклад: 1. Неможливість зносу та фізичного знищення інформацій-

ного продукту. 2. Можливість "морального старіння" інформаційного продукту. 3. Легке тиражування інформаційного продукту. 4. Можливість одночасного відтворення у кількох процесах. [2]

Проте в контексті інформаційних послуг інформаційний продукт може бути однією з форм надання послуги, іншою формою може бути, наприклад, надання доступу до бази даних або створення інформаційного контенту для клієнта. Звідси виникає плутанина в тлумаченні понять.

Законодавство може надавати визначення і регулювати співвідношення між інформаційними продуктами та послугами в різних контекстах. Ф. Махлуп розглядає інформаційні послуги у широкому філософському контексті, визначаючи їх як виробництво знань та створення, зміну або підтвердження розуміння чи визнання певних фактів. Такий погляд відображає філософську сутність інформаційних послуг, але в практичному та правовому контексті може бути занадто абстрактним. Науковці, такі як Н. Федосенко та В. Мілаш, більше акцентують увагу на об'єктивному результаті інформаційних послуг та визначають їх як надання діяльності, результатом якої є інформація. Цей погляд відображає практичний аспект інформаційних послуг. Л. Саннікова визначає інформаційні послуги як зміну стану інформації, що включає збір інформації, її обробку, аналіз та передачу замовнику. Це більш конкретне і практичне визначення, яке може бути корисним для регулювання правових відносин у цій галузі. [3]

Визначення інформаційних послуг може різнитися в залежності від галузі та правового контексту, і важливо розуміти конкретний контекст та специфіку понять у кожному випадку. Підходи, які розглядають інформаційні послуги як надання споживачеві певного контенту, можуть бути обмежені і не охоплювати всі різноманітні види інформаційних послуг, які доступні на сучасному ринку. Погляди, які підкреслюють корисний ефект від надання інформаційних послуг, важливі, оскільки корисність для споживача може бути однією з ключових характеристик послуг.

Висновки. Результати дослідження свідчать про необхідність чіткого регулювання інформаційних відносин у сфері господарювання. Запропонована дефініція інформаційної послуги має бути внесена до Господарського кодексу України, щоб виділити цей вид господарських договорів як окремий. Зважаючи на зростаючий попит і актуальність інформаційних послуг у господарських правовідносинах, а також з метою створення ефективного правового механізму для їх регулювання, наша робота вказує на необхідність подальшого дослідження цієї проблеми.

Список використаних джерел:

1. ІНФОРМАЦІЙНА ПОСЛУГА У СФЕРІ ГОСПОДАРЮВАННЯ: ПОНЯТТЯ ТА ОЗНАК: веб-сайт. URL : http://pgp-journal.kiev.ua/archive/2019/10/11.pdf
2. РИНОК ІНФОРМАЦІЙНИХ ПОСЛУГ: ПОНЯТТЯ, ОЗНАКИ Й ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ: веб-сайт. URL : http://www.lawbulletin.oduvs.od.ua/archive/2020/16/21.pdf
3. ПОНЯТТЯ Й ОЗНАКИ ПОСЛУГИ ЯК ПРЕДМЕТА ГОСПОДАРСЬКО-ПРАВОВОГО РЕГУЛЮВАННЯ: веб-сайт. URL : http://surl.li/mpkgm

Ключові слова: інформація, інформаційна послуга, інформаційний продукт
Keywords: information, information service, information product

Науковий керівник: к.ю.н., доцент Добровольська В.В.

ЩОДО КІБЕРБЕЗПЕКИ ГОСПОДАРСЬКИХ ПРАВОВІДНОСИН

Ляховецький Олександр

аспірант кафедри господарського права і процесу Національного університету «Одеська юридична академія»

Чисельні господарські відносини на сьогоднішній день існують як у реальному житті так і в цифровому середовищі та потребують надійного захисту для належного забезпечення їх реалізації, відомостей про їхні сторони та предметну складову. Саме, «кібербезпека має забезпечувати захист інформаційно-комунікаційних технологій та захист інформаційно-комунікаційних систем в економіці, інших галузях господарства. Це в повній мірі стосується і господарсько-правових відносин в таких галузях як виробництво, транспорт, енергетика, рух цінних паперів, аудиторська діяльність, фінансові послуги, в бізнесі, в торгівлі тощо» [1, с. 638]. Кормич Б.А. зазначає, що «кібербезпека — це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави» [2, с. 142]. Зазначені процеси цілком розповсюджуються на сферу господарювання задля реалізації безпеки здійснення господарської діяльності та відповідних відносин. Ряд дослідників пропонують наступне авторське визначення поняття інформаційної безпеки, частковим випадком якої є кібербезпека, як «стан захищеності особи, держави і суспільства, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди» [3, с. 10]. Тобто, зазначене характеризує мету кібербезпеки та її суб'єктну складову. Нормативно кібербезпека визначена як «захищеність життєво важливих інтересів людини та громадянина, суспільства й

держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [4]. У літературі слушно вказується на те, що «нажаль, дія спеціального Закону не поширюється на відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах, соціальних мережах, приватних електронних інформаційних ресурсах в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші вебресурси)» [5]. Кібербезпеку у сфері господарювання можливо визначити як комплекс заходів і стратегій, спрямованих на забезпечення безпеки інформаційних ресурсів та кіберінфраструктури підприємства з метою запобігання кібератакам, захисту конфіденційної інформації, забезпечення безперервності бізнес-процесів та виконання вимог законодавства у сфері захисту даних. Ключові аспекти кібербезпеки в господарюванні включають в себе: захист інформації та кіберінфраструктури, виявлення і своєчасна відповідь на кіберзагрози, надійне та безпечне зберігання даних, підвищення інформаційної грамотності співробітників, дотримання чинного законодавства.

Суб'єкти господарювання є сторонами цифрових господарських відносин через використання чисельних комп'ютерних пристроїв та систем. Як вважає Бакалінська О.О. «уразливими для реалізації кіберзагроз є об'єкти, функціонування комп'ютерних систем яких пов'язане з використанням ресурсів кіберпростору. Таким чином, об'єкти, завдання шкоди яким можливе шляхом деструктивного кібервпливу (кібератаки) тобто спрямованих (навмисних) дій в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» [6].

09 травня 2018 року набрала чинності Директива Європейського парламенту і Ради (ЄС) №2016/1148, під назвою «Безпека мереж та інформації» (Network and Information Security), за якою кожна держава-член ухвалює національну стратегію щодо безпеки мережевих та інформаційних систем, що визначає стратегічні цілі та доречну політику та регуляторні інструменти з

метою досягнення та підтримання високого рівня безпеки мережевих та інформаційних систем [7].

Таким чином кібербезпека стала критично важливою для сучасних господарських правовідносин через зростання кількості кіберзагроз та значущість їхніх наслідків та розвиток цифрових технологій. Під час реалізації заходів щодо кібербезпеки господарських правовідносин важливо приділяти увагу законодавству, яке регулює питання кібербезпеки в господарських правовідносинах, включаючи заходи, які суб'єкти господарювання повинні приймати для дотримання закону. Кібербезпека вимагає співпраці між підприємствами, урядовими органами та іншими зацікавленими сторонами з метою обміну інформацією та взаємодопомоги у вирішенні кіберзагроз, які постійно змінюються, тому важливо постійно вдосконалювати знання та практику, щоб ефективно захищати господарські правовідносини в цифровому світі. Також потрібно пам'ятати, що як порушення, так і нехтування забезпеченням кібербезпеки може мати серйозні наслідки, включаючи юридичну відповідальність для суб'єктів господарювання та їх керівників.

Список використаних джерел:

1. Бойко В.Д., Василенко М.Д. Кібербезпека як складова цифрового суспільства в контексті розвитку господарсько-правових відносин Правове життя сучасної України : у 2 т. : матер. Міжнар. наук.-практ. конф. (м. Одеса, 17 трав. 2019 р.) / відп. ред. Г.О. Ульянова. Одеса : ВД «Гельветика», 2019. Т. 2. С. 637–640.
2. Кормич Б. А. Кібербезпека: організаційно-правові основи : Навч. посібн. К. : Кондор, 2008. 382 с.
3. Калюжний Р.А. Інформаційне забезпечення управлінської діяльності в умовах інформатизації : організаційно-правові питання теорії і практики : підручник для студ. вищ. навч. закл. / Р.А. Калюжний, В.О. Шамрай, М.Я. Швець та ін. ; за ред. Р.А. Калюжного та В.О. Шамрая. К. : Академія державно-податкової служби України, 2002. 296 с.
4. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05 жовтня 2017. URL : https://www.rada.gov.ua/ (дата звернення 11.10.2023 р.).
5. Раєцький А. Кібербезпека бізнесу це не лише технічні заходи. URL: https://legalitgroup.com/ (дата звернення 11.10.2023 р.).
6. Бакалінська О.О. Сучасні тенденції правового регулювання кібербезпеки та інтелектуальна власність. Координата. 17.11.2022. URL : https://coordynata.com.ua/(дата звернення 11.10.2023 р.).
7. Директива Європейського парламенту і Ради (ЄС) № 2016/1148. URL : https://www.rada.gov.ua/ (дата звернення 11.10.2023 р.).

Ключові слова: господарські правовідносини, кібербезпека, кіберзагрози
Keywords: economic legal relations, cybersecurity, cyber threats

Науковий керівник: к.ю.н., доцент Добровольська В.В.

ДЕЯКІ АСПЕКТИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ЗМІН

Грезіна Олена

студентка 1-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Актуальність теми визначається необхідністю адаптації правового регулювання до швидкозмінних умов кіберпростору. Зростання кількості та складності кіберзагроз, а також постійне вдосконалення технологій створюють потребу в ефективних та сучасних нормативних рамках для захисту інформаційної безпеки. Нові виклики та загрози вимагають постійного оновлення та удосконалення законодавчих актів для забезпечення високого рівня кібербезпеки. Це сприятиме розгляду важливих аспектів, таких як захист особистих даних, кіберзахист корпоративних інформаційних систем та боротьба з кіберзлочинністю в контексті актуальних правових норм.

В контексті цього питання Гребенюк М. зазначає, що «…у сучасних умовах питання забезпечення кібербезпеки не обмежуються лише організацією системи захисту інформації на окремому об'єкті критичної інформаційної інфраструктури, а й передбачають створення єдиної системи захисту кібернетичного простору як складової частини інформаційної та національної безпеки будь-якої держави світу» [1. с, 203].

Зокрема, це стосується захисту особистої інформації громадян, для чого потрібно розробляти та вдосконалювати правові норми, спрямовані на забезпечення конфіденційності та безпеки особистих даних. Паралельно важливо створювати гнучкі механізми для ефективної реакції на швидкозмінювані кіберзагрози, сприяючи співпраці між державними структурами, приватним сектором та міжнародними партнерами.

Одним із аспектів вважатимемо підвищення кваліфікації фахівців у галузі кібербезпеки та правозахисту для ефективної реалізації нових законодавчих ініціатив. Крім того, акцент слід робити на попередженні кіберзлочинності, впроваджуючи превентивні заходи та стимулюючи відповідальність за порушення кібербезпеки.

Фахівці з правозахисту кібербезпеки мають за розробку та впровадження інноваційних стратегій щодо захисту інформації, виявлення та вирішення порушень безпеки даних, а також вивчення та впровадження відповідних правових норм та політик в галузі кібербезпеки. Вони забезпечують відповідність діяльності організацій законодавству щодо захисту інформації та реагують на еволюцію кіберзагроз, забезпечуючи адаптацію стратегій захисту.

Навчання персоналу щодо розпізнавання фішингових атак, обізнаності щодо використання сильних паролів та інших базових принципів безпеки може значно знизити ризик випадкових порушень. Організації також можуть впроваджувати системи двофакторної аутентифікації та регулярно аудитувати свої мережі для виявлення можливих слабкостей у захисті. Дані превентивні заходи повинні мати під собою обов'язкове правове підґрунтя.

Міжнародне співробітництво в цій області також має велике значення, оскільки воно дозволяє обмінюватися передовим досвідом та підвищує ефективність національних заходів забезпечення кібербезпеки.

Дослідженням цього питання займались такі науковці, як І. Доронін, О. Потій, А. Семенченко, О. Бакалинський, Д. Мялковський, В. Шемчук та інші.

Відносини, пов'язані із забезпеченням кібернетичної безпеки в Україні, регулюються чинними нормативно-правовими актами. А саме, Законом України «Про основні засади забезпечення кібербезпеки України», Законом України «Про інформацію», Законом України «Про науково-технічну інформацію», Законом України, «Про доступ до публічної інформації.

Слушними є думки Потій О., Семенченко А., Бакалинського О., Мялковського Д. У своїй науковій праці вони: «…визнаючи кіберпростір одним із середовищ застосування геостратегій та «п'ятим плацдармом» проведення бойових дій, разом із суходолом, морем, повітрям і космосом, дедалі більше уваги приділяється розвитку й захисту інформаційних ресурсів, а також можливостям впливати на інформаційні ресурси інших країн, що загалом описується як проблема забезпечення кібербезпеки держави» [2, с. 139].

Рекомендаціями до вирішення проблеми правового захисту кібербезпеки можуть стати подальший розвиток нормативно-правового поля в контексті правового захисту, посилення захисту інформаційних ресурсів, підтримку міжнародного співробітництва та проведення наукових досліджень для вивчення можливостей впливу на інформаційні ресурси. Дані заходи спрямовані на поліпшення загальної кібербезпеки держави в умовах сучасного кіберпростору.

У висновку зазначимо, що адаптація правового регулювання до динамічних змін у кіберпросторі є небхідною дією. Зростання кількості та складності кіберзагроз потребує сучасних нормативних рамок для ефективного захисту інформаційної безпеки. Нові виклики вимагають постійного оновлення законодавства для забезпечення високого рівня кібербезпеки, зокрема в контексті захисту особистих даних, кіберзахисту корпоративних інформаційних систем та боротьби з кіберзлочинністю.

Список використаних джерел:

1. Гребенюк М. Деякі питання організаційно-правового забезпечення кібербезпеки: огляд кращих практик зарубіжного досвіду. Підприємництво, господарство і право. 2019. 2. С. 203-207. URL: http://www.pgp-journal.kiev.ua/archive/2019/2/39.pdf
2. Потій О., Семенченко А., Бакалинський О., Мялковський Д. Публічне управління інституціональним розвитком у сфері кіберзахисту. Науковий вісник: Державне управління. 2021. (3(9). С. 136–162. URL: https://doi.org/10.32689/2618-0065-2021-3(9)-136-162

Ключові слова: правове забезпечення кібербезпекі, кіберпростір, правовий захист, превентивні заходи
Keywords: legal provision of cyber security, cyberspace, legal protection, preventive measures

Науковий керівник: к.пед.н., доцент Логінова Н.І.

ВИКОРИСТАННЯ АЛГОРИТМІВ YOUTUBE ДЛЯ ОРГАНІЗАЦІЇ ТЕРОРИСТИЧНИХ НАПАДІВ.

Динту Валерія

доцент кафедри криміналістики, детективної та оперативно-розшукової діяльності Національного університету «Одеська юридична академія», кандидат юридичних наук, доцент

Інтернет демократизував мову, створивши форум для публічного самовираження та об'єднавши мільярди спікерів і слухачів, які до того не мали можливості та засобів знайти один одного. Ніколи раніше так багато людей не мали таку велику свободу висловлювати свої думки, бути почутими та ділитися інформацією з іншими. Однак, слід зазначити, що Інтернет є засобом, вектор використання якого залежить від мотивів та наміру користувача. Зокрема, виявлені непоодинокі випадки використання мережі Інтернет для вчинення кримінальних правопорушень. Приміром, терористи часто швидко опановують нові технології та використовують їх у непередбачуваний спосіб, для реалізації суспільно небезпечних діянь.

Так на сьогодні виявлені випадки застосування терористами алгоритмів відеохостингу YouTube для розповсюдження інформації та організації терористичних актів.

Старший радник Проекту боротьби з екстремізмом (CEP) д-р Хані Фарід, професор Каліфорнійського університету в Берклі, заявив, що алгоритмічне посилення є основною причиною безпрецедентного поширення мови ненависті, дезінформації, теорій змови та шкідливого контенту в Інтернеті. Платформи дізналися, що суперечливий вміст приваблює найбільшу

кількість користувачів, і тому справжня сила полягає в цих алгоритмах рекомендацій.

CEP також провів дослідження з 2 по 3 серпня 2018 року під назвою «OK Google, покажи мені екстремізм», у якому 649 відео YouTube було перевірено на наявність екстремістського та контрнаративного вмісту. Контррозповіді є частиною методу перенаправлення Google, який спрямований на людей, які шукають контент, пов'язаний з ІДІЛ «Ісламська держава Іраку та Леванту», і спрямовує їх на контрнаративні відео, які намагаються підірвати повідомлення екстремістських груп. З 649 відео CEP у чотири рази частіше зустрічав екстремістські матеріали, ніж контрнаративи. Результати пошуків CEP підкреслили масштаби екстремістського контенту на YouTube і спростували заяви YouTube про ефективність його зусиль щодо просування контрнаративних відео [1].

Наразі, використання алгоритмів відеохостингу YouTube в терорестичних цілях лягло в основу судового позову Рейнальдо Гонсалеса проти Google LLC, який є власником YouTube.

Донька Рейнальдо Гонсалеса Нохемі, громадянка США, яка навчалася за кордоном у Франції, загинула в результаті терористичних актів у Парижі які відбулися 13 листопада 2015 року. Кілька атак стали подією практично одночасно: вибухи біля стадіону "Стад де Франс" в Сен-Дені, напади на відвідувачів декількох ресторанів, і також напад у концертному залі «Батаклан», де близько 100 людей були утримані у заручниках. Ці терористичні акти призвели до 130 загиблих і понад 350 поранених, із них 99 перебували у критичному стані. Наступного дня ІДІЛ взяла на себе відповідальність, оприлюднивши письмову заяву та опублікувавши відео на YouTube. Рейнальдо Гонсалес, батько Нохемі, разом з іншими членами сім'ї подали скаргу на Google LLC про відшкодування збитків

Відповідно до скарги, поданої Гонсалесом проти Google, Google несе вторинну відповідальність за смерть його доньки, оскільки Google своїми діями та бездіяльністю сприяв і підбурював, дозволяючи ІДІЛ «вербувати членів, планувати терористичні атаки, видавати терористичні погрози, вселяти страх і залякувати цивільне населення» через YouTube. Зокрема, Гонсалес стверджував, що Google несе відповідальність за використання комп'ютерних алгоритмів, щоб рекомендувати своїм користувачам відео, опубліковані ІДІЛ або пов'язані з ІДІЛ. Таким чином Гонсалес стверджував, що Google допомагав ІДІЛ поширювати повідомлення організації. Крім того, Гонсалес стверджував, що Google несе відповідальність за те, що не видалив або видалив лише частину вмісту, опублікованого ІДІЛ або пов'язаного з ІДІЛ, хоча й має повноваження, як власник YouTube, повністю видаляти такий контент із YouTube. Грунтуючись на вищезазначених діях або бездіяльності

Google, Гонсалес стверджував, що YouTube став «важливою та невід'ємною частиною», а також «унікальним і потужним інструментом комунікації» терористичної організації ІДІЛ [2]. Рейнальдо Гонсалес стверджує, що алгоритм Google сприяв постачанню радикальних відео YouTube людям, яким алгоритм вважав, що це може сподобатися, безпосередньо сприяючи зростанню таких груп, як ІДІЛ, яка вбила Нохемі та інших.

Відповідно до законодавства США YouTube має імунітет, підпадаючи під категорію «видавник», та не несе відповідальності за контент розміщений автором. Ключове питання полягає в тому, чи рекомендація безпосередньо надсилає шкідливий сторонній вміст користувачам у формі файлу, чи вона просто містить інформацію про сторонній вміст у формі URL-адреси чи сповіщення. Гонсалес стверджує, що надсилання файлу є актом публікації, тоді як надсилання URL-адреси чи сповіщення – ні. Таким чином, коли YouTube рекомендує користувачам відео, пов'язані з ІДІЛ, YouTube не діє як «видавець», оскільки він просто надсилає користувачам інформацію про відео у формі URL-адреси. Подібним чином YouTube, зв'язує користувачів із контентом, і не може розглядатися як видавець цього контенту [3].

Також, рекомендації YouTube не вважаються «інформацією, наданою іншим постачальником інформаційного контенту» оскільки вони створені самим YouTube, а не іншим постачальником інформаційного контенту. Коли рекомендації YouTube містять URL-адреси, ці URL-адреси не є «інформацією, наданою іншим постачальником інформаційного контенту», оскільки функція URL-адрес полягає в тому, щоб надати користувачам адресу відео на сервері комп'ютера. Таким чином, оскільки URL-адреси надають інформацію про місцезнаходження, вони є «інформацією». Важливо, що Гонсалес відрізняє URL-адреси YouTube від URL-адрес, які з'являються в пошукових каналах Google, вказуючи, що YouTube створює власні URL-адреси, тоді як URL-адреси, знайдені як результати пошуку Google, генеруються сторонніми веб-сайтами. Також, пошукова система Google кваліфікується як інтерактивна комп'ютерна служба, оскільки вона надає результати пошуку у відповідь на пошуковий запит користувача. На відміну від цього, YouTube надсилає незапитані відео користувачам за допомогою автоматичного алгоритму рекомендацій [4].

Ще однією серйозною перешкодою, з якою стикається сім'я Гонсалес, яка має криміналістичну цінність, це встановлення причинно-наслідкового зв'язоку. Зокрема, вони повинні довести, що вбивці Нохемі дійсно споживали контент YouTube, який сприяв їх радикалізації та, зокрема, призвів до її вбивства. Поки що позивачі у справі Гонсалеса змогли довести в судовому процесі, що двоє з дванадцяти терористів, причетних до нападу, використовували платформи соціальних мереж, щоб розміщувати посилання на радикалізуючий контент ІДІЛ [5].

Наразі, Верховний Суд США повернув спарву на новий розгляд. Однак, не дивлячись на результати розгляду справи, вона ставить перед криміналістикою низьку фундаментальних питань, щодо визначення місця алгоритмів YouTube у системі криміналістичної характеристики злочинів, та їх використання у кримінальному провадженні з метою ефективного та раціонального розслідування кримінальних правопорушень.

Список використаних джерел:

1. Counter extremism project. Retrieved from https://www.counterextremism.com/blog/new-study-confirms-youtube-algorithm-promotes-misinformation-conspiracies-extremism. [in English]. (2023, November 13);
2. Reynaldo Gonzalez, et al., v. Google LLC. No. 21–1333. [2023]. Supreme Court of the United States. Retrieved from https://www.supremecourt.gov/opinions/22pdf/21-1333_6j7a.pdf. [in English]. (2023, November 13);
3. Reynaldo Gonzalez, et al., v. Google LLC. No. 21–1333. [2023]. Argument transcripts. Retrieved from https://www.supremecourt.gov/oral_arguments/argument_transcripts/2022/21-1333_q4lp.pdf. [in English]. (2023, November 13);
4. Cornell Law School. Retrieved from https://www.law.cornell.edu/supct/cert/21-1333. https://www.supremecourt.gov/opinions/22pdf/21-1333_6j7a.pdf. [in English]. (2023, November 13);
5. Yasmin M. Khodaei. (October 17, 2022). Unintentional Terrorists: An Upcoming Supreme Court Case Challenges the Role of the Youtube Algorithm in Terrorist Attacks. North Carolina Journal of Law & Technology. Retrieved from https://ncjolt.org/blogs/unintentional-terrorists-an-upcoming-supreme-court-case-challenges-the-role-of-the-youtube-algorithm-in-terrorist-attacks%EF%BF%BC/.[in English]. (2023, November 13).

Ключові слова: тероризм, алгоритми YouTube, кримінальні розслідування.
Keywords: terrorism, YouTube algorithms, criminal investigation.

THE BLETCHLEY DECLARATION ТА ПРОБЛЕМИ МІЖНАРОДНОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Чанишев Рашид

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат юридичних наук, доцент

Розроблення програм і систем, здатних самостійно, подібно до людського мозку, виконувати завдання з генерації осмислених текстів або зображень на задану тему, здійснювати управлінські функції, розпочалося ще в 50-х роках XX століття. Тривалий час цей процес не привертав уваги громадськості та політиків, які вважали, що поняття "штучний інтелект" більше належить до сфери наукової фантастики, ніж до реалій сучасності.

Однак в останні кілька років ситуація різко змінилася. Після того, як доступ до нових систем штучного інтелекту зміг отримати кожен охочий, у суспільстві з'явилося усвідомлення того факту, що програми ШІ дійсно здатні до самостійної творчості. Склалося враження, що йдеться вже і про створення в найближчому майбутньому повноцінного штучного розуму, здатного замінити людину в більшості сфер її діяльності.

Цей факт викликав велику тривогу в суспільстві. Так, ще у квітні 2021 року в Європейському Союзі почалося розроблення The Artificial Intelligence Act, документа, завданням якого є правове регулювання штучного інтелекту на території країн Європейського Союзу [1]. Приблизно за півроку до цієї події, Кабінетом Міністрів України була затверджена «Концепції розвитку штучного інтелекту в Україні». Однак швидка поява нових поколінь систем ШІ (наприклад, GPT-4, розробленого компанією OpenAI 2023 року) засвідчила, що процес розроблення заходів правового регулювання ШІ став різко відставати від темпів технічного прогресу.

В зв’язку з цим 22 березня 2023 року був опублікований відкритий лист, підписаний десятками тисяч провідних фахівців у сфері штучного інтелекту та представниками IT-індустрії, в якому закликалося запровадити щонайменше піврічний мораторій на створення нових систем ШІ, більш потужних, ніж GPT-4 [2].

Однак уже 14 листопада 2023 року гендиректор компанії OpenAI Сем Альтман (Sam Altman) в інтерв'ю виданню Financial Times повідомив про те, що компанія OpenAI вже веде розробку нової системи ШІ GPT-5 [3].

Крім того, у своєму більш ранньому виступі на конференції, організованій компанією OpenAI для розробників, що відбулася 7 листопада 2023 року, Сем Альтман згадав той факт, що продукти OpenAI вже використовують 92% компаній зі списку Fortune 500, і повідомив про те, що його компанія планує створення системи "сильного ШІ" (Artificial general intelligence), здатного діяти автономно, без втручання людини. Слід зазначити, що "сильний ШІ" у певних межах можна вже вважати "штучним розумом".

Ілля Суцкевер, головний науковий співробітник OpenAI, у своїх інтерв'ю висловлював аналогічні думки. Однак 18 листопада 2023 року з'явилося повідомлення про те, що рада директорів OpenAI, за ініціативою Суцкевера, звільнила Сема Альтмана з компанії OpenAI. При цьому про причини звільнення нічого не повідомлялося. Це звільнення генерального директора компанії виявилося повною несподіванкою для всіх, включно з найближчими бізнес-партнерами OpenAI (наприклад, для компанії Microsoft) [4].

Те, що сталося, свідчить про те, що проблеми, пов'язані зі швидким розвитком ШІ, дуже глибокі та не завжди можуть бути відомі громадськості.

Існують обґрунтовані підозри, що повсюдне впровадження систем ШІ може призвести до масового безробіття, виникнення непередбачуваних економічних і соціальних проблем. Крім того, ШІ може бути використаний для тотальної дезінформації (генерація фейкових, але вельми правдоподібних новин, підроблених фото і відеозображень, які не відрізнити від справжніх, точна імітація голосу людини, її почерку та інших даних).

Необхідність термінового вжиття заходів зі створення системи міжнародного регулювання штучного інтелекту у 2023 році стала очевидною для всіх.

У зв'язку з цим на початку листопада 2023 року було організовано та проведено міжнародні переговори на вищому рівні з безпеки ШІ (AI Safety Summit 2023). У переговорах взяли участь як представники урядів 29 держав (включно з представниками України), так і представники провідних компаній, що займаються розробленням систем штучного інтелекту (OpenAI, Google Deepmind та ін.), а також представники громадськості, експерти в цій галузі досліджень [5].

Показово, що ця зустріч відбулася в Bletchley Park (Велика Британія), у садибі, в якій під час Другої світової війни розташовувалася британська Урядова школа кодів і шифрів (Government Code and Cypher School, GC&CS) та в якій працював один із батьків-засновників сучасної інформатики Алан Тьюрінг. Саме Тьюринг запропонував використовувати метод, що дає змогу виявити наявність сильного ШІ в комп'ютерної програми (так званий "тест Тьюринга").

Завданнями зустрічі були виявлення проблем, які можуть бути створені "сильним AI" у разі його швидкої появи, і вироблення можливих заходів для їх запобігання, пошук можливостей мінімізації їхніх наслідків.

За підсумками зустрічі було узгоджено текст декларації, що отримала назву Блетчлійської декларації (The Bletchley Declaration). Декларацію підписали представники 29 країн, зокрема й представники України [6].

Незважаючи на виявлені під час зустрічі відмінності в думках, уряди різних країн світу зобов'язалися працювати разом над вирішенням проблем, пов'язаних із проблемою стрімкого розвитку систем штучного інтелекту.

У тексті Декларації зазначається, що штучний інтелект потенційно може забезпечити процвітання і мир для всього людства. Але для реалізації цих можливостей системи ШІ мають проєктуватися, розроблятися, впроваджуватися і використовуватися з дотриманням норм, що забезпечують безпеку його використання.

Також зазначено, що використання ШІ створює і значні ризики, які наразі остаточно не визначено і які потребують докладання спільних зусиль на міжнародному рівні для їхнього вивчення та вироблення заходів для усунення

потенційного негативного впливу систем ШІ на наявні й усталені практики та норми, зокрема на питання захисту прав людини, недоторканності приватного життя та захисту даних.

Крім того, в Декларації наголошується на можливості появи ризиків, пов'язаних з можливістю маніпулювання інформацією або створення дезінформації.

Слід зазначити, що, на жаль, проблеми з маніпулюванням інформацією та створення дезінформації вже перестали бути потенційними. Наразі ШІ активно використовується для створення діпфейків, текстів і зображень, що містять завідомо неправдиву інформацію. Крім того, однією з особливостей наявних систем ШІ виявилася їхня можливість генерувати фейкову інформацію без участі людини [7].

У Декларації наголошується, що найнебезпечнішою загрозою у теперішній час є ризики, що виникають у сфері кібербезпеки. Потенційний збиток від цих ризиків може виявитися катастрофічним. З урахуванням швидких темпів розвитку ШІ та невизначеності їхніх можливих наслідків, безперервно зростаючих інвестицій у ці технології, розв'язання цієї проблеми є вкрай нагальною справою.

Загалом слід зазначити, що Декларація має дещо запізнілий характер, бо належні рішення треба було ухвалювати раніше. На жаль, ніхто не зміг передбачити настільки швидкого розвитку технологій, що дали раптовий якісний стрибок. Тим часом серйозні проблеми (наприклад, зростаюче безробіття), що пов'язані з повсюдним впровадженням ШІ, вже з'явилися в деяких представників творчих професій (зокрема і у програмістів) [8].

У Блетчлійській декларації не пропонується вжиття якихось конкретних заходів, що значною мірою пов'язано з тим, що країни, які брали участь у зустрічі (такі як Сполучені Штати, Велика Британія, Європейський союз і Китай), мають конфліктні інтереси та використовують різні правові системи.

Важливо зазначити, що саміти з безпеки ШІ надалі проводитимуться регулярно, наступний саміт відбудеться в Кореї за шість місяців, а за рік заплановано саміт у Франції.

Список використаних джерел:

1. Чанишев Р.І. Проект Ai Act: перша спроба правового регулювання використання технологій штучного інтелекту в Європейському Союзі. Інформаційне суспільство: проблеми та перспективи: матеріали VIII Всеукраїнської науково-практичної конференції (м. Одеса, 2 черв. 2023 р.) /відп. ред. Н.І. Логінова. - Одеса, 2023. С. 42 - 44.
2. Чанишев Р.І. Проблеми розвитку та правового регулювання штучного інтелекту. Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень: у 2 т.:

матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редакцією С.В. Ківалова. – Одеса : Видавництво «Юридика», 2023. – Т. 1. С. 603-606.
3. OpenAI chief seeks new Microsoft funds to build 'superintelligence' URL: https://www.ft.com/content/dd9ba2f6-f509-42f0-8e97-4271c7b84ded. – Last access: 18.11.2023.
4. A statement from Microsoft Chairman and CEO Satya Nadella URL: http://surl.li/nhmfk. – Last access: 18.11.2023.
5. AI Safety Summit 2023 URL: http://surl.li/nhmfy. – Last access: 03.11.2023.
6. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023 URL: http://surl.li/nhmfd. – Last access: 10.11.2023.
7. The world's most powerful AI model suddenly got 'lazier' and 'dumber.' A radical redesign of OpenAI's GPT-4 could be behind the decline in performance. URL: http://surl.li/nhnea. – Last access: 03.11.2023.
8. IT Unemployment Soars to 4.3% Amid Overall Jobs Growth URL: http://surl.li/nhnlh. – Last access: 10.11.2023.

Ключові слова: Саміт з безпеки штучного інтелекту 2023, Декларація Блетчлі, системи штучного інтелекту, OpenAI, GPT-5, ризики розвитку та використання штучного інтелекту.
Keywords: AI Safety Summit 2023, The Bletchley Declaration, artificial intelligence systems, OpenAI, GPT-5, risks of development and use of artificial intelligence.

ПРАВОВА ПРИРОДА ШТУЧНОГО ІНТЕЛЕКТУ

Бааджи Наталія

доцент кафедри права інтелектуальної власності та патентної юстиції Національного університету «Одеська юридична академія», кандидат юридичних наук

Штучний інтелект - це нечітко визначений термін, який існує вже кілька десятиліть. Штучний інтелект можна розділити на низку унікальних підгалузей, таких як: машинне навчання, обробка природної мови, робототехніка та комп'ютерний зір – і це лише деякі з підгалузей штучного інтелекту. Штучний інтелект вже зміг перевершити людину в середньому тесті на IQ; створювати твори мистецтва, які не можна відрізнити від творів, створених людиною, і перемагати професійних гравців-людей [5;10]. Штучний інтелект також став статус-кво у повсякденній діяльності більшості технологічних компаній. Так, пошук Google від Alphabet використовує потужні алгоритми для видачі релевантних результатів і реклами, а система рекомендацій Amazon також покладається на методи машинного навчання, які сприяють підвищенню прибутку компанії та задоволеності клієнтів [4].

«Нині в провідних державах з розвинутими правовими порядками вже замислилися над питаннями визначення правового статусу штучного інте-

лекту, правового регулювання особливостей його розробки та використання. … надалі все це може зумовити глобальні зміни у правовій системі аж до розвитку повноцінних комплексних інститутів права та законодавства, можливо, галузей і підгалузей права» [13, с. 132-134].

Наразі проблематика, пов'язана з питаннями правового регулювання суспільних відносин у сфері використання та розробки штучного інтелекту актуалізується та знаходить своє віддзеркалення як у національній, так і зарубіжній правових доктринах. Правовідносини у сфері використання штучного інтелекту досліджувались у роботах таких науковців, як: І. Городиський, М. Карчевський, О. Кривецький, Ж. Павленко, О. Радутний, В. Токарєвої, Р. Стефанчук, Є. Харитонова, О. Харитонової, K. Hristov та інші.

Окреме місце займають наукові розвідки щодо використання штучного інтелекту у юридичній практиці (судова, адвокатська тощо) (Кривицький Ю., Радутний О., Храпенко О., Меденцев А., Bell F., Mihalache I., Mihalescu C., Chen A., Legg M., та інші.

Якщо еволюція людства є повільною та безперервною, відбувається з покоління в покоління, то світ роботів має іншу швидкість та закономірності свого шляху вдосконалення. В інтелектуальній робототехніці, яку зазвичай називають когнітивною робототехнікою, вже є досвід конфігурування машини, її апаратного та програмного забезпечення, адаптації до контексту. Цей процес характеризується великою інтенсивністю [2].

У першому наданому науковцями визначенні штучного інтелекту, запропонованому у 1956 році, зазначалося, що штучний інтелект має на меті зробити машини здатними навчатися і виконувати певні функції, які зазвичай виконує людина [9]. У літературі існує багато й інших визначень штучного інтелекту. Наприклад, штучний інтелект це те, що дозволяє об'єкту функціонувати належним чином і передбачливо у навколишньому середовищі. Крім того, штучний інтелект визначають як галузь комп'ютерних наук, що присвячена вирішенню когнітивних проблем, які зазвичай асоціюються з людським інтелектом, таких як: навчання, розв'язання проблем, розпізнавання мови та образів, прийняття рішень і переклад між мовами [6]. Штучний інтелект - це також теорія і розробка комп'ютерних систем, здатних виконувати завдання, які зазвичай вимагають людського інтелекту [3]

Штучний інтелект пережив винятковий прогрес у своїй здатності навчатися і міркувати, і, відповідно, був описаний як «технологія, що найшвидше розвивається». Як інструмент штучний інтелект не має жодних обмежень для потенційного діапазону використання. У своїй найфундаментальнішій основі інструменти з штучного інтелекту працюють, піддаючи обробці великі масиви даних алгоритмами швидкого машинного навчання, здатними розпізнавати шаблони, статистичну кореляцію, прогнозувати, робити висновки та вирі-

шувати проблеми, «адже «цифровий світ», який налічує понад 2,5 квінтильйона байт даних, створюється щодня» [8].

Наразі під штучним інтелектом в цілому фахівцями розуміється моделювання процесів людського інтелекту за допомогою машин, комп'ютерних систем, яке включає в себе навчання (отримання інформації та правила її використання), міркування (використання правил для досягнення приблизних або певних висновків) і самокорекцію.

Багато хто з вчених визначає штучний інтелект як «комп'ютерну програму, яка навчається». Під навчанням розуміється «глибоке навчання», яке полягає в тому, щоб розглядати те, що комп'ютер хоче вивчити, як масу даних, передавати ці дані в складну, багаторівневу мережу обробки даних (глибоку нейронну мережу), а потім перевіряти, чи відповідають отримані дані, оброблені мережею, вимогам. Якщо це так, то мережа зберігається в якості цільової моделі; якщо ні - знову і знову наполегливо підлаштовуються параметри мережі налаштувань, доки вихідні дані не будуть відповідати вимогам [11].

Важливою складовою дослідження технологій штучного інтелекту є правова компонента, яка пов’язана з визначенням правового статусу штучного інтелекта, авторським правом на твори, створені штучним інтелектом, відшкодування шкоди, завданої роботами тощо [16]. Впровадження і використання технологій штучного інтелекту матиме наслідки як для законодавства та політики в галузі інтелектуальної власності, так і для адміністрування систем інтелектуальної власності по всьому світу.

Штучний інтелект наразі не визнається суб'єктом права в більшості юрисдикцій, хоча питання про його правосуб'єктність вже дискутується серед дослідників і політиків. Разом з тим, у Резолюції Європейського Парламенту 2018/2088(INI) штучний інтелект позиціонується саме як «електронна особа». 21 квітня 2021 року Європейська комісія представила комплексну юридичну пропозицію щодо регулювання штучного інтелекту, так званий Artificial Intelligence Act (AIA, 2021) [1]. «За правовим підходом ЄС, поняття «система штучний інтелект» охоплює майже всі комп'ютерні програми. Єдине, що їх об'єднує, –це те, що вони спрямовані на обробку даних» [7].

Сьогодні поширеною є позиція, у відповідності до якої штучний інтелект за аналогією з тваринами може розглядатись як суб’єкт права, але правосуб’єктність його передбачає тільки правоздатність, але не у комплексі з дієздатністю. Є.О. Харитонов та О.І. Харитонова пропонують визнати роботів зі штучним інтелектом квазі-юридичною особою, а до переліку видів правосуб’єктності юридичної особи науковці пропонують включити також «кіберздатність» (здатність бути активним учасником відносин у ІТ-сфері). При цьо-

му, на думку вчених кіберздатність може реалізовуватися за допомогою не лише правочинів, а й юридичних вчинків [17].

Разом з тим, варто наразі підтримати думку тих дослідників, які розуміють робота й штучний інтелект як об'єкт цивільних правовідносин. До того ж регулювання цивільно-правової відповідальності на рівні споживчих відносин дає підстави розуміти штучний інтелект як продукт (товар). «Застосування технологій штучного інтелекту в таких сферах, як медицина або публічне адміністрування, спонукає до роздумів стосовно поширення на цей об'єкт цивільних прав правового режиму джерела підвищеної небезпеки. Це сприятиме кращому захисту прав користувачів технологій штучного інтелекту» [12]. Подібні погляди на штучний інтелект як об'єкт правового регулювання або об'єкт права поділяють й інші вчені-юристи.

З набранням чинності нового закону «Про авторське право та суміжні права» [15] результати роботи штучного інтелекту підпадає під правове регулювання як неоригінальний об'єкт, згенерований комп'ютерною програмою, що охороняється правом особливого роду (sui generis). «Ці права регулюють об'єкти, створені внаслідок роботи комп'ютерної програми. Ці об'єкти не містять творчого підходу та генеруються без участі людини. Як результат, особисті немайнові права на такі об'єкти не виникають, адже вони можуть належати лише фізичній особі, але аж ніяк не штучному інтелекту» [14].

Список використаних джерел

1. AIA (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. COM/2021/206 final. URL: https://eur-lex.europa.eu/legal-contentEN/ TXT/?uri=celex%3A52021PC0206
2. Azevedo A., Azevedo P. A. Digital Education, Work and Artificial Intelligence: Health and Law. EDEN Conference Proceedings 2020. (1) 277-288 DOI: 10.38069/edenconf-2020-ac0026
3. Chassignol M., Khoroshavin A., Klimova A., Bilyatdinova A Artificial Intelligence trends in education: a narrative overview. Procedia Computer Science. 2018, Vol. 136. P.16-24. URL: https://api.semanticscholar.org/ CorpusID:7021006
4. Hristov K. Artificial Intelligence and the Copyright Survey. 2019. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3490458
5. Hristov K. Policy Analysis: Artificial Intelligence and the Copyright Survey. Journal of Science Policy & Governance. 2020. Vol. 16, Is. 01.
6. Lim, W. M., Kumar, S., Verma, S., and Chaturvedi, R. Alexa, what do we know about conversational commerce? Insights from a systematic literature review. Psychol. Market. 2022. № 39, p. 1129–1155. doi: 10.1002/mar.21654
7. Mökander J., Axente, M., Casolari F., & Floridi, L. (2022). Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI regulation. Minds Mach, 2022. Vol. 32, P, 241–268. URL: https://doi.org/10.1007/s11023-021-09577-4

8. O'Keefe L., Rafferty J., Gunder A.,Vignare K. (2020). Delivering high-quality instruction online in response to COVID-19: Faculty playbook. Every Learner Everywhere.2020. URL:http://www.everylearnereverywhere.Org /resources
9. Pinnock R, McDonald J, Ritchie D, Durning SJ. Humans and machines: Moving towards a more symbiotic approach to learning clinical reasoning. Med Teach. 2020 Mar;42(3):246-251. doi:10.1080/0142159X .2019. 1679361. Epub 2019 Oct 28. PMID: 31658842
10. Silver, D., A. Huang, C. J. Maddison, A. Guez, L. Sifre, G. Van Den Driessche, J. Schrittwieser et al. Mastering the game of Go with deep neural networks and tree search. Nature. 2016. 529(7587): 484
11. Yu H., Guo Y. Generative artificial intelligence empowers educational reform: current status, issues, and prospects. Frontiers in Education. DOI: 10.3389/ feduc.2023.1183162 URL: https://www.frontiersin.org/articles/10. 3389 / feduc.2023.1183162/full
12. Марценко Н. Правовий режим штучного інтелекту в цивільному праві. Актуальні проблеми правознавства. 2019. Вип. 4. С. 91–98. doi: 10.35774/ app2019.04.091
13. Павленко Ж. Право в цифровій реальності. Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія. 2021. 2(49). https://doi.org/10.21564/2663-5704.49.229779
14. Петрів О. Штучний інтелект та авторське право. Центр демократії та верховенства права : вебсат. URL:https://cedem.org.ua/analytics /shtuchnyi -intelekt-avtorske-pravo/
15. Про авторське право та суміжні права : Закон України від 01.12.2022 № 2811-IX. База даних «Законодавство України» / ВР України. URL: https:// zakon.rada.gov.ua/laws/show/2811-20
16. Стефанчук Р. Інформаційні технології та право: quo vadis? Право України. 2018. № 1. С. 30–50. doi: https://doi.org/10.33498/louu-2018-01-030.
17. Харитонов Є.О., Харитонова О.І. До проблеми цивільної правосуб'єктності роботів: матеріали наук.-практ. конф. Інтернет речей: 244 проблеми правового регулювання та впровадження (м. Київ, 29 листопада 2018 р., НТУУ «КПІ ім. Ігоря Сікорського») /упоряд. В.М. Фурашев, С.О. Дорогих. Київ: Вид-во «Політехніка», 2018. С. 42-46

Ключові слова: штучний інтелект, авторські права, об'єкт, комп'ютерна програма
Keywords: artificial intelligence, copyright, object, computer program.

СУЧАСНІ ПРОБЛЕМИ ВЗАЄМОДІЇ ЛЮДИНИ І КІБЕРСЕРЕДОВИЩА

Руденко Каріна

студентка 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасний світ переживає революцію інформаційних технологій, яка впливає на всі сфери нашого життя. У життя сучасної людини активно впроваджуються інформаційно-комунікативні технології, які не мають аналогів у минулому[2]. Кіберсередовище стає все більш невід'ємною частиною нашої повсякденності, перетворюючи спосіб, яким ми спілкуємося, навчаємося, працюємо та відпочиваємо. Проте цей розвиток також викликає велику увагу до питань управління та соціально-психологічних аспектів цього кібернетичного простору. Під кіберпростором розуміється середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення (ПЗ) і послуг в Інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі[3].

Кіберсередовище не обмежується лише технічними аспектами, воно також формує соціальні та психологічні реалії нашого сучасного світу. Управління цим простором вимагає не лише технологічної експертизи, але і розуміння впливу цифрового середовища на суспільні відносини та психологію індивідів.

Управлінські та соціально-психологічні аспекти кіберсередовища є ключовими для розуміння сучасного світу, і їх вивчення допомагає сформувати більш повне уявлення про те, як ми функціонуємо у цьому цифровому столітті.

Соціально-психологічні аспекти кіберсередовища визначають спосіб, яким ми взаємодіємо в цифровому світі, впливають на нашу психологію. З одного боку, інтернет створює можливості для спілкування та співпраці, допомагає збирати та обмінюватися інформацією. З іншого боку, це середовище може призводити до проблем, таких як кібербулінг, інтернет-залежність та порушення приватності.

Співвідношення між онлайн та офлайн життям стає предметом соціальних та психологічних досліджень. Питання про вплив соціальних мереж, віртуальної реальності та онлайн-ігор на психіку та емоційний стан особистості стають все важливішими.

Стає зрозумілим, що на даному етапі розвитку людства, існування особистості поза взаємодією з комп'ютерними системами вже важко уявити. Проведення індивідами в мережі все більшої кількості часу, як виразна тенденція надання переваги мережевій комунікації та використання послуг кі-

берпростору з метою віртуальної самореалізації, підтверджують надзвичайну актуальність цього питання.

Один з ключових аспектів кіберсередовища є управління цим середовищем. Висока швидкість розвитку технологій та об'єм інформації, що генерується в інтернеті, створюють виклики для бізнесу, уряду та громадянського суспільства.

У цих умовах актуальною є проблема визначення змісту терміна "кібернетична безпека". Кібербезпека - це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах [1]. Зростання кількості кібератак та загроз вимагає розробки стратегій та заходів для захисту інформації, інформаційних систем та мереж. Організації повинні вдосконалювати свої підходи до кібербезпеки та навчати персонал виявляти й реагувати на ці загрози.

Психологічний вплив кіберсередовища на людину не може бути недооцінений. Онлайн-середовище впливає на наші ставлення, спосіб спілкування та сприйняття світу. Спілкування у соціальних мережах може впливати на формування самооцінки та ставлення до інших.

Кіберпростір також створює виклики для соціальних відносин. Питання етики та правил спілкування в інтернеті стають важливими, оскільки цифровий світ дозволяє анонімність і може призводити до негативних проявів, таких як кібербулінг та онлайн-гонитви.

Співвідношення між реальним та віртуальним життям стає предметом соціальних досліджень. Вирішення проблематики негативних проявів кіберпростору, є надзвичайно важливим завданням, оскільки ці явища можуть значущо впливати на психологічний стан та добробут індивідів. Нижче наведено кілька способів вирішення цієї проблематики:

- Просвітницькі заходи: Один з ключових шляхів боротьби з кібербулінгом та онлайн-гонитвами - це посилення освіти та усвідомлення проблеми серед дітей, підлітків та їх батьків. Школи та організації повинні надавати інформацію про небезпеки цифрового світу та способи виявлення та запобігання кібербулінгу.
- Створення безпечних онлайн-середовищ: Платформи та соціальні мережі повинні приділяти особливу увагу виявленню та блокуванню користувачів, які здійснюють кібербулінг чи онлайн-гонитви. Технологічні рішення, такі як алгоритми виявлення образливих коментарів, можуть бути корисними.
- Підтримка та консультування: Важливо створити середовище, де жертви кібербулінгу та онлайн-гонитв можуть шукати допомогу та підтримку. Психологічна підтримка та консультування можуть допомогти жертвам подолати емоційні та психологічні труднощі.

Отож, кіберсередовище стало необхідною складовою сучасного світу, і його управління вимагає особливої уваги та підходів. Управління кібербезпекою стає надзвичайно важливим завданням у цифровому світі. Організації повинні розробляти стратегії та заходи для захисту інформації та інформаційних систем від кіберзагроз.

Список використаних джерел:

1. Баранов, О. А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика, 2014, 2.42: 54-62.
2. Данильян, О. Г.; дзьобань, о. П. Віртуальна реальність і кіберпростір як атрибути сучасного суспільства. Інформація і право, 2020, 4 (35): 9-21.
3. Завгородня, Ю. В. Кіберпростір як сучасна платформа для політичних конфліктів. Publishing house “baltija publishing”, 2021.

Ключові слова: кіберпростір, кіберсередовище, кібербезпека, онлайн середовище
Keywords: cyberspace, cyber environment, cybersecurity, online environment

Науковий керівник : к. ф.-м. н., доцент Черевко Є.В.

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ У СИСТЕМІ МІСЦЕВОГО САМОВРЯДУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ

Холостенко Світлана

студент 2-го курсу магістратури ННІ публічної служби та управління Національного університету «Одеська політехніка»

Ровинська Катерина

доцент кафедри державознавства, права та європейської інтеграції Національного університету «Одеська політехніка», кандидат наук з державного управління, доцент

За умов широкомасштабної агресії на територію України визначальну роль у здатності реалізовувати власні повноваження посадовими особами місцевого самоврядування зіграли впроваджені до того часу цифрові технології та інструменти, які зберегли систему місцевого самоврядування для функціонування, а, також надали посадовим особам місцевого самоврядування реалізовувати закріплені повноваження та завдання.

Застосування цифрових технологій у діяльності органів місцевого самоврядування дозволило зробити процедуру надання публічних послуг ефективною у часі та ресурсних затратах, проте виявило певні виклики щодо потреби розвитку цифрових компетентностей членів громади та посадових осіб місцевого самоврядування.

За умов карантину через пандемію COVID-19, а згодом через війну, органи місцевого самоврядування України подекуди вимушено перейшли в онлайн-режим на віддалену роботу, використовуючи системи електронного документообігу, голосування з використанням електронних кваліфікаційних підписів на пленарних засіданнях.

Визначений механізм електронного урядування систематизує документообіг, сприяє прозорості та відкритості влади, покращує роботу та економить бюджетні кошти, час посадових осіб місцевого самоврядування та держслужбовців [1]. Автоматизована система електронного документообігу АСКОД дозволяє автоматизувати процеси опрацювання документів шляхом впровадження єдиної технології роботи з різноманітними службовими документами, кореспонденцією, зверненнями громадян та іншими фінансово-господарськими документами [2].

Практиками успішного впровадження цифрових інструментів, які оптимізують систему місцевого самоврядування є:

– електронні сервіси: надання електронних послуг громадянам та бізнесу у Центрах надання адміністративних послуг (ЦНАП) пропонує зручну онлайн реєстрацію на послуги, електронну подачу заяв та документів, електронні платежі тощо;

– електронна звітність: можливість електронної подачі звітів та документів від підприємств та організацій сприяє зменшенню бюрократичних процедур та швидшому обміну інформацією;

– електронна взаємодія з громадянами: використання електронних каналів для спілкування з громадянами (вебсайтів, соціальних мереж, електронної пошти, месенджерів тощо) дозволяє швидко дистанційно вирішувати питання громадян у зручній для них формі;

– електронні петиції як особлива форма колективного звернення громадян до Президента України, Верховної Ради України, Кабінету Міністрів України, органу місцевого самоврядування є зручним способом звернення до влади для громадян. Для формування і подання такої петиції достатньо зареєструватись, викласти своє звернення на сайті та спостерігати за кількістю голосів, поданих на підтримку петиції. З моменту оприлюднення електронної петиції її може прочитати та підтримати кожен громадянин, а за умови набрання необхідної кількості голосів вона є обов'язковою до розгляду відповідними органами влади [3, 4].

Наразі, проблемними викликами щодо широкого впровадження цифрових технологій у діяльність органів місцевого самоврядування є:

– кібербезпека: разом із впровадженням цифрових технологій стрімко зростають ризики кібератак та витоків персональних даних. Задля забезпечення надійного рівня кібербезпеки для збереження конфіденційності даних

громадян важливо: запровадити програми ІТ-навчання персоналу органів місцевого самоврядування з правил кібергігієни та вимог кібербезпеки; дотримуватись розроблених процедур щодо кібергігієни; користуватись безпечним ліцензійним програмним забезпеченням; моніторити рівень захищеності використовуваних електронних ресурсів фахівцями з кібербезпеки [5];

– цифрова грамотність: для ефективного впровадження та функціонування електронного урядування варто забезпечити належний рівень цифрової грамотності і навичок роботи співробітників відділів із програмними системами, використання електронного кваліфікаційного підпису для реалізації повноцінного і дієвого електронного документообігу, що надаватиме можливість їм якісно і швидко виконати свої посадові обов'язки.

Ще однією успішною цифровою технологією, яка пройшла випробування війною в Україні, є Єдина інформаційна система соціальної сфери (ЄІССС). Вона дозволила автоматизувати та централізувати ділові процеси в соціальній сфері, зробила доступними низку виплат, зокрема постраждалим від підриву Каховської ГЕС, а також сервіси для ВПО.

Отже, повсюдне впровадження цифрових технологій, зокрема систем електронного документообігу в діяльність органів місцевого самоврядування скорочує витрати коштів на матеріально-технічні ресурси, покращує стан виконавчої дисципліни та якість надання адміністративних послуг населенню громади, а в умовах воєнного стану, є визначальним підґрунтям ефективної системи місцевого самоврядування.

Список використаних джерел:

1. Гавриленко Т.С. Упровадження сучасних технологій в органах місцевого самоврядування України на прикладі міста Києва. Юридичний науковий електронний журнал. 2021. № 9. С. 18-20. DOI: 10.32782/2524-0374/2021-9/2.
2. Система електронного документообігу АСКОД. URL: https://askod.online/terms-of-use.ua.html.
3. Закон України «Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції». Голос України від 28.07.2015. № 134. URL: https://zakon.rada.gov.ua/laws/show/577-19/card6#Public
4. Закон України «Про звернення громадян». Відомості Верховної Ради України (ВВР). 1996. № 47. Ст.256. URL: https://zakon.rada.gov.ua/laws/show/393/96-bp#Text.
5. Трофименко О.Г. Аналіз стану е-урядування в Україні. Кібербезпека в сучасному світі: актуальні виклики : матер. II всеукр. наук.-практ. конф. (20 листопада 2020 р.). Одеса: Видавничий дім «Гельветика», 2020. С. 58–61.

Ключові слова: інформаційна система соціальної сфери, електронні сервіси, електронне урядування, органи місцевого самоврядування, цифрові компетентності.
Keywords: social information system, e-services, local governments, e-government, digital competences.

Секція 4. УПРАВЛІНСЬКІ ТА СОЦІАЛЬНО-ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРСЕРЕДОВИЩА

ПАРИТЕТ ТРАНСПАРЕНТНОСТІ ТА КІБЕРБЕЗПЕКИ У ХОЛОКРАТИЧНІЙ МОДЕЛІ УПРАВЛІННЯ БІЗНЕСОМ

Горбаченко Станіслав

завідувач кафедри кібербезпеки Національного університету «Одеська юридична академія», доктор економічних наук, професор

Управління бізнесом можна визначити як цілеспрямовану діяльність суб'єкта управління (власника чи менеджера бізнесу/підприємства) щодо об'єкта управління через відповідний механізм управління (систему принципів, методів, функцій, інструментів тощо) з метою збільшення прибутку та цінності для клієнта, удосконалення самого бізнесу та його процесів [1, с. 78].

В останні роки, саме в контексті організації управління бізнесом дуже часто згадується холократія, тобто система, в якій влада і прийняття рішень розподілені між командами за принципом самоорганізації. На відміну від більш звичної для українського бізнесу вертикальної управлінської ієрархії холократія передбачає створення ролей, які наділені конкретними обов'язками та відповідальністю. При цьому проводиться чітке розмежування між ролями і кількістю співробітників, які їх виконують, адже одна людина може виконувати відразу декілька ролей одночасно.

Незважаючи на те, що перші згадки про холократичну модель датуються ще 1960-ми роками минулого сторіччя, популярність і широке розповсюдження вона отримала вже після 2014 року. Як сучасна модель управління бізнесом холократія довела свою ефективність у численних компаніях різних сфер діяльності, насамперед, в IT сегменті де її використовують в компаніях Google, Amazon, Facebook, Valve тощо.

Основною фундаментальною ідеєю, яка обумовила виникнення холократії є те, що концентрація влади нагорі спричиняє безліч проблем і виявляє тіньовий бік кожної людини, а саме недовіру, страх, заздрість, інтриги, що породжує покору й образу. Як наслідок, у такому середовищі немає місця ні мотивації, ні самовираженню [2].

Відтак на практиці використання холократичної моделі означає, що бізнес майже повністю відмовляється від менеджменту середньої ланки, тобто залишаються виключно стратегічні управлінці-візіонери, як представники топ менеджменту та пересічні співробітники, які, у свою чергу, мають розширені повноваження щодо прийняття рішень у власній функціональній зоні.

В теорії чи не головною перевагою холократії вважається безпековий аспект, адже вона зменшує ризик концентрації влади в руках однієї особи

або невеликої групи осіб, а кожен співробітник може та, навіть, повинен вносити свій вклад у прийняття рішень. В цьому сенсі для переходу до холократичної моделі управління, потрібно перш за все воля та бажання власників компанії, ради директорів та CEO (головний виконавчий директор). Без їхньої підтримки побудувати вказану модель не можна. Адже, зазвичай як тільки з'являються проблеми, лідери бажають брати усе під повний контроль, та повертаються до традиційних методів управління. Принципи холократії повинні перш за все відповідати принципам мислення лідерів організацій [3].

Іншою важливою ознакою холократичній моделі управління бізнесом є транспарентність, тобто прозорість та відкритість інформації для всіх співробітників, без приховування або обмеження доступу. Транспарентність сприяє кращому розумінню колективом бізнес-процесів, стимулює співпрацю між відділами та покращує взаємодію з клієнтами. Співробітники будь-якого рівня мають можливість бачити загальну картину, що дозволяє їм працювати результативніше та ефективніше.

Однак відкритість обумовлює й відповідні ризики, які досягають апогею у кіберсередовищі, адже інформація стає доступною не тільки для внутрішніх, але й для зовнішніх користувачів. Паралельно із цим система базується на взаємодії різних ролей, тому можливим є виникнення конфліктів та непорозумінь між співробітниками, що також може призвести до витоку інформації. А те, що відповідальність розподілена між численними ролями ускладнює визначення відповідальності у випадку проникнення в систему або інших проблем з безпекою.

В цьому сенсі побудова ефективної системи кібербезпеки, яка при цьому не порушує фундаментальних принципів холократії, виступає ключовим елементом для захисту конфіденційної інформації та даних суб'єктів бізнесу. Адже, незважаючи на децентралізовану структуру, будь-який суб'єкт бізнесу прагне створити ефективні системи контролю та моніторингу, щоб забезпечити стабільність та безпеку бізнес-процесів.

З точки зору практичних інструментів для забезпечення кібербезпеки у холократичній моделі управління бізнесом необхідно розробити чіткі протоколи та процедури, що регулюють доступ до інформації. Наприклад, можна впровадити двофакторну автентифікацію для доступу до важливих систем або використовувати спеціалізоване програмне забезпечення для моніторингу та виявлення зловмисних дій. Також, важливо розуміти, що побудова ефективної системи кібербезпеки не обмежується тільки технічними аспектами. Ефективним інструментом можуть виступати тренінги для співробітників щодо основ безпеки, правил поведінки в мережі Інтернеті та розуміння

потенційних загроз є невід'ємною частиною створення культури безпеки суб'єкта бізнесу.

Таким чином холократична модель управління бізнесом створює нові можливості для підприємств та організацій, але, одночасно, привносить й нові виклики у контексті кібербезпеки. Тому для її ефективного впровадження необхідно враховувати обидва аспекти і забезпечити паритет між ними. Щодо конкретних дій для забезпечення кібербезпеки в умовах холократії, мова може йти про створення спеціальних ролей, відповідальних за кібербезпеку, розробку процедур для оцінки кіберризиків, а також навчання співробітників основам кібербезпеки в умовах відкритості та прозорості.

Список використаних джерел:

1. Єршова О. О., Гончаренко І. М. Сучасні моделі управління розвитком бізнесу: сутність, види, інноваційні бізнес-моделі. Журнал стратегічних економічних досліджень. 2022. № 2(7). С. 75-85.
2. Чорній В. В., Приступа Т. В. Бірюзові організації: майбутнє чи модний тренд? URL: http://www.pev.kpu.zp.ua/journals/2019/5_16_uk/5_16_2019.pdf
3. Джур О. Є., Шепеленко Д. Ю. Застосування Teal-моделі в системі управління української компанії. Економіка та суспільство. 2021. № 32. URL: https://economyandsociety.in.ua/index.php/journal/article/download/849/816/

Ключові слова: управління, холократія, транспарентність, ризики, кібербезпека.
Keywords: governance, holocracy, transparency, risks, cybersecurity.

ІНТЕГРАЦІЯ КРИТИЧНИХ КОМПОНЕНТІВ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВОДНОГО ТРАНСПОРТУ

Пунченко Наталія

в.о. завідувача кафедри інформаційних технологій Одеського державного аграрного університету, кандидат технічних наук, доцент

В інноваційному суспільстві така галузь, як судноводіння під час зародження, визначила себе до інноваційної. Такому визначенню є доказ. Взято основний курс на збирання, інтеграцію, передачу та аналіз інформації про ситуацію на морі, на борту кораблів та на березі за допомогою електронних засобів з метою забезпечення навігації «від причалу до причалу», інновації суднобудування та технології освоєння світового океану [1]. Світ судноплавства зараз потребує управління безпекою сучасних інформаційних мереж водного транспорту – це комплекс заходів та технологій, спрямованих на забезпечення надійної та безпечної роботи мереж, що використовуються у сфері водного транспорту. Доктрина управління інформаційної безпекою показано рисунку 1. Комплекс є важливим аспектом у сучасній судноплавної

промисловості, оскільки водна промисловість включає пасажирські, вантажні перевезення і управління портової інфраструктурою. Ось деякі ключові аспекти управління безпекою в інформаційних мережах: захист від кіберзагроз, забезпечення надійності засобів зв'язку для координації дій, моніторингу погоди та інших аспектів роботи водного транспорту, запобігання аваріям, дотримання нормативів та стандартів. Особливістю сучасних інформаційних мереж, що вони інтерпретуються з наявністю штучного інтелекту. Сучасні інформаційні мережі належать до складних систем. Які розвиваються на користь систем управління роботою флоту, і що дає можливість формуванню віртуальних мультисервісних мереж з динамікою зміни структурних параметрів. Забезпечують вимогу інших систем управління генерацією інформаційних послуг. А ось інтенсифікація засобів і засобів захисту інформаційних ресурсів істотно ускладнює контроль низки параметрів, що викликає необхідність розробки засобів і засобів захисту у взаємозв'язку з процесом розробки методів і засобів контролю. Відмінна особливість сучасних інформаційних мереж управління в судноводженні полягає в наявності тісної взаємної залежності їх основних інтеграційних властивостей: готовності, мобільності, пропускної спроможності, скритності, доступності, керованості.

Рис. 1. Управління інформаційної безпекою.

Посилення взаємозалежності основних властивостей є наслідком конвергенції технологій. Крім того, новою інтегративною властивістю інформаційних мереж є наявність і характеристики розподіленої системної пам'яті, що дозволяє протягом певного періоду часу зберігати повідомлення, що передаються, що радикально впливає на інші властивості мережі. На додаток, системи мають агентів природного (професіоналізм) та штучного інтелекту. У таких системах агенти штучного інтелекту не обов'язково наділені самосвідомістю, але, на відміну від сучасних нейромереж, здатні справлятися з широким колом завдань у різних умовах. Вони вдаються до реалізації технологій вузько спеціалізованого штучного інтелекту, що вимагає налаштування та повторної перевірки з боку людини. Сукупність агентів за певних умов утворює суперсистему, поведінка якої може бути повною мірою формалізовано рамках класичної теорії управління. Труднощі формалізації пов'язані з високим ступенем невизначеності інфраструктури та впливом людського фактору (професіоналізму) у динаміці функціонування суперсистеми.

Суперсистема характеризується віртуальністю функціональної структури, в контексті інформаційної безпеки вказують на використання віртуальних систем або технологій для моделювання функцій та завдань у межах суперсистеми судноводіння. Віртуальні системи допомагають відтворювати та аналізувати різноманітні сценарії та ситуації без необхідності реального фізичного втручання. Такий підхід дозволяє удосконалювати та тестувати системи безпеки та управління судовими процесами. Також вказує на комплексну систему, яка включає у собі різноманітні підсистеми для управління судном та навігації. Віртуальність тут може використовуватись для створення віртуальних аналогів окремих компонентів суперсистеми для аналізу та тестування їх функціональності. У цьому можливі конфлікти управління системами управління безпекою сучасних інформаційних мереж.

Інформаційно-алгоритмічне забезпечення сучасної інформаційної мережі судноводіння в рамках кібербезпеки охоплює широкий спектр технологій та заходів для забезпечення безпеки та надійності інформаційних систем, що використовують у морському судноплавстві [2-4]. І є багаторівневими, включають фундаментальну та адаптаційну частину, заміна якої забезпечує нову спеціалізацію елементів. Технології Soft Definition Network (SDN), Network Function Virtualization (NFV), Soft Definition Radio (SDR) приклади такого забезпечення.

У зв'язку з цим інформаційна система загалом має пам'ять і гнучкість поведінки, для стійкого функціонування якої має виконуватися така умова: швидкість адаптації елементів до нових функціональних завдань має бути вищою за швидкість зміни зовнішніх факторів, що впливають [5]. У зв'язку з

цим актуальною є тематика досліджень, що існують та розробка нових підходів до забезпечення якісного зворотного зв'язку в системі управління безпекою сучасних інформаційних систем судноплавства, що й становить мету роботи. Існуюча методологія управління складними системами передбачає визначення необхідних умов організації управління. Роботи авторів Крючкової Л.П., Трофименка А.О., Майданевич С.Б., Лахно В.А. показують, що вимоги сучасних систем моніторингу інформаційних систем, які генерують нескінченний потік подій безпеки, які задля забезпечення повноти охоплення контролем і забезпечення режиму реального часу налаштовані фіксацію зміни параметрів кожного з елементів системи без деталізації його стану. Виникає надлишок повідомлень та нестача їхнього контексту, що ускладнює завдання ідентифікації стану безпеки та потребує додаткових перевірок, отже, знижується оперативність реагування на інциденти безпеки. Таким чином, виникає завдання обробки у режимі, близькому до реального часу, великого потоку повідомлень про події безпеки без втрати їхньої змістовності. Це і не дозволяє повною мірою забезпечувати взаємодію одночасно по вертикалі та горизонталі. Іншими словами, технологічні недоліки, не дають можливості вирішувати завдання взаємодії та контролю у сучасних інформаційних систем.

Необхідно домагатися стійкості у частині передбачуваності поведінки та повної функції управління системою. Це можливо за рахунок синтезу інтелектуальної системи контролю на основі теорії функціональних систем та формалізації процесу зіставлення, відбору та об'єднання (синтезу) різноманітних за значенням аферентних потоків збуджень, що становить основу початкового етапу розгортання функціональної системи поведінки. Скорочення циклу контролю ІБ можливе на основі нового підходу до забезпечення самоорганізації системи контролю ІБ за заданими критеріями якості результатів контролю шляхом автоматичної генерації профілів контролю та самосинхронізації мультиагентної мережі контролю.

Список використаних джерел:

1. N. Punchenko, V. Strelbitskyi, O. Tsyra. Shaping the future of the marine industry as a condition for adaptation in an innovative society. Short Paper Proceedings of the 2nd International Conference on Intellectual Systems and Information Technologies (ISIT 2021). CEUR Workshop Proceedingsthis link is disabled, 2021, 3126 CEUR-WS.org, ISSN 1613-0073. P. 103–107.
2. Analysis of cyber security aspects in the maritime sector. ENISA (10.2011). P. 31.
3. AIS Exposed: Understanding Vulnerabilities & Attacks 2.0 (4. video), Dr. M. Balduzzi, Black Hat Asia. (2014).
4. Preparing for Cyber Battleships – Electronic Chart Display and Information System Security, Yevgen Dyryavyy, NCC Group. (03.03.2014).

5. Слюсаренко А. Впровадження та вплив кібер-безпеки на сучасне технічне обслуговування обладнання суден і судноплавних компаній. Λ΄ΟΓΟΣ. ОНЛАЙН. 2020. № 10. Водний транспорт № 1 (37) 2023 187 DOI: 10.36074/2663-4139.10.09.
6. Лахно В.А. Підвищення кібербезпеки інформаційно-комунікаційних систем транспорту. Безпека інформації. 2016. Том 22. No 1. С. 44-50.

Ключові слова: інформаційні системи судноводіння, морський транспорт, кіберзахист.
Keywords: navigation information systems, maritime transport, cyber defense, threat.

СТРАТЕГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ ТА ІННОВАЦІЙНОГО УПРАВЛІННЯ ДЛЯ СТАЛОГО РОЗВИТКУ СУСПІЛЬСТВА

Котлубай Вячеслав

доцент кафедри національної економіки Національного університету «Одеська юридична академія», кандидат економічних наук, доцент

Сучасний світ характеризується швидким розвитком інформаційних технологій та комунікацій, що відкриває нові можливості для соціального, економічного та культурного прогресу. Однак, разом з цим, зростає й обсяг кіберзагроз, які ставлять під загрозу безпеку, стабільність та благополуччя суспільства. Кіберзлочинність, кібершпигунство, кібертероризм, кібервійна, кібератаки на критичну інфраструктуру, порушення конфіденційності, цілісності та доступності інформації - це лише деякі з викликів, з якими стикаються держави, організації та окремі особи в кіберпросторі.[1, 2]

У цьому контексті, кібербезпека стає одним з ключових факторів сталого розвитку суспільства, який вимагає стратегічного підходу та інноваційного управління. Стратегічний підхід передбачає визначення цілей, пріоритетів, принципів та механізмів забезпечення кібербезпеки на національному та міжнародному рівнях, а також врахування глобальних тенденцій, ризиків та можливостей в кіберсередовищі. [3]

Стратегічний підхід до кібербезпеки має бути застосований на національному та міжнародному рівнях, що означає, що держава має враховувати свої внутрішні та зовнішні інтереси, можливості та обмеження, а також співвідносити свої цілі, пріоритети, принципи та механізми з тими, що мають інші держави, міжнародні організації та інші зацікавлені сторони. В якості цілей повинно бути встановлено: захист суверенітету, прав та інтересів громадян, інтеграція до європейських та євроатлантичних структур, розвиток інформаційного суспільства. При цьому головними пріоритетами є: посилення національної системи кібербезпеки, протидія кіберзагрозам, співпраця з міжнародними партнерами, інноваційний розвиток. Все це повинно бути реалізо-

вано на підставі принципів відповідальності, прозорості, відкритості, гнучкості та партнерства.

Інноваційне управління передбачає використання нових технологій, методів та практик для підвищення ефективності, гнучкості та адаптивності систем кібербезпеки, а також залучення та співпрацю всіх зацікавлених сторін: державних органів, бізнесу, громадськості, науки та освіти. [4]

Основними проблемами в сфері кіберпростору, з якими стикається Україна в умовах війни, є:

- порушення кібербезпеки та кібератаки на критичну інфраструктуру, державні органи, підприємства, ЗМІ, громадські організації та окремих громадян, що створює ризики для національної безпеки, стабільності, демократії та прав людини;
- недостатність ресурсів, знань та компетенцій для ефективного протидії кіберзагрозам, розробки та впровадження стратегічних документів, нормативно-правових актів, стандартів та механізмів забезпечення кібербезпеки на різних рівнях [5, 6];
- низький рівень інтеграції та співпраці між різними секторами та зацікавленими сторонами у сфері кібербезпеки, що ускладнює координацію, обмін інформацією та досвідом, навчання та підвищення обізнаності та зацікавленості;
- відставання в розвитку та використанні інноваційних технологій та рішень для підвищення ефективності, гнучкості та адаптивності систем кібербезпеки, а також для підтримки та розвитку інших сфер суспільного життя, таких як освіта, охорона здоров'я, енергетика, транспорт, е-урядування тощо.

Можливими шляхами вирішення наведених проблем з кібербезпеки та інноваційного управління в Україні є:

- розробка та впровадження нового Закону України "Про кібербезпеку", який би відповідав сучасним викликам та стандартам, а також оновити НД ТЗІ та КСЗІ відповідно до міжнародних рекомендацій та практик [1];
- створення та фінансування Національного центру кібербезпеки, який би координував дії всіх суб'єктів кібербезпеки, забезпечував моніторинг, аналіз, прогнозування та реагування на кіберзагрози, а також проводив навчання, просвітування та підвищення обізнаності з питань кібербезпеки [7];
- розширення та поглиблення співпраці між державним, приватним та громадським секторами у сфері кібербезпеки, зокрема за допомогою державно-приватного партнерства, обміну інформацією та досвідом, створення спільних проєктів та ініціатив [8];

– стимулювання та підтримка розвитку та використання інноваційних технологій та рішень для підвищення ефективності, гнучкості та адаптивності систем кібербезпеки, а також для підтримки та розвитку інших сфер суспільного життя, таких як освіта, охорона здоров'я, енергетика, транспорт, е-урядування;

– зменшення технологічної залежності від іноземних виробників IT-продукції, та розвиток власної національної IT-індустрії, забезпечуючи її конкурентоспроможність, якість та безпеку.

Стратегічний підхід до кібербезпеки та інноваційне управління є необхідними умовами для сталого розвитку суспільства в умовах глобалізації та цифровізації. Україна, яка зазнає великих викликів та загроз у зв'язку з війною, має визначити свої цілі, пріоритети, принципи та механізми забезпечення кібербезпеки на національному та міжнародному рівнях, а також використовувати нові технології, методи та практики для підвищення ефективності, гнучкості та адаптивності систем кібербезпеки, а також для підтримки та розвитку інших сфер суспільного життя.

Зміни, які відбуваються у світі, вимагають від країн, зокрема від України, активного впровадження новаторських рішень у сфері кібербезпеки та управління змінами. Однією з основних складових є розвиток кібербезпеки для захисту важливих національних інфраструктур та конфіденційної інформації від кіберзагроз та кібератак. Це включає в себе розробку стратегій та політик, вдосконалення законодавства, створення та підтримку кібервійськ, та надання освіти та підтримки для ефективного управління кібербезпекою.

Окрім цього, інноваційне управління змінами дозволяє пристосовуватися до швидкозмінних умов та впроваджувати нові стратегії та методи для вирішення економічних, соціальних, технологічних та політичних викликів. Цей підхід стимулює креативність та інновації, що є важливими складовими для забезпечення сталого розвитку суспільства.

Україна повинна активно співпрацювати з міжнародними організаціями та партнерами з метою обміну досвідом та розробки спільних підходів до кібербезпеки та управління змінами. Тільки шляхом взаємодії та інновацій можна ефективно відповісти на сучасні виклики та забезпечити безпечний та сталий розвиток у цифровому віці.

Список використаних джерел:

1. Кібербезпека бізнесу в умовах нестабільності. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html. (дата звернення: 4.11.2023)
2. Микитенко Д.О. Захист інформації та кібербезпека як складова частина національної безпеки України. Юридичний науковий електронний журнал. 2020. №8. С. 381-385.

3. Дубов Д. В. Формуючи нову стратегію кібербезпеки україни: чи можемо уникнути помилок першої спроби стратегування? URL: https://niss.gov.ua/sites/default/files/2021-01/tezy-dubov-2.pdf. (дата звернення: 4.11.2023)
4. Проєкт Стратегі] кібербезпеки України (2021 – 2025 роки). URL: https://rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf. (дата звернення: 4.11.2023)
5. Соціолог назвав проблеми, з якими зіткнуться українці після закінчення війни. URL: https://www.unian.ua/society/viyna-v-ukrajini-z-yakimi-zitknutsya-ukrajinci-pislya-peremogi-nad-rosiyeyu-novini-ukrajini-11860779.html. (дата звернення: 4.11.2023)
6. Економічні наслідки війни в Україні відчують далеко за її межами. URL: https://www.bbc.com/ukrainian/news-60619288. (дата звернення: 4.11.2023)
7. Уряд ухвалив Положення про організаційно-технічну модель кіберзахисту. URL: https://www.kmu.gov.ua/news/uryad-uhvaliv-polozhennya-pro-organizacijno-tehnichnu-model-kiberzahistu. (дата звернення: 4.11.2023)
8. Кібербезпека та управління ризиками IT. URL: https://kpmg.com/ua/uk/home/services/consulting/technology/information-protection-and-cyber-security.html. (дата звернення: 4.11.2023)

Ключові слова: кібербезпека, кіберзагрози, стратегічний підхід, інноваційне управління, сталий розвиток, суспільство.
Keywords: cybersecurity, cyberthreats, strategic approach, innovative management, sustainable development, society.

ЗАСТОСУВАННЯ ІНСТРУМЕНТІВ КІБЕРБЕЗПЕКИ В ЕКОНОМІЦІ ЗАМКНУТОГО ЦИКЛУ

Клєвцєвич Наталія

старший науковий співробітник відділу розвитку підприємництва ДУ «Інститут ринку і економіко - екологічних досліджень НАН України», кандидат економічних наук, доцент

Останнім часом вся світова економічна система працювала в парадигмі лінійності, значимість якої в тому, що використання ресурсів виробництва відбувалося на базі ресурсів природного середовища, які застосовувалися для напрацювання різноманітних продуктів і ставали відходами після того як були використані. Але така соціально-економічна конструкція масового виробництва й масового ж споживання наразі є дуже небезпечною в перспективі для стійкої життєдіяльності всього людства, яке наразі використовує природних ресурсів на порядок більше, ніж може відновити. Економіка замкнутого циклу (циркулярна економіка, кругова економіка) створює можливості для зміни цього. У масштабах всього світу модель економіки замкнутого циклу розтлумачується як можливість функціонування в умовах оптимального використання економікою ресурсів, які є в її розпорядженні. В ній ресурси

застосовуються, але не витрачаються взагалі. Така економічна схема передбачає економічне зростання з перетворенням лінійної виробничі практики. Але не дивлячись на те, що перехід від лінійної моделі до моделі економіки замкнутого циклу глобально тільки розпочинається, потенціал таких змін дуже значний. Економія тільки за рахунок скорочення витрат на матеріали у світі оцінюється експертами в 1 трлн доларів США на рік до 2025 року у разі переходу до бізнес-моделей економіки замкнутого циклу [1]. Наразі лише маленька доля економіки світу є замкнутою, проте світова спільнота поступово визнає значимість такої трансформації для забезпечення сталого зростання та розвитку. Цифрові технології відіграють важливу, якщо не сказати ключову роль у забезпеченні такого переходу, що вимагає випробування нових уявлень для трансформації моделі виробництва та споживання. Впровадження цифрових технологій належать до тих потенційних можливостей, що використовуються для створення умов для переходу до економіки замкнутого циклу. Але нові технології та бізнес-моделі, а також швидкість з якою вони впроваджуються несуть нові ризики. Адже невпевненість користувачів у безпеці онлайн-сервісів та захисті конфіденційності загрожує можливості використання всього потенціалу інформаційних та комунікаційних технологій для стимулювання інновацій, циркулярного економічного зростання та прогресу у напрямку таких трансформаційних перетворень. Подібним загрозам піддаються усі без виключення країни світу, а проблема кібербезпеки суттєво актуалізується. З цього слідує, що подальший розвиток циркулярної економіки на умовах цифровізації і отримання людством її переваг нерозривно пов'язаний із одночасною розбудовою відповідних систем кібербезпеки.

Трансформація економіки у напрямку циркулярності потребує застосування прогресивних інноваційних рішень на всіх етапах життєвого циклу продукції, більшість з яких передбачають активізацію використання цифрових технологій. І з цього погляду цифровізація може прискорити та зробити більш ефективним перехід до економіки замкнутого циклу, закриваючи ланцюжок ресурсів та надаючи повну інформацію про їхню наявність, місцезнаходження та стан товарів тощо [1]. Цифрові технологічні рішення містять в собі великий потенціал для створення відповідних умов для переходу до циркулярної економіки, тому що тільки завдяки її прогресивним інноваціям можливо докорінно трансформувати існуючі наразі уявлення в більш екологічні та стійкі (рис.1.).

Рис. 1. Взаємозв'язок ціфровізації та циркулярної економіки для досягнення цілей сталого розвитку

Джерело: складено автором

Саме вони можуть забезпечити зміну існуючих процесів, оскільки являють собою інструменти, які здатні створювати економічну цінність і при цьому знижувати існуючі витрати [2]. Наразі існує велика кількість практик, що свідчать про перші кроки до реалізації ідей циркулярної економіки. Багато компанії вже використовують нові технології для виключення відходів та забруднення з ланцюжків створення вартості, надаючи при цьому позитивний екологічний та соціальний вплив [3]. Але ж нові технології та бізнес-моделі, а також високі темпи їх впровадження несуть нові ризики, проте кібербезпека робить швидкі цифрові зміни безпечнішими. З розвитком цифровізації і комп'ютеризації як у виробничих процесах так і повсякденному житті масштаби кіберзагроз зростатимуть пропорційно збільшенню набору циркулярних продуктів і послуг, у яких застосовуються інформаційні технології, та кількості їх споживачів. З урахуванням цього гарантування кібербезпеки є актуальним завданням для публічного та приватного секторів, а розробка адекватних заходів протидії подібним викликам і загрозам стають важливим вектором публічної політики.

Якщо підприємці, що ставлять за мету перехід на циркулярні рейки розвитку та використовують при цьому цифрові технології не роблять активних кроків із захисту цифрових активів бізнесу, вони безперечно ризикують. Як стверджують експерти приблизно 43% усіх кібератак, зосереджені на малому бізнесі - частково тому, що вони досить великі, щоб бути цінними, але також досить малі, щоб бути вразливими [3].

Існує безліч інструментів, які можуть захистити від переважної більшості потенційних кібер атак (рис. 2.).

Рис. 2. Інструменти кібер безпеки в економіці замкнутого циклу
Джерело: складено автором

В результаті можемо зробити висновок, що перехід до економіки замкнутого циклу може сприяти покращенню соціально-екологічної ситуації в світі, оскільки ця концепція спрямована на більш раціональне використання обмежених природних ресурсів нашої планети. Однак такий перехід вимагає зміни природного процесу виробництва. Динамічнішому впровадженню запропонованих ідей можуть сприяти цифрові технології. Розвиток яких, у свою чергу, неможливий без посилення кібербезпеки, як на загально національному та регіональному рівні, так і на рівні окремих суб'єктів господарювання. Сприйняття публічним та приватним секторами того факту, що кібер загрози та їх наслідки є дуже важливими є вкрай необхідним для формування відповідного цифрового простору, який стане основою подальших циркулярних змін в нашій країні. Існує тісний зв'язок між рівнями кібербезпеки та цифрового розвитку: підвищення першої неминуче веде до прискорення другого і, як наслідок, досягнення сталого розвитку. Тому кібербезпека повинна посісти чільне місце у загальній візії розвитку нашої країни та окремо взятих компаній.

Список використаних джерел:

1. Горбаченко С.А., Клєвцєвич Н.А. Можливості економічного розвитку на засадах циркулярності в умовах цифрової трансформації. Держава та регіони. Серія: Економіка та підприємництво. 2023. № 1 (128). С.35-41
2. Moşteanu N.R., Faccia A., Cavaliere L.P.L. Digitalization and Green Economy – changes of business perspectives. ICCBDC '20: Proceedings of the 4th International Conference on Cloud and Big Data Computing. August 2020. P. 108 –112. (дата звернення: 10.10.2023).
3. Green and digital transition: More resilience and sustainable jobs for the EU. 2022.

Ключові слова: економіка замкнутого циклу, кругова економіка, циркулярна економіка, інформаційні технології, напрямки кібербезпеки, інструменти кібербезпеки.
Keywords: closed cycle economy, circular economy, circular economy, information technologies, directions of cyber security, cyber security tools.

ВИКОРИСТАННЯ КОМПЛЕКСНИХ ЧИСЕЛ У РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Гурін Євген

студент 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Вища математика активно використовується у розробці програмного забезпечення у сьогоденні, ба більше: велика частина індустрії IT ґрунтується саме на вищій математиці. Доволі важливою частиною вважаються комплексні числа, які дуже активно використовують у:

- Комп'ютерній графіці
- Штучному інтелекті
- Квантових обчисленнях
- Gamedev-і

Комп'ютерна графіка та розробка ігор. Комплексні числа використовують при геометричній інтерпретації руху або дій на площинах: рух по колу, рух по кривій тощо. Розглянемо функцію f(t)=it: така математична конструкція широко використовується при зображенні циклічного руху по колу, де уявна одиниця «i» виступає як об'єкт, а «t» інтерпретується як деякий момент часу, де, за допомогою вектора, що пролягає з початку координат до одиниці, ми показуємо циклічний рух по колу, який може бути заданий у будь-якому числі повторювань за допомогою t. Щоб зробити запис більш класичним та зрозумілим для математичного погляду, функцію можна зобразити у вигляді (-1)t/2 , що буде тотожно it. Так само можна представити й інші рухи по кривій: еліпсоїдний, косинусоїдний, синусоїдний, або ж інші криві. Варто зазначити, що для деяких варіантів переміщення не бажано використовувати декілька варіантів задання функцій, це може викликати ускладнення у майбутніх обчисленнях (одна з причин: у таких функцій будуть різні похідні та первісні) [1].

Комплексні числа у розробці, аналізі, та підтримці штучного інтелекту. Одна з основних функцій комплексних чисел у галузі нейромереж, після обчислень, - кодування та шифрування інформації алгоритмів штучного інтелекту від зламу, які могли б зняти обмеження у наданні інформації, що спричинило б надання доступу до створення шкідливого ПЗ: вірусів, фішинг- та хак-програм. Або ж інше: за допомогою включення декількох комплексних

значень, які б посприяли поліпшенню візуалізації, можна навчити штучний інтелект розпізнавати графічні об'єкти (наприклад – капчі), що дуже економить час, порівняно з сотнями, якщо не тисячами, ітерацій, які б знадобилися для машинного навчання ШІ.

Комплексні числа можуть бути використані у модифікації системи пошуку ШІ, наприклад, технологією градієнтної регулярізації, принцип якої ґрунтується на зменшенні діапазону пошуку для алгоритму, що також оптимізує час пошуку відповіді. Але до чого тут комплексні числа? Функції комплексних чисел дуже допомагають у аналізі та описі синусоїдальних хвиль, за принципом яких штучний інтелект і шукає інформацію. Метод пошуку відповіді у алгоритму ШІ виглядає як нитка, яка поступово вирівнюється: кожен період синусоїдальної функції означає варіант відповіді, які з плином часу аналізу вирівнюються до однієї лінії, що б відповідала на запит користувача, та співпадала б з усіма варіантами відповіді ШІ [2].

Квантові нейромережі. Такі нейромережі є синтезом штучних нейромереж з деякими перевагами квантової інформації, у яких одиницею інформації виступають кубіти – аналог одиниці інформації для квантового числення. Такий аналог містить у своєму чистому [3] заданні вираз з комплексними числами, які також використовують і у операціях над цими кубітами. Перевага цього виду нейомереж полягає у нечіткій логіці, яка, як би це не було парадоксально, видає більш направлені та змістовні відповіді на запити. Процес навчання такого штучного інтелекту пов'язують з циклічними алгоритмами, які використовують класичні нейромережі, але модернізовані, що містять у собі принципи вище написаного синусоїдального алгоритму, з комплексними моделями, які виступають допоміжним чинником до традиційного процесу, але вже з мінімальними обчислювальними витратами [4].

Кватерніони у геймдеві. Кватерніонами є чотиривимірні гіперкомплексні числа, які використовують у квантовій фізиці та описі теорії відносності, але до чого тут ІТ? Кватерніони надзвичайно часто присутні у геймдеві: деталізація 3D графіки, реалізм фізики, векторний рух об'єктів. При розробці ігор на Unity програмісти майже завжди зустрічаються з цими числами, хоча і самі не знають про це, наприклад використовуючи скрипт Physics.BoxCast, який використовують для збільшення реалізму в 3D іграх за рахунок змінної типу bool (true-false); один із параметрів функції цього скрипту є кватерніоном, який дозволяє змінювати його кінцевий оберт. Також однією з найголовніших функцій кватерніонів у цій галузі є оберти матриць об'єктів (наприклад: у низькорівневих класах для малювання, також відоме як GL); щоб відобразити їх оберт нам обов'язково треба використати скрипт, який містить у собі кватерніони. На прикладі коду:

Matrix4x4 rotationMatrix = Matrix4x4.TRS(transform.position, transform.rotation, transform.lossyScale); Gizmos.matrix = rotationMatrix;

Крім обертання матриць, функцію з кватерніонами використовують у заданні повороту на декілька градусів для 3D об'єкту у просторі, приклад у повороті об'єкту з осі X до осі Y:

*object.rotation = Quaternion.AngleAxis(myAngle, Vector3.right) * object.rotation*

(на прикладі мови C#). Такий принцип також використовують і у віртуальній реальності [5].

Список використаних джерел

1. Показникова форма комплексного числа: https://studfile.net/preview/5454001/page:5/
2. Комплексні числа у штучному інтелекті: https://pratt.duke.edu/news/imaginary-numbers-machine-learning/
3. Кубіти:https://uk.wikipedia.org/wiki/%D0%9A%D1%83%D0%B1%D1%96%D1%82
4. Квантові нейронні мережі: https://uk.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0_%D0%BD%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0
5. Кватерніони у геймедві https://gamedev.dou.ua/articles/mathematics-gamedev-quaternion/

Ключові слова: комплексні числа, штучний інтелект, gamedev, кватерніони.
Keywords: complex number, artificial intelligence, gamedev, quaternions.

Наукові керівники: старший викладач Баландіна Н.М., к. ф.-м. н., доцент Черевко Є.В.

ОСОБЛИВОСТІ ПРОСУВАННЯ БРЕНДІВ В КІБЕРСЕРЕДОВИЩІ

Рева Аніта

студентка 2-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасному цифровому світі, де велика частина бізнес-взаємодій відбувається в Інтернеті, важливість просування брендів в кіберсередовищі стає критичною для успіху компаній. Кіберпростір пропонує унікальні особливості та можливості для просування, відмінні від традиційних маркетингових каналів.

Тепер одним з актуальних способів стає використання цифрового маркетингу для того, щоб донести образ бренду до споживачів.

Цифровий маркетинг - це термін, що визначає досягнення цілей і завдань бізнесу з використанням онлайн-каналів, що включають, але не обмежуються пошуковими системами, платформами соціальних мереж, створенням контенту та рекламою з метою навчання, залучення та просування продукту або послуги на ринок потенційним покупцям [1].

Якщо розглядати маркетинг, то це процес управління, який відповідає за виявлення, прогнозування та задоволення вимог клієнтів. Тобто це визначення підкреслює орієнтацію на клієнта, маючи на увазі необхідність зв'язку з іншими бізнес-операціями для досягнення задоволеності споживача.

Однак, це слабке визначення стосовно цифрової діяльності, оскільки воно не підкреслює комунікацію, яка так важлива. У процесі проведення цифрового маркетингу бренд може використовувати веб-сайти, пошукові системи, блоги, соціальні мережі, відео, електронну пошту та аналогічні канали для залучення клієнтів.

Цифровий маркетинг можна використовуватиме досягнення цих цілей такими способами [2]:

- Ідентифікація – інтернет можна використовувати для дослідження ринку, щоб з'ясувати потреби та бажання клієнтів.
- Прогнозування – інтернет надає додатковий канал, через який клієнти можуть отримати доступ до інформації та здійснювати покупки. Оцінка цього попиту є ключем до управління розподілом ресурсів.
- Задоволеність – ключовим фактором успіху є досягнення задоволеності клієнтів через відповідний канал, що порушує такі питання, як: чи легко використовувати сайт, чи адекватно він працює, які стандарти належного обслуговування клієнтів та як доставляються фізичні продукти?

Однією з найбільш значущих переваг просування бренду в кіберпросторі є можливість охоплення глобальної аудиторії. На відміну від традиційних методів реклами, які часто обмежені географічними рамками, Інтернет допомагає компаніям просувати свій бренд серед людей по всьому світу. Таке глобальне охоплення дає змогу компаніям розширювати клієнтську базу та освоювати нові ринки, незалежно від їхнього фізичного місцезнаходження.

Якщо розглядати, то як компанії залучали своїх цільових споживачів 15 років тому, то вони використовували традиційні засоби маркетингу: телебачення, радіо та печать. Просто тому, що саме там потенційні клієнти проводили найбільше свого вільного часу. Однак із людством розвивалися і технології, що призвело до цифрової революції. Простіше кажучи, люди стали проводити більше часу на онлайн-платформах, соціальних мережах і в додатках, наприклад таких як Google, Facebook, Instagram, YouTube тощо. У них користувачі отримують безліч постійного потоку інформації, використовують як

розвагу і можливість проводити комерційну діяльність. Таким чином, сьогодні наше життя протікає на відстані одного кліка.

Це допомагає інтерактивно взаємодіяти зі споживачами та розповідати про бренд. За допомогою соціальних мереж, форумів, блогів та інших платформ компанії можуть налагодити діалог із цільовою аудиторією. Така двостороння комунікація сприяє підвищенню лояльності до бренду, оскільки клієнти відчувають, що їх чують і цінують. Компанії можуть отримувати цінні відгуки та інформацію, що дає змогу покращувати стратегії просування бренду та асортимент продукції. Те, яким чином компанії взаємодіють зі своїми клієнтами, розглянуто в таблиці 1.

Таблиця 1 – Аналіз брендів в кіберсередовищі

Компанія	**Взаємодія з клієнтами**	**Загальна сума фінансування**	**Кількість користувачів**	**Бізнес-модель**
Netflix	Онлайн-платформа для потокового відтворення відео, активно просуває свої послуги через інтернет і соціальні мережі.	$5 млрд	Понад 200 мільйонів підписників у більш ніж 190 країнах.	Місячні підписки, що надають користувачам необмежений доступ до контенту без реклами.
Uber	Надання послуги таксі та каршерінгу через мобільний застосунок, покладається на кіберпростір для взаємодії з клієнтами та управління своїм бізнесом.	$25,2 млрд	Активних облікових записів не рідше ніж раз на місяць до 118 млн.	Отримання комісії з кожної поїздки, а також надання додаткових послуг, таких як доставка їжі через Uber Eats.
Google	Ключовий учасник у кіберпросторі, надає пошукові запити, рекламні послуги (Google Ads), електронну пошту (Gmail), відеохостинг (YouTube), карти та інші онлайн-сервіси.	$26,1 млн	Близько 3,3 мільярда людей користуються цим сервісом.	Google AdWords і Google AdSense надають інструменти для рекламодавців і видавців відповідно. Компанія також надає хмарні послуги через Google Cloud Platform, зокрема сховище даних і обчислювальні ресурси.
Amazon	Найбільша онлайн-торгова платформа, що діє в кіберпросторі, забезпечуючи покупцям доступ до мільйонів товарів і послуг через свій веб-сайт.	$8,1 млрд	Кількість користувачів сервісу Amazon Prime понад 100 млн.	Компанія активно розвиває хмарні послуги через Amazon Web Services (AWS). Amazon також володіє різними сервісами потокового відео, такими як Amazon Prime Video, і бере участь у виробництві оригінального контенту.

LinkedIn	Надає платформу для створення професійного профілю, включно з досвідом роботи, освітою та навичками.	$154,8 млн.	Понад 740 млн. активних користувачів на місяць.	Продаж послуг рекрутингу (LinkedIn Recruiter), рекламу і платні підписки (Premium).

Джерело: складено за даними [3]

Крім того, для компанії будь-якого масштабу, підприємства з обмеженими ресурсами або ж стартапів просування бренду в кіберсередовищі, буде економічно ефективним. Компанії можуть охопити ширшу аудиторію за менших витрат, що робить цей спосіб привабливим.

Ще одним важливим аспектом для просування в кіберсередовищі є цифровий брендинг. Цифровий брендинг - це метод управління брендом, що використовує поєднання інтернет-брендингу та цифрового маркетингу для розвитку бренду на різних цифрових майданчиках, включно з відносинами в Інтернеті, додатками на пристроях або медіа-контентом [4]. Він охоплює створення чіткої та впізнаваної ідентичності для продукції або послуг. Сильний бренд не лише вирізняє компанію з-поміж конкурентів, а й викликає відгук у клієнтів, довіру, лояльність і позитивні асоціації. Що більше користувачів побачать бренд, то ймовірніше вони його запам'ятають і розглядатимуть як потенційного постачальника продуктів або послуг [5].

Не варто забувати про те, що велика кількість даних, що зберігається в Інтернеті, і вони доступні компаніям, які можуть використовувати для цільового маркетингу. За допомогою різних цифрових рекламних інструментів компанії визначають конкретні демографічні характеристики, інтереси та моделі поведінки. Це дає змогу створювати персоналізовані маркетингові повідомлення та доставляти їх потрібним людям у потрібний час. Цільовий маркетинг - це вид маркетингової діяльності, спрямований на просування певних товарних груп із урахуванням особливостей цільової аудиторії. Простіше кажучи, цільовий маркетинг охоплює не весь ринок разом, а рухається від узагальненого до окремого у своїх стратегіях [6]. У кіберпросторі підвищує ефективність просування бренду, гарантуючи, що повідомлення знайде відгук у цільової аудиторії.

З огляду на все вищесказане, можна зробити висновок, що просування бренду в кіберсередовищі пропонує численні переваги і можливості для компаній, що розвиваються, і стартапів, які починають свою діяльність. Інтернет стає тим самим прогресуючим інструментом, який забезпечує глобальне охоплення, даючи змогу компаніям розширювати свою клієнтську базу і виходити на нові ринки. Враховуючи те, що сучасна людина бажає здійснювати дії через "один клік", то брендам слід адаптувати свої платформи для цього. За допомогою стратегій цифрового маркетингу та брендингу компанії можуть

взаємодіяти зі своєю цільовою аудиторією, формувати лояльність до бренду та отримувати цінний зворотний зв'язок.

Список використаних джерел:

1. Посібник з цифрового маркетингу для початківців. URL: https://www.webmarketingacademy.in/wp-content/uploads/2018/10/A-Beginners-Guide-to-Digital-Marketing.pdf (дата звернення: 10.11.2023)
2. Чеффі Д. Досконалість цифрового маркетингу: планування, оптимізація та інтеграція онлайн-маркетингу. PR Smith, 2017. (дата звернення: 10.11.2023)
3. Холодна Ю.Є. Світові практики розвитку брендів в сучасних умовах. Економіка та суспільство. Харківський національний економічний університет імені Семена Кузнеця. Випуск # 54 / 2023. (дата звернення: 10.11.2023)
4. Що таке цифровий бренд? URL: https://thebrandsmen.com/what-is-digital-branding/ (дата звернення: 10.11.2023)
5. Технології СММ. URL: https://lemon.school/blog/tehnologiyi-smm (дата звернення: 10.11.2023)
6. Сегментація і персоналізація: чому цільовий маркетинг став ефективнішим за масовий. URL: https://datawiz.io/uk/blog/segmentation-and-personalisation-why-target-marketing-has-become-more-effective-than-mass-one (дата звернення: 10.11.2023)

Ключові слова: бренд, кіберсередовище, брендинг, соціальна мережа, маркетинг.
Keywords: brand, cyber environment, branding, social media, marketing.

КІБЕРРИЗИКИ ФУНКЦІОНУВАННЯ ЕЛЕКТРОМОБІЛЬНОЇ ІНФРАСТРУКТУРИ

Разінкін Нікіта

аспірант кафедри економіки Одеського національного економічного університету

Кіберризики, пов'язані з функціонуванням електромобільної інфраструктури, є важливою темою в сучасному світі, де технології постійно розвиваються, а залежність від цифрових систем стає все більшою. Розуміння цих ризиків та розробка стратегій для їх запобігання та мінімізації є ключовими для забезпечення безпеки та стійкості електромобільної інфраструктури.

Один з основних аспектів кіберризиків при експлуатації електромобілів та зарядних станцій - це їхня пряма залежність від цифрових технологій, включаючи інтернет речей (IoT), бездротові комунікації та хмарні обчислення. Вказані обставини створюють потенційні вектори атак для хакерів, які можуть намагатися викрасти дані, здійснити неконтрольоване управління

системами або навіть перешкоджати нормальному функціонуванню інфраструктури.

Основною проблемою є безпека даних. Електромобілі та зарядні станції збирають величезні обсяги даних, включаючи інформацію про місцезнаходження, звички водіння, а також фінансові транзакції під час зарядки. Недостатня захист цих даних може призвести до їх витоку або маніпуляції, що становить загрозу для конфіденційності користувачів та може призвести до фінансових втрат [1].

Забезпечення безперервності роботи також є одним з важливих аспектів. Електромобільна інфраструктура стає все більш важливою для транспортної системи, і будь-які перебої в її роботі можуть мати серйозні наслідки, включаючи зупинку транспорту, проблеми з логістикою та навіть безпеку. Кібератаки, які цілеспрямовано блокують доступ до зарядних станцій або перешкоджають процесу зарядки, можуть мати великий вплив на повсякденне життя людей та бізнес-операції. Основні кіберризики електромобільної інфраструктури проаналізовано в таблиця 1.

Таблиця 1 – Аналіз кіберризиків електромобільної інфраструктури [2]

№	Кіберризик	Опис	Потенційні наслідки	Заходи щодо запобігання/ мінімізації
1	Неавторизований доступ до систем керування	Хакери можуть отримати доступ до систем управління зарядними станціями та іншої важливої інфраструктури	Переривання роботи зарядних станцій, неправильна робота обладнання	Використання фаєрволів, сильних аутентифікаційних механізмів, регулярне оновлення ПЗ
2	Інтерфейси безпровідного з'єднання	Атаки через Wi-Fi/Bluetooth можуть призвести до несанкціонованого доступу або витоку інформації	Крадіжка персональних даних користувачів, несанкціонований контроль над зарядними станціями	Шифрування передачі даних, обмеження доступу до безпровідних мереж
3	Вразливості у ПЗ	Недоліки в програмному забезпеченні можуть бути використані для атак	Несанкціонований доступ, втрата контролю над системами	Регулярне оновлення програмного забезпечення, використання патчів безпеки
4	Заперечення сервісу (DoS/ DDoS атаки)	Перевантаження системи великою кількістю запитів може зупинити її роботу	Неможливість зарядки електромобілів, втрата доступу до послуг	Розподілена архітектура систем, використання спеціалізованих служб захисту від DDoS
5	Витоки даних	Несанкціонований доступ до даних користувачів та іншої конфіденційної інформації	Крадіжка особистих даних, фінансові збитки для користувачів	Шифрування даних, регулярні аудити безпеки, обмеження доступу до даних
6	Фізичний доступ до інфраструктури	Несанкціонований фізичний доступ до критичної інфраструктури	Пошкодження обладнання, несанкціонований доступ до систем	Використання систем безпеки та відеоспостереження, контроль доступу

7	Інтеграція з іншими транспортними системами	Взаємодія з іншими системами може створити нові вразливості	Непередбачені збої у роботі, ризик взаємного впливу систем	Використання стандартів інтеграції, тестування на сумісність
8	Маніпуляції з даними та софтвером	Шкідливе ПЗ або зміни у програмному коді можуть вплинути на роботу систем	Пошкодження обладнання, втрата контролю над системами	Антивірусне програмне забезпечення, контроль цілісності систем
9	Залежність від зовнішніх постачальників послуг	Перебої у роботі зовнішніх сервісів можуть вплинути на доступність послуг	Переривання роботи системи, неможливість зарядки електромобілів	Договори про рівень обслуговування (SLA), вибір надійних постачальників

Джерело: розроблено автором

Крім зазначених ризиків, які впливають на користувачів, існує і певний макро аспект, а саме, загроза втручання в управління транспортними потоками. Електромобілі часто інтегровані в ширші мережі інтелектуального транспорту, які оптимізують рух на дорогах та управління енергоресурсами. Кібератаки, які спотворюють або блокують обмін даними в цих системах, можуть призвести до хаосу на дорогах і навіть до аварій.

Для вирішення цих проблем важливо впроваджувати комплексні заходи безпеки. Це включає розробку сильних протоколів аутентифікації та шифрування, створення надійних систем виявлення та реагування на інциденти, а також регулярне оновлення програмного забезпечення для запобігання вразливостям. Також важливо працювати над підвищенням обізнаності та навчанням співробітників, користувачів та партнерів у сфері кібербезпеки [3].

У світлі постійного розвитку електромобільної інфраструктури, зростаюча складність та взаємозалежність систем вимагає більш витончених підходів до кібербезпеки. Це стосується не тільки технічних рішень, але й стратегічного планування на рівні організацій та державних структур.

По-перше, важливою є реалізація концепції «безпеки за замовчуванням» у розробці продуктів та послуг. Це означає, що системи безпеки мають бути інтегровані на ранніх етапах розробки електромобільної інфраструктури та її компонентів. Зокрема, мова йде про засоби ідентифікації та автентифікації користувачів, шифрування комунікацій, а також про забезпечення фізичного захисту критичних компонентів інфраструктури [4].

По-друге, важливим є створення централізованих систем моніторингу та управління, які дозволяють відстежувати стан інфраструктури в реальному часі та оперативно реагувати на кіберзагрози. Це може включати в себе не тільки виявлення і блокування атак, але й прогнозування потенційних вразливостей, використовуючи методи штучного інтелекту та машинного навчання [5].

По-третє, підвищення обізнаності користувачів є критично важливим. Багато кібератак починаються з елементарних помилок або недбалості користувачів. Профілактичні навчання, роз'яснювальні кампанії та інструктажі можуть значно підвищити рівень загальної безпеки системи [6].

Крім того, співпраця між компаніями, державними органами та науковими установами в галузі обміну інформацією про кіберзагрози та передові практики є ключовою для розвитку ефективних заходів безпеки. Це може включати участь у спільних кібербезпекових ініціативах, створення галузевих стандартів та протоколів, а також співпрацю в області досліджень та розробок.

З огляду на все вищесказане, кіберризики, пов'язані з електромобільною інфраструктурою, вимагають глибокого та багатогранного підходу. Забезпечення безпеки цих систем – це не лише технічне завдання, але й комплексний виклик, який включає розробку нормативної бази, стратегічне планування, розбудову корпоративної культури безпеки та підтримку інновацій. Від ефективності цих заходів залежить не лише безпека даних та інфраструктури, але й довіра до цієї важливої складової сучасної транспортної системи.

Список використаних джерел:

1. Батареї на колесах. Федерація роботодавців автомобільної галузі. URL: https://fra.org.ua/uk/an/publikatsii/analitika/batareyi-na-kolesakh (дата звернення: 05.11.2023)
2. Інформаційна система маркетингових досліджень в сфері автомобільного ринку електромобілів. URL: https://dspace.nuft.edu.ua/jspui/bitstream/123456789/39089/1/122_Banias_Andrii_Vitaliyovich_600_60398.pdf (дата звернення: 05.11.2023)
3. Столбовий В.М., Кисленко Д.П. Заходи з підвищення кібербезпеки на державному та корпоративному рівнях в умовах діджеталізації суспільства. URL: https://nzlubp.org.ua/index.php/journal/article/download/802/729 (дата звернення: 05.11.2023)
4. Які перспективи електромобілізації в Україні? Інформаційно-аналітична група. URL: https://autoconsulting.ua/article.php?sid=53998 (дата звернення: 05.11.2023)
5.Кисільова К. Ю. Програмна система моніторингу і контролю енергозабезпечення електромобіля : автореф. дип. роботи на здобуття освітнього ступеня «магістр»: спец. 124 «Системний аналіз» / К. Ю. Кисільова , ЧНУ ім. Петра Могили. - Миколаїв, 2019. - 13 с. (дата звернення: 05.11.2023)
6.Безпека електромобілів: що потрібно знати щоб спокійно спати. URL: https://oncharger.com.ua/ua/a462928-bezopasnost-elektromobilej-chto.html (дата звернення: 05.11.2023)

Ключові слова: електромобіль, ризики, інфраструктура, кібербезпека.
Keywords: electric vehicle, risks, infrastructure, cybersecurity.

Науковий керівник: д.е.н., професор Горбаченко С.А.

ПЕРСПЕКТИВИ РОЗВИТКУ СЕГМЕНТУ ГЕЙМДЕВ В УКРАЇНІ

Скідан Владислав

аспірант кафедри менеджменту Національного університету «Одеська юридична академія»

Геймдевелопмент (від англійського «game development») або скорочено геймдев - це інтердисциплінарна область діяльності, що вивчає та розвиває процес створення відеоігор, яка поєднує в собі елементи програмування, дизайну, мистецтва, інженерії та інших галузей знань. На практиці геймдев включає в себе весь цикл створення відеоігор, починаючи з ідеї та концепції і закінчуючи релізом та підтримкою готового продукту.

Геймдев постійно розвивається, проходячи через кризи та успішно їх подолаючи. Головна причина цього процесу - повторення існуючих тенденцій. В деякий момент з'являється новий тренд, будь то гра, підхід або жанр, який набуває величезного успіху. Всі ігрові розробники наступають на цей шлях, ретельно досліджуючи його з різних сторін. В результаті вони створюють велику кількість продуктів, які, на жаль, не завжди приносять щось нове, але натомість насичують ринок безліччю миттєвих варіацій. Цей процес постійно повторюється. Прикладами можуть бути популярні квести 2000-х, вибух інтересу до VR-систем, чи сучасна пристрасть до NFT-продуктів. Проблема полягає в тому, що багато людей мають одну мету - заробити гроші, копіюючи успішні проєкти та масово їх клонуючи.

Що стосується України, то період найвищого розвитку припадає на роки 2018-2020. Український геймдев виник з приходом комп'ютерів до країни, і спочатку це були ентузіасти, які віддавали свою енергію створенню ігор. Першою компанією, яка відома у зв'язку з виникненням української геймдев індустрії, є GSC Game World. Ця компанія відома завдяки іграм «Козаки» і «S.T.A.L.K.E.R», хоча на початку свого існування вона досить довго шукала свій шлях.

Однак, якщо говорити точніше, геймдев в Україні виник з команди Меридіан 93, яка була заснована в 1993 році і випустила свій перший ігровий продукт «Admiral: Sea Battles» в 1996 році. У 90-х роках з'явилися перші ознаки зростання геймдеву, хоча більшість компаній того часу займалися не стільки розробкою, скільки локалізацією та адаптацією інеземних ігор для вітчизняного ринку. Часто ці локалізації були піратськими, і творцям ігор не платили роялті [1].

Навіть в умовах війни Україна мала численні передумови для створення ефективного та результативного геймдев співтовариства. Однак, можливо, найцікавішою передумовою був розвинутий рольовий ігровий рух на теренах країни. Чимала кількість осіб з цього руху, які мали бажання творити

неординарні ігри, знайшли себе в геймдеві. Це було пов'язано з їхньою загальною прагненням до новаторства та креативності, що ідеально вписувалось в сучасну парадигму геймдеву. Тому багато з них стали активними учасниками української індустрії відеоігор.

В країні склалися сприятливі умови для західних компаній, які вирішили виробляти ігри саме тут. У нас велика кількість висококваліфікованих фахівців, і українські розробники виробляють високоякісний контент - будь то програмний код, мистецтво або інші аспекти, пов'язані з розробкою ігор.

З цими факторами інвестори з США та Європи почали відкривати свої представництва у нашій країні.

На практиці в Україні виробляється неймовірна кількість всіх світових IT-рішень. Якщо придивитися до всіх топових проєктів, то майже в кожному з них можна знайти спеціалістів з України. На сьогоднішній день у світі спостерігається зростання числа автоматизованих систем, і це призводить до зниження рівня зайнятості серед населення. Це представляє собою важливу глобальну проблему для цивілізації.

Щодо світового ринку геймдева, у 2022 році він досягнув загального обсягу вартості у розмірі 184,4 мільярда доларів, і цільовий сектор мобільних ігор займає вражаючу половину цього ринку.

Структура світового ринку геймдева зображено на рисунку 1.

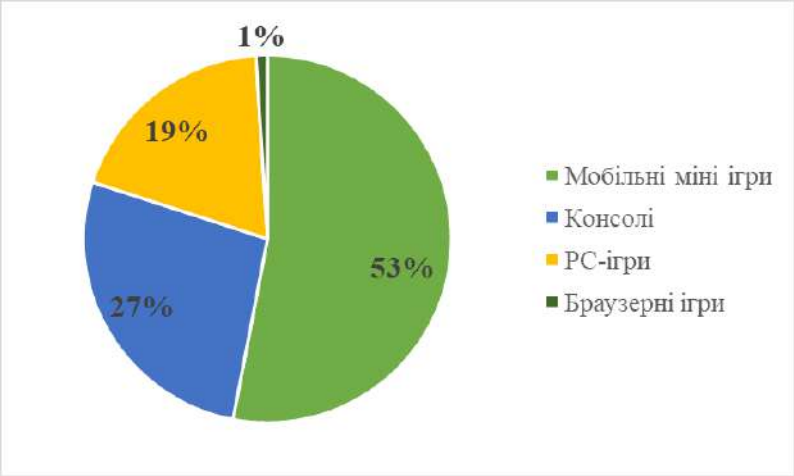


Рис. 1 – Структура світового ринку геймдева [2]

З огляду на найважливіші показники цієї індустрії, ресурс Sensor Tower надав такі дані:

– за найвищими доходами, Сполучені Штати Америки лідирують з великим відривом, досягнувши показника в 20,8 мільярда доларів;

– з точки зору видавців, китайська приватна інвестиційна компанія Tencent посідає перше місце з доходами у розмірі 6,8 мільярда доларів.

На четвертому місці розташувався Playrix з прибутком у розмірі 2 мільярдів;

– у номінації «ігри» лідирує Honor of Kings, яка заробила найбільше доходу, досягнувши показника у 2,5 мільярда доларів;

Щодо завантажень мобільних ігор, ось деякі цікаві факти:

– Індія відзначилася найбільшою кількістю завантажень мобільних ігор, які склали вражаючих 8,9 мільярда;

– відомий видавець Azur Interactive Games зареєстрував понад 1,1 мільярда завантажень своїх ігор;

– Subway Surfers, мобільна гра у жанрі платформера для iOS і Android, підкорила серця гравців і була завантажена понад 275 мільйонів разів [3].

У майбутньому люди будуть мати все більше вільного часу завдяки технологічному прогресу, і вони все більше будуть шукати способи розваги. Медіарозваги стануть невід'ємною частиною їх відпочинку, і в цьому контексті ігри відіграють важливу роль, надаючи можливість не лише забавлятися, але й спілкуватися та відчувати радість.

Ринок геймдеву завжди буде розвиватися, оскільки постійно виникають нові геймінгові пристрої, що пропонують гравцям новий і захоплюючий досвід. Це було виявлено при запуску Nintendo Switch і подібних інноваційних продуктів.

З цього можна зробити висновок, що індустрія відеоігор залишається високо популярною і прибутковою. Це означає, що все більше людей буде зацікавлено в кар'єрі в галузі геймдеву, що стає ще одним трендом. Проте важливо відзначити, що зростання попиту на роботу в геймдеві не рівномірне. В історії розвитку цієї галузі спостерігалася зміна від генералістів до спеціалістів. Розробники стали спеціалізованими у певних областях, і тепер кожна людина працює над конкретним аспектом гри. З'явилися навіть дуже специфічні напрями, такі як 3C (Character Camera Control), де фахівець відповідає за оптимальний ракурс камери в грі, щоб зробити гру більш кінематографічною та захоплюючою [4].

Однак велика кількість таких спеціалізацій ще досить нова і не має загальних стандартів чи шаблонів. Кожна компанія розробляє ігри за власними уявленнями про те, що є найкращим. Хоча зараз світові інститути починають розробляти системи та математичні підходи до геймдеву, намагаючись встановити математичні закономірності та наукові визначення в цій сфері. Це допоможе краще розуміти процеси, які відбуваються в іграх у майбутньому.йти наших фахівців.

Станом на квітень 2023 року, геймдев індустрія в Україні продемонструвала динамічний розвиток, незважаючи на значні виклики, зокрема че-

рез військову агресію росії та світові економічні турбулентності. З точки зору формування пропозиції у індустрії геймдев в Україні переважають малі та середні студії, що розробляють інноваційні ігри. Також, в Україні існує велика кількість технічних університетів та курсів, які сприяють підготовці кваліфікованих спеціалістів у галузі. Однак, індустрія стикається з викликами, пов'язаними з воєнним конфліктом, що впливає на роботу студій, переміщення талантів та інвестиції. Також, глобальні економічні коливання та внутрішня нестабільність впливають на фінансові потоки та інвестиційні можливості [5].

Щодо перспектив розвитку, то вони включають глобалізацію та партнерства з міжнародними компаніями, цифрову диверсифікацію з орієнтацією на розробку ігор для різних платформ і використання новітніх технологій, як VR/AR. Прямі інвестиції та урядова підтримка, особливо в плані податкових пільг та грантів для стартапів, також мають велике значення. Тісна співпраця з освітніми установами для підготовки кадрів та акцент на створенні унікального контенту з особливим фокусом на локалізацію та культурні особливості можуть допомогти українським іграм виділитися на світовому ринку.

Таким чином, український геймдев має значний потенціал для зростання та розвитку, а ключем до успіху є адаптація до змінюваних умов, використання сильних сторін місцевих розробників, інвестиції у технологічний розвиток та активне входження в глобальні ринки.

Список використаних джерел:

1. Мартиненко Є. Зародження геймдеву в Україні і перспективи його розвитку. URL: https://gamedev.dou.ua/blogs/the-origin-of-gamedev-in-ukraine/ (дата звернення: 06.11.2023)
2. Мобільні міні ігри займають 53% світового ринку геймдеву - аналітики URL: https://kg.ua/news/mobilni-mini-igri-zaymayut-53-svitovogo-rinku-geymdevu-analitiki (дата звернення: 06.11.2023)
3. Горбік В. Світовий ринок ігор у 2022 став дорожче усіх активів Ілона Маска. Підсумки року за версією Games Industry. URL: https://dev.ua/news/naipopuliarnishi-ihry (дата звернення: 06.11.2023)
4. Шевлюга А.Г. Розроблення програми виведення нової гри компанії Enixan на ринок мобільних ігор України. URL: https://ela.kpi.ua/bitstream/123456789/43806/1/Shevliuga_bakalavr.pdf (дата звернення: 06.11.2023)
5. Економічні проблеми сталого розвитку. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/78992/1/Zaitsev_electronic_games.pdf (дата звернення: 06.11.2023)

Ключові слова: геймдев, мобільні ігри, відеоігри, перспективи.
Keywords: game dev, mobile games, video games, prospects.

Науковий керівник: д.е.н., професор Горбаченко С.А.

СУЧАСНІ ТРЕНДИ ІНТЕРНЕТ-МАРКЕТИНГУ

Науменко Аліна

студентка 2-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У нинішньому динамічному світі поняття "інтернет-маркетинг" отримало різноманітні інтерпретації. Ця багатогранність та широке використання у діяльності компаній та індивідуальних підприємців пояснюється великою кількістю його визначень.

Станом на січень 2023 рік, за даними Statista, 5,16 мільярда людей були активними користувачами Інтернету, з яких 5,44 мільярда використовували мобільний інтернет, а 4,76 мільярда активно користувалися соціальними мережами. Інтернет надає можливість спілкуватися з людьми по всьому світу, ділитися фотографіями, створювати розважальний контент, ш укати однодумців.

Витрати на рекламу в соціальних мережах зазнали значного зростання, майже подвоївшись з часу початку пандемії Covid-19. Як було вказано раніше, кількість користувачів соцмереж продовжує зростати. З моменту виникнення пандемії, популярні соціальні платформи відзначили збільшення аудиторії на 30%, що становить приблизно 1 мільярд нових користувачів за останні три роки.

Однак слід відмітити, що в 2023 році темпи приросту аудиторії сповільнились. Передбачається, що ця тенденція продовжиться і в 2024 році.

На сьогоднішній день звичайний інтернет-користувач витрачає в соціальних мережах приблизно 2,5 години на день, що є найвищим показником за всю історію. Таким чином, реклама в соцмережах є надзвичайно важливою і, безсумнівно, збереже свою актуальність у 2023 році. У середньому, користувачі проводять 4 з кожних 10 хвилин онлайн саме на соціальних платформах, таких як Instagram, Facebook, Twitter, LinkedIn, YouTube, TikTok, Telegram, WhatsApp [1].

Більш детальна інформація щодо користувачів соціальних мереж зображена на рисунку 1.

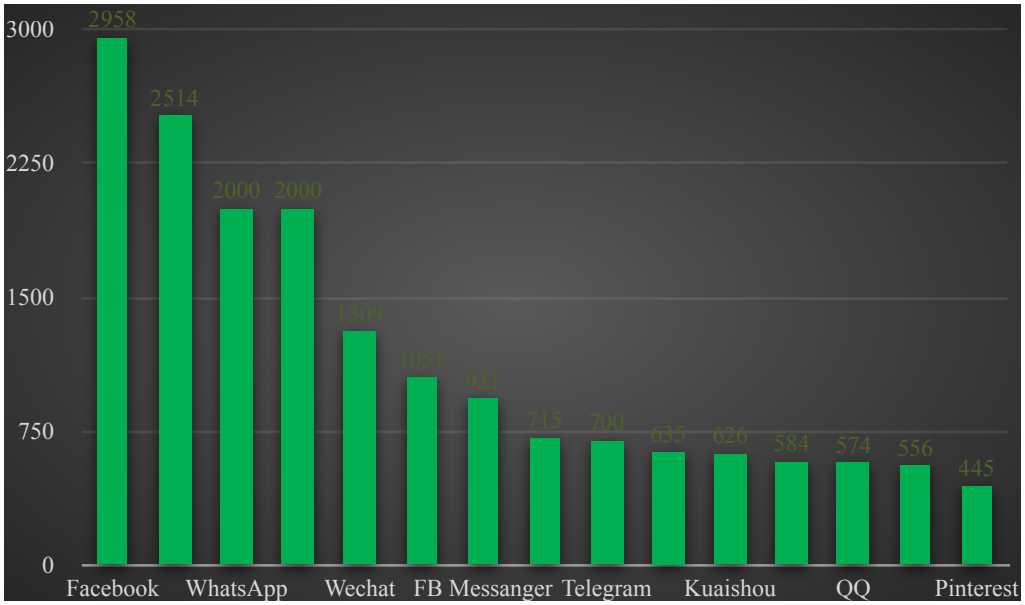


Рис. 1 – Світові показники користування соціальними мережами на 2023 рік [1]

Instagram, відома платформа для обміну фото та відео, була створена Кевіном Сістромом і Майком Кригером, і зараз належить компанії Meta Platforms з США. Інстаграм перетворився на місце, де можна розвивати особистий бренд, рекламувати магазини, ресторани та розважальні заклади, а також політики та бізнесмени використовують його для залучення нової аудиторії. Ця платформа також відкрила нові професії та способи заробітку, такі як блогер, менеджер соціальних медіа, спеціаліст з реклами, фахівець з відеомонтажу, та багато інших.

У 2022 році, одним з головних трендів Instagram є Reels - короткі відеоролики до 60 секунд. Вони мають вертикальний формат та залишаються в профілі користувача, на відміну від сторіс, які зникають через 24 години. Reels здатні швидко привернути увагу аудиторії. В Україні, формат Reels відрізняється від того, що доступний у Європі та США, оскільки в Україні немає окремого розділу для Reels, тому їх можна знайти лише у стрічці або в рекомендаціях [2].

Оглядаючи наступну соціальну платформу, варто зупинитись на TikTok – пекінському сервісі ByteDance, що дозволяє створювати та переглядати короткі відеоролики і обмінюватися ними. TikTok нині користується великою популярністю серед молоді, але його також активно використовують блогери, шоу-бізнес зірки та інші впливові особи для залучення нових підписників і клієнтів. Ця платформа стала ключовим інструментом у вірусному маркетингу для популяризації власних брендів, продуктів та послуг.

TikTok швидко розвивається, і тренди там змінюються стрімко. Тому важливо слідкувати за останніми відеороликами, щоб зрозуміти, що зараз

цікавить аудиторію. Основним напрямом у соцмережах є тісна і підтримуюча взаємодія бізнесів з клієнтами [3].

В області Інтернет-маркетингу, крім соціальних мереж, стає все популярнішим email-маркетинг. Це метод промоції продуктів або послуг через email-розсилки, який залучає та утримує клієнтів, підвищуючи їх вірність бренду.

Розглянемо ключові тренди описані в таблиці 1.

Таблиця 1 – Ключові тренди інтернет-маркетингу [4]

№	Тренд	Опис
1.	Персоналізація листів	Загальні листи без персонального звернення втрачають свою актуальність. Використання імені, прізвища, віку, статі, країни проживання, інтересів користувача дозволяє створити більш персоналізовані пропозиції, підвищуючи таким чином конверсію, коефіцієнт клікабельності та чистий прибуток від кампанії.
2.	Застосування штучного інтелекту	Штучний інтелект аналізує поведінку користувачів, їх часовий пояс, налаштування електронної пошти та історію покупок, покращуючи таким чином взаємодію між брендом та аудиторією.
3.	Автоматизація email-маркетингу	Багато маркетингових процесів, таких як відправлення тригерних та транзакційних листів, вимагають автоматизації, що підсилює їх ефективність.
4.	Використання AMP та гейміфікації	Інтерактивні AMP-листи з анімацією, формами зворотного зв'язку, галереями зображень та гейміфікацією збільшують залученість користувачів. Гейміфікація, яка може вимагати додаткових часових та фінансових витрат, допомагає розважити клієнтів та налагодити довгострокові відносини.

Під час конфлікту виникла нова важлива тенденція – звертати увагу на емоції споживачів, виявляти турботу, організовувати опитування та запитувати, чи перебуває абонент у безпечному місці, чи потребує перерви в розсилці наразі. Такий підхід демонструє турботу бренду і, безсумнівно, згодом матиме позитивний вплив на репутацію компанії. Водночас ця тенденція допомагає уникнути образи клієнтів через недоречні повідомлення та зменшує роздратування тих, хто сприймає розсилку як вантаж.

Впровадження чат-ботів – це інший напрямок у сфері інтернет-маркетингу. Наразі люди високо цінують свій час і швидке відповідання на їхні запитання збільшує лояльність, відповідно, сприяючи зростанню продажів. Чат-боти роблять процес отримання відповідей на основні питання простішим, не

потребуючи дзвінка оператору чи довгих переписок, спрощуючи роботу не тільки для клієнтів, але й для менеджерів, які не мусять відповідати на однакові питання кілька разів. Особливо за часів конфлікту, коли час стає ще цінішим.

Ще одним трендом є маркетинг через впливових особистостей (influencer marketing). Ця стратегія базується на тому, що інфлюенсери, блогери, знаменитості передають важливі повідомлення обраній аудиторії. Згідно з дослідженням HypeAuditor, популярність інфлюенсерів у сферах фінансів та бізнесу зросла на 25% у 2022 році порівняно з 2021 роком, за ними слідують телевізійні інфлюенсери зі зростанням активності на 24%. Прогнозується, що сектор influencer-маркетингу в Instagram зросте до 22,2 млрд доларів до 2025 року [5].

Останнім великим трендом є контент-маркетинг, який являє собою комплекс маркетингових методів, що ґрунтуються на створенні та розповсюдженні інформації, корисної для споживача, з метою здобуття довіри та приваблення потенційних клієнтів. Важливо, щоб контент був інформативним, захоплюючим, відповідав сучасним реаліям, включаючи елементи української символіки та відображаючи події війни через колірні гами червоного та чорного (символи крові та смерті) та жовто-блакитні. Пошукові системи, як Google, постійно удосконалюють свої алгоритми, підвищуючи важливість якісного контенту.

Інтернет-маркетингові інструменти забезпечують широке охоплення та залучення аудиторії, одночасно інформуючи значно більше людей. Вони сприяють покращенню взаємодії з покупцями, зміцненню відданості до бренду, зростанню доходів компаній або хоча би збереженню існуючих показників. Такі інструменти допомагають оптимізувати витрачений час та поліпшити зручність спілкування з клієнтами. Зростання та розвиток цієї сфери продовжуватиметься, адаптуючись до воєнних подій, розширюватися та нарощувати оберти, враховуючи нові умови сучасного світу.

Список використаних джерел:

1. We are social 2023: соціальні мережі, інтернет та тенденції електронної комерції. Elit Blog. URL: https://elit-web.ua/ua/blog/we-are-social-2023 (дата звернення: 09.11.2023)
2. Сучасні тренди Instagram: рік 2023. Gromada Group. URL: https://gromada.group/news/statti/24397-suchasni-trendi-instagram-rik-2023 (дата звернення: 09.11.2023)
3. Головні тренди TikTok, які варто спробувати цього тижня. Pro Ідеї. URL: https://www.proidei.com/tiktok-trends-0805/ (дата звернення: 09.11.2023)
4. Тренди в маркетингу 2023 від експертів Бізнес-школи УКУ. Бізнес-школа УКУ (LvBS). Український католицький університет. URL: https://lvbs.com.ua/news/

trendy-u-marketyngu-2023-vid-ekspertiv-biznes-shkoly-uku/ (дата звернення: 09.11.2023)
5. Храпкіна В.В. Сучасні тренди інтернет-маркетингу / Храпкіна Валентина Валентинівна, Брюшко Наталія Олегівна // Економіка та суспільство. - 2022. - Вип. 38. - 7 с. - https://doi.org/10.32782/2524-0072/2022-38-64 (дата звернення: 09.11.2023)

Ключові слова: інтернет-маркетинг, реклама, соціальна мережа, тенденція.
Keywords: internet marketing, advertising, social network, trend.

Науковий керівник: д.е.н., професор Горбаченко С.А.

КІБЕРБЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ ШЛЯХОМ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ

Грезіна Олена

студентка 1-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасному цифровому світі, де освіта все більше стає залежною від технологій, питання кібербезпеки учасників освітнього процесу виходить на передній план. Застосування інтелектуального аналізу даних в цьому контексті визначає новий рівень захисту конфіденційності, доступу до інформації та цілісності освітніх ресурсів. Збільшення кількості цифрових платформ та онлайн-інструментів у навчальному процесі створює нові виклики щодо кібербезпеки. Зростає ймовірність кібератак, спрямованих на отримання особистих даних учасників освітнього процесу.

Дослідженням цього питання займались такі науковці, як Л. Дегтярьова, С. Доценко, Т. Маганова, О. Одрущенко, Т. Павлова, Н. Протас та інші.

Особи з злочинними намірами використовують різноманітні техніки та стратегії для атак на освітній сектор, спрямовані на крадіжку конфіденційної інформації, порушення приватності учасників освітнього процесу, а також перешкоджання нормальному функціонуванню освітніх систем. Збільшення обсягів електронного навчання та використання онлайн-платформ робить учасників освітнього процесу особливо вразливими перед кіберзагрозами.

Мета технологій інтелектуального аналізу полягає у виявленні неочевидних, об'єктивних і практично корисних закономірностей великих обсягів даних.

Застосування інтелектуального аналізу даних в освітньому процесі дозволяє ефективно виявляти та передбачати кіберзагрози. Аналізуючи великі об'єми інформації, такі технології можуть виявити незвичайні патерни та

аномалії, що вказують на можливі атаки або потенційні ризики для кібербезпеки учасників освітнього процесу.

Безпека даних стає особливо важливою в умовах, де технології інтелектуального аналізу використовуються для розвитку освіти. Забезпечення конфіденційності, цілісності та доступності інформації є пріоритетом, і використання інтелектуального аналізу даних може допомогти у виявленні та запобіганні потенційним загрозам кібербезпеки. Таким чином, ці технології стають невід'ємною частиною стратегії захисту інформації та забезпечення безпеки учасників освітнього процесу.

Поєднання кібербезпеки та інтелектуального аналізу даних є важливою складовою сучасної освітньої системи, спрямованою на створення безпечного та надійного середовища для всіх його учасників.

Кібербезпека в освітньому процесі має свої особливості через використання технологій та залучення різних даних. Учасники освітнього процессу повинні бути уважні до кіберзагроз та дотримуватися безпечних практик.

У цьому контексті Доченко С. зазначає, що: «Кібербезпека освітнього закладу передбачає комплекс заходів різного характеру, а саме: 1) захист персональних даних та інформаційного простору від несанкціонованих втручань, розкрадання інформації і зміни конфігурації системи з боку третіх осіб; 2) захист здобувачів освіти від будь-яких видів пропаганди, реклами, забороненої законом інформації тощо» [1, с. 207].

Одарущенко О., Протас Н., Дегтярьова Л. визначають що, «інтелектуальний аналіз даних є коротким позначенням досить широкого спектру процедур автоматичного аналізу даних. Загалом процес інтелектуального аналізу даних складається з трьох стадій: 1. Виявлення закономірностей (вільний пошук); 2. Використання виявлених закономірностей для передбачення невідомих значень (прогностичне моделювання); 3. Аналіз винятків, призначений для виявлення та тлумачення аномалій у знайдених закономірностях» [2, с. 25].

У контексті кібербезпеки це може означати ідентифікацію аномалій в мережевій активності, прогнозування можливих кібератак на основі інтелектуального аналізу та виявлення та вирішення кіберінцидентів у реальному часі. Такий підхід створить умови для автоматизування процесів виявлення та вирішення кіберзагроз, забезпечуючи високий рівень безпеки та ефективність у сфері освіти.

У висновку важливо підкреслити, що застосування інтелектуального аналізу даних у сфері кібербезпеки учасників освітнього процесу є невід'ємною та важливою частиною сучасного освітнього ландшафту. Важливо відзначити можливість ефективного виявлення, прогнозування та вирішення потенційних кіберзагроз, забезпечуючи високий рівень безпеки конфіденцій-

ної інформації учасників освітнього процесу. Інтелектуальний аналіз даних допомагає не лише реагувати на поточні загрози, але й адаптуватися до нових та розвивати стратегії захисту, сприяючи створенню надійного та безпечного освітнього середовища. Зазначений підхід вирішує виклики сучасного цифрового середовища, де кібербезпека стає пріоритетом для забезпечення успішного та безпечного освітнього процесу.

Список використаних джерел:

1. Доценко С.О. Кібербезпека учасників освітнього процесу в умовах дистанційного навчання. Психолого-педагогічні проблеми вищої і середньої освіти в умовах сучасних викликів: теорія і практика : матеріали VII Міжнар. наук.-практ. конф., Харків, 16–18 берез. 2023 р. Харків : ХНПУ ім. Г. С. Сковороди. 2023. С. 207–209. URI: https://dspace.hnpu.edu.ua/handle/123456789/11649
2. Одарущенко О. Б., Протас Н. М., Дегтярьова, Л. М. Аналіз особливостей систем інтелектуального аналізу даних. International scientific conference Publishing House «Baltija Publishing». 2021. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/download/186/5536/11613-1?inline=1

Ключові слова: кібербезпека, учасники освітнього процесу, інтелектуальний аналіз даних, безпека конфіденційної інформації, аномалії в мережевій активності.
Keywords: cyber security, participants of the educational process, intelligent data analysis, security of confidential information, anomalies in network activity

Науковий керівник: к.пед.н, доцент Лобода Ю.Г.

СУТНІСТЬ ТА НЕОБХІДНІСТЬ УПРАВЛІННЯ РИЗИКОМ

Дем'янова Тетяна

студентка 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасному глобальному середовищі, де бізнес, фінансові установи, організації та проекти стикаються з різноманітними небезпеками та невизначеністю, управління ризиками стає важливою стратегічною функцією для досягнення успіху та сталості. Ризик, незалежно від його характеру, може мати як позитивний, так і негативний вплив на діяльність організацій та проекти. Для кращого розуміння управління ризиками розглянемо ключові поняття.

Ризик можна визначити як можливість виникнення подій або ситуацій, які можуть негативно вплинути на досягнення цілей організації. Управління ризиками є систематичним процесом ідентифікації, оцінки, контролю та зменшення ризиків з метою досягнення цілей організації. Цей процес включає в себе кілька етапів:

1. Ризикова ідентифікація - це процес визначення, опису та класифікації можливих ризиків, які можуть впливати на організацію.

2. Оцінка ризиків - це процес визначення ймовірності виникнення ризику та його впливу на організацію, що дозволяє встановити пріоритетність ризиків.

3. Аналіз ризиків - це докладне вивчення ризиків, включаючи їх можливі наслідки та ймовірність виникнення.

4. Стратегія управління ризиками - це набір рішень та заходів, спрямованих на керування ризиками, включаючи рішення про прийняття, зменшення чи уникнення ризику.

5. Моніторинг та контроль ризиків - це процес постійного відстеження ризиків і вжиття заходів для забезпечення їх відповідності стратегії управління ризиками.

6. Страхування ризику - це передача частини ризику страховій компанії в обмін на сплату страхових внесків [1].

Ризики можуть бути різного характеру і впливати на різні аспекти діяльності організацій. На IT-підприємствах існують різні види ризиків:

1. Технічні ризики: пов'язані з технічними аспектами розробки, впровадження та обслуговування інформаційних систем, включаючи можливі системні збої, проблеми з безпекою даних та технічні помилки.

2. Бізнес-ризики: пов'язані з економічними та бізнес-аспектами діяльності IT-підприємства, такі як зміни в попиті на послуги, фінансові ризики та конкуренція на ринку.

3. Ризики забезпечення якості: включають в себе можливі проблеми з якістю розроблених продуктів чи послуг, затримки в виконанні проектів та недоліки в тестуванні.

4. Кадрові ризики: можуть бути пов'язані з втратою ключових спеціалістів, нестабільністю команди та змінами в персоналі.

5. Безпека та кібербезпека: ризики, пов'язані з можливістю кібератак, витоком конфіденційної інформації, порушеннями безпеки даних та іншими аспектами кібербезпеки.

6. Законодавчі ризики: пов'язані з змінами у законодавстві, регулюючому інформаційні технології та захист даних, а також можливими штрафами та судовими справами.

7. Ризики забезпечення: включають в себе можливі проблеми з постачанням необхідного обладнання, програмного забезпечення, послуг та інфраструктури.

8. Ризики змін: пов'язані зі змінами в технологічному середовищі, новими технологіями та апгрейдами. [2]

Сучасні підходи до управління ризиками в IT-підприємствах постійно еволюціонують та вдосконалюються, оскільки ця галузь швидко розвивається та постійно стикається з новими викликами. Ось огляд сучасних підходів до управління ризиками в IT-підприємствах:

1. «Ризик-орієнтований підхід:» Замість реактивного управління ризиками, IT-підприємства все частіше використовують прогностичний підхід, активно ідентифікуючи, аналізуючи та керуючи майбутніми ризиками.

2. «Кібербезпека та захист даних:» Зростання загроз в галузі кібербезпеки призвело до акценту на управлінні кіберризиками, з фокусом на захисті систем, даних та конфіденційності клієнтів.

3. «Дотримання та регуляторні вимоги:» Звершується все більше уваги дотриманню регуляторних вимог, особливо в сферах, що стосуються обробки особистих даних, таких як GDPR, HIPAA і т.д. IT-підприємства забезпечують відповідність з цими вимогами.

4. «Аналіз великих даних і штучний інтелект:» Використання аналізу великих даних і штучного інтелекту допомагає ідентифікувати та передбачати ризики в реальному часі, полегшуючи процеси прийняття рішень і реагування на них.

5. «Управління інноваціями та новими технологіями:» IT-підприємства активно впроваджують нові технології, такі як хмарні обчислення, блокчейн, Інтернет речей і інше, що потребує уважності до ризиків, пов'язаних з інноваціями.

6. «Управління ризиками в постачанні (Supply Chain Risk Management):» З огляду на глобалізацію та складні ланцюги постачання, IT-підприємства акцентують на управлінні ризиками в постачанні, включаючи глобальні кризи та порушення ланцюгів постачання.

7. «Агільний підхід до управління ризиками:» IT-підприємства використовують агільні методології для швидкого реагування на ризики та адаптації до змін в динамічному середовищі.

8. «Соціальна відповідальність та сталий розвиток:» IT-підприємства все більше приділяють увагу ризикам, пов'язаним зі сталим розвитком, і враховують питання соціальної відповідальності.

9. «Доступність управління ризиками як сервіс (RaaS):» Зростає популярність інструментів та платформ для управління ризиками, які надаються як послуга, спрощуючи доступ до засобів управління ризиками.

10. «Управління ризиками в реальному часі (Real-time Risk Management):» З огляду на динамічність IT-систем, управління ризиками переходить до реального часу з постійним моніторингом і миттєвим реагуванням.

11. «Управління ризиками в області штучного інтелекту (AI Risk Management):» Використання штучного інтелекту та машинного навчання для автоматизації ідентифікації та аналізу ризиків для точнішого управління ними.

12. «Внутрішній аудит та незалежність (Internal Audit Independence):» Зростає важливість незалежного внутрішнього аудиту для оцінки ефективності систем управління ризиками та відповідності стандартам

13. «Управління ризиками в поєднанні з кіберзахистом (Cybersecurity Risk Management):» Захист від кіберзагроз стає невід'ємною частиною управління ризиками, особливо для IT-підприємств.

14. «Розвиток стандартів та регуляторних вимог:» Регулятори та стандартні організації розробляють все більше нормативів для управління ризиками в галузі IT.

15. «Ризик-центри (Risk Centers):» Створення спеціалізованих центрів, що відповідають за управління ризиками на рівні організації та забезпечують координацію та комунікацію в цій області[3].

В результаті використання таких сучасних підходів управління ризиками в IT-підприємствах, може призвезти до зменшення ризиків та втрат, покращення реагування на кризи, збільшення довіри клієнтів і інвесторів, оптимізація витрат, забезпечення дотримання регуляторних вимог, стабільність та довгостроковий успіх, підвищення конкурентоспроможності, збільшення внутрішньої ефективності, підвищення інноваційності, підвищення свідомості співробітників, зниження ступеня невизначеності, забезпечення внутрішньої контрольованості покращення репутації, полегшання доступності до фінансування, можливість розвитку нових ринків, підвищення залучення та задоволеності клієнтів.

Список використаних джерел:

1. Вітлінський В. В., Великоіваненко Г. І. Ризикологія в економіці та підприємництві : монографія. Київ :КНЕУ, 2004. 480 с.
2. Посохов І. М. Аналіз досліджень зарубіжних наукових шкіл ризик-менеджменту. Маркетинг і менеджмент інновацій. 2013. № 4. С. 164–172.
3. Вербіцька І. І. Ризик-менеджмент як сучасна система управління ризиками підприємницьких структур. Сталий розвиток економіки. 2013. № 5. С. 282–291.

Ключові слова: управління, ризики, кібербезпека
Keywords: governance, risks, cybersecurity

Науковий керівник: к.ф.-м.н., доцент Чепурна О.Є.

ВПЛИВ ІНФОРМАЦІЙНИХ ВІЙН НА СОЦІАЛЬНУ ПСИХОЛОГІЮ СУЧАСНИХ СУСПІЛЬСТВ

Чепурна Олена

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат фізико-математичних наук, доцент

Козловський Ігор

студент 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Поняття інформаційної війни можна розглядати на основі трьох різних підходів. 1. Інформаційна війна – це сукупність політичних, економічних, соціальних, дипломатичних та технічних методів, способів і засобів, які передбачають вигідний вплив на інформаційну сферу об'єкта зацікавленості та захисту власної в інтересах досягнення поставленої цілі. 2. Інформаційна війна – це найгостріша форма протистояння в інформаційному просторі, обов'язковою умовою якої є протистояння різних за спрямованістю агресивних сторін. 3. Інформаційна війна трактується як форма ведення військових дій за допомогою інформаційних електронних засобів[1].

Сучасна інформаційна війна впливає не тільки на політичний ландшафт країн, але й на соціальну свідомість і психологію громадян.

Зазначимо основні методи та техніки інформаційного впливу на населення:

1.Пропаганда: форма комунікації, спрямована на поширення в суспільстві: світогляду, теорії, твердження, фактів, аргументів, чуток та інших відомостей для впливу на суспільну думку на користь певної спільної справи чи громадської позиції. Разом із цим найзагальнішими методами пропаганди є спрощення (засіб перетворення складних проблем на прості), замовчування (приховування небажаної інформації) і витіснення (інструмент відволікання уваги від негативних поточних подій)[2].

2.Дезінформація: поширення неправдивої інформації для введення в оману опонентів або населення. Включає створення фейкових новин, фотошоплені зображення, вирізані з контексту відео та інші маніпулятивні техніки. Поширення фейкових новин має серйозні психологічні наслідки. Воно може викликати конфузію, невпевненість у визначенні достовірності інформації та загальну недовіру до медіа та інституцій.

3.Кібератаки: використання кіберпростору для атак на інформаційні системи, з метою отримати контроль над ними або знищити інформацію. Це також може включати викрадення даних або блокування доступу до критично важливих сервісів.

4.Контроль над медіа: регулювання або цензурування засобів масової інформації з метою контролю над інформацією, що поширюється в суспільстві.

Кожна з цих технік може використовуватися самостійно або в комбінації з іншими для досягнення стратегічних цілей інформаційної війни. Розуміння та аналіз цих методів є ключовими для розробки ефективних засобів захисту в сучасному інформаційному просторі.

З метою маніпулювання громадською свідомістю використовуються різні стратегії. Зазначимо основні з них: повторення, де одне й те ж повідомлення висвітлюється знову і знову в різних джерелах, що сприяє його запам'ятовуванню та прийняттю як істини; емоційне залучення, де повідомлення викликають сильні емоції, змушуючи людей діяти під впливом почуттів, а не раціонального аналізу; створення штучної драми, використання конспірологічних теорій, а також "gaslighting", при якому особа або група сумнівається у власному сприйнятті реальності через систематичне заперечення фактів.

Отже, перенасичення інформацією провокує у суспільства інформаційний стрес та інформаційну втому, що може привести до відчуття перевантаження, ускладнення процесу прийняття рішень та зниження здатності до концентрації. В умовах інформаційних війн ці стани можуть бути спровоковані цілеспрямованим затопленням інформаційного простору великою кількістю повідомлень, в тому числі конфліктуючих або неперевірених. Це призводить до того, що люди або намагаються відключитися від інформаційних потоків, або некритично приймають інформацію, що відповідає їхнім вже існуючим переконанням.

Вплив інформаційних війн на соціальну психологію суспільства є значним, оскільки вони можуть спричиняти глибокі соціальні та психологічні зміни, які можуть мати довготривалі наслідки. Отже, у сучасному інформаційному суспільстві критичне мислення є ключовим інструментом для розпізнавання та аналізу змісту повідомлень, що мають маніпулятивний характер.

Основа критичного мислення полягає у здатності людини запитувати, перевіряти факти, розрізняти думки від фактів, виявляти упередження та оцінювати джерела інформації. Цей навик дозволяє людям не стати жертвами інформаційної війни.

Інформаційна безпека є дуже важливою сьогодні, під час воєнного стану, адже неправильно подана чи помилкова інформація може змусити населення панікувати, вплинути на хід подій, прискорити міграцію населення, викликати психічні та фізичні захворювання. Нинішня агресивна війна добре демонструє, що інформація - це зброя масового ураження[3].

Освітні програми можуть грати вирішальну роль у формуванні інформаційної культури, що включає розуміння механізмів медіа, вміння критично

оцінювати інформацію та здійснювати відповідальний вибір джерел інформації. Психологічні програми, своєю чергою, допомагають зміцнити емоційну стійкість та розвинути стратегії протистояння інформаційному стресу.

Державні органи та міжнародні організації, також, відіграють ключову роль у захисті проти інформаційних війн. Вони можуть впроваджувати законодавчі заходи для регулювання інформаційного простору, забезпечувати підтримку факт-чекінгових ініціатив, розвивати міжнародну співпрацю у боротьбі з дезінформацією.

Отже, для захисту громадян важливо зосередитися на розробці та імплементації ефективних механізмів кібербезпеки, освітніх та психологічних програм, щоб знизити негативний вплив інформаційної небезпеки на суспільство.

Список використаних джерел:

1. Карнаух А. А., Шевчук З. Ю. Інформаційна війна на сучасному етапі розвитку суспільства [Електронний ресурс] // Національний педагогічний університет імені М. П. Драгоманова. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/18824/Karnaykh_Shevchuk.pdf (дата звернення: 08.11.2023)
2. Сергій Корсунський. Інформаційна складова війни: як Росія намагається послабити підтримку Заходу .20.07.22/https://www.radiosvoboda.org
3. /a/informatsiyna-viyna-rosiyskyy-vplyv/31811302.html
4. "Методи пропаганди" [Електронний ресурс]. Телекритика. 2014. URL: http://ru.telekritika.ua/kontekst/print/96572 (дата звернення: 08.11.2023)

Ключові слова: інформаційні війни, пропаганда, дезінформація, інформаційна безпека, кібербезпека, контроль над медіа.
Keywords: information wars, propaganda, disinformation, information security, cyber security, media control.

СТРАТЕГІЯ УПРАВЛІННЯ РИЗИКАМИ ПІД ЧАС ВОЄННОГО СТАНУ

Ничипорук Анастасія

студентка 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Управління фінансовою стійкістю підприємства здійснюється в умовах невизначеності, зумовленої науковим прогресом, нестабільністю політичної ситуації, зростанням конкуренції на товарних і фінансових ринках, посиленням глобалізаційних процесів та дефіцитом інформації, а також за наявності різноманітних способів і варіантів перетворення можливостей у дійсність та багатоваріантності реалізації управлінських рішень [1].

Важливою частиною у воєнний час є питання методів управління економічними ризиками підприємства. В основі цього питання стоять методи управління ризиками, але нажаль в воєнний стан в Україні призупиняти свою роботу, або навіть закриватися. Війна завдала величезної шкоди як українському бізнесу і державі, так і мирному населенню.

Одним з показників, що характеризують загальну картину втрат української економіки, є кількість діючих підприємств, які попри війну продовжили свою роботу та частково перекваліфікували свою діяльність під потреби ЗСУ [2].

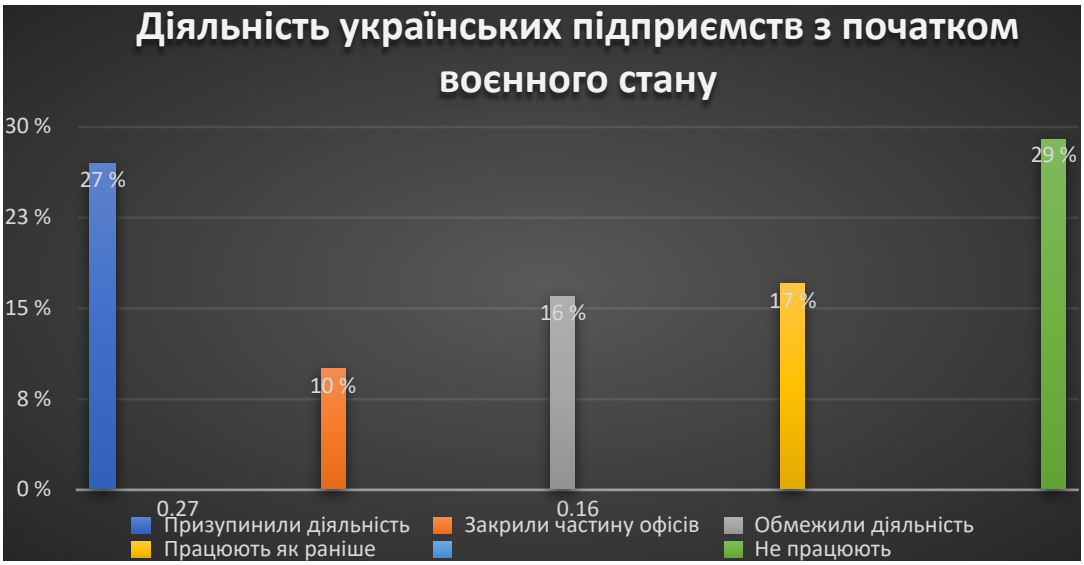


Рисунок 1 – Аналіз діяльності українських підприємств з початком війни [3].

Як показує діаграма(Рисунок 1) 27% підприємств призупинили свою діяльність, проаналізувавши дані можна сказати що це можливо через їх розташування яке не дозволяє благополучно розвивати свій бізнес. Але не зважаючи на це 17% підприємств працюють як раніше, тобто лише в деяких аспектах їх діяльність обмежена, але не критично. Під час війни існує багато ризиків, але бізнес в Україні розвивається, що дуже корисно впливає на економіку країни, бо саме з державного бюджету йдуть соціальні виплати, та кошти на ЗСУ.

«Київський політехнічний інститут імені Ігоря Сікорського» запропонував альтернативні методи запобігання ризиків в період воєнного стану, задля мінімізації економічних ризиків підприємств.

Таблиця 1 - Характеристика основних методів з мінімізації економічних ризиків підприємств в умовах військового стану [2].

Вид ризику	Вплив на підприємство	Метод мінімізації впливу ризику
Коливання курсу валют	Не залежно від того, чи займається компаніям експортом чи ні, вона залежить від коливання курсу валют. Адже з початку війни курс валют стрімко піднявся, і відповідно призвів до збільшення цін на більшість товарів. Особливо гостро позначилося підняття курсу валют на цінах на паливо та продовольчі продукти.	Використовувати хеджування для страхування ризиків від несприятливих змін цін на будь-які продукти за контрактами і комерційних операцій, що передбачають поставки (продажу) товарів в майбутніх періодах. Укладання довгострокових договорів на поставку за фіксованою ціною. Таким чином можна уникнути ризику коливань валютних курсів при здійсненні зовнішньоекономічних операцій.
Обмеження сировини та порушення логістичних ланцюгів	Порушення логістичних ланцюгів та встановлення списку критичного імпорту на іноземну сировину призвело до її дефіциту, що позначилося на неможливості вітчизняних компаній вчасно виконувати свої замовлення.	Постійне оновлення списку критичного імпорту. Створення резервних обсягів запасів сировини. Укладання договорів про спільну діяльність із виробниками сировини. Більш широка диверсифікація постачальників сировини для виробництва продукції. Передача операцій постачання продукції на аутсорсинг.
Зниження купівельної спроможності населення	Війна та її наслідки призвели до зростання цін товарів, що вплинуло на купівельну спромож-ність населення та одночасно позначилося на зменшенні покупок й погіршенні фінансових результатів діяльності підприємства.	Розробити лінійку продукції з врахуванням реальної купівельної спроможності населення.
Підвищення цін на нафту на світовому ринку	Через санкції ЄС для росії попит на нафту зріс, що призвело до зростання цін на пальне, які прямопропорційно вплинули на ріст кінцевої продукції.	Створення системи резервів на покриття непередбачених витрат. Гнучке управління і адаптація ціноутворення до змін цін на світовому ринку.
Зниження попиту	Зростання інфляції, зменшення зар плат та інші чинники призвели до зменшення попиту на товари зі сторони населення. Особливо гостро це позначилося на компаніях, які продають продукцію, яка не є товаром першої необхідності (меблі, одяг, нерухомість, тощо).	Розробити маркетингову програму формування лояльності споживача за допомогою використання акційних пропозицій і програму просунення продукції на ринок для розширення обізнаності споживача у властивостях і якості продукції.

Завдяки людям котрі знаються на управлінні ризиків, ми маємо шанс розвивати та створювати бізнес. Саме підприємці одні з головних платників податків, завдяки цим людям та їх робітникам ми маємо соціальні виплати, та гроші на потреби ЗСУ.

Список використаних джерел:

1. Приймак І. Управління ризиком втрати фінансової стійкості підприємства в умовах невизначеності зовнішнього середовища. Формування ринкової економіки в Україні. 2009. Вип. 19. С. 413–419.
2. Скоробогатова, Н. Є. Методи управління економічними ризиками в умовах військового стану / Скоробогатова Н. Є., Товкачова А. С., Федоренко К. В. // Бізнес, інновації, менеджмент: проблеми та перспективи : зб. тез доп. III Міжнар. наук.-практ. конф., м. Київ, 08 груд. 2022 р. – Київ, 2022. – С. 195-196.
3. Ярослав Голобородько (2022)Війна в Україні: економіка, бізнес, логістика, допомога URL: https://trans.info/ru/viyna-v-ukrayiniekonomika-biznes-logistika-dopomoga-279148

Ключові слова: внутрішні загрози, кібератаки, соціальний інжиніринг
Keywords: internal threats, cyberattacks, social engineering

Науковий керівник: к. ф.-м. н., доцент Чепурна О.Є.

ВПЛИВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ПОВЕДІНКУ КОРИСТУВАЧІВ: АНАЛІЗ МЕТОДІВ ТА ЗАХОДІВ ЗАХИСТУ

Нігуренко Аміна

студентка 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Інформаційні технології формують багато сфер життя, і суспільство стає все більш залежним від цифрового середовища. Однак водночас зростають загрози інформаційній безпеці та приватності користувачів.

З розвитком сучасних технологій інженери соціального впливу активно використовують психологічні та маніпулятивні методи для отримання доступу до конфіденційної інформації та ресурсів. Вони використовують соціальні мережі, фішингові атаки та інші методи для отримання конфіденційних даних, які можуть бути використані в різних шахрайських діях.

Крім того, інциденти кібербезпеки, пов'язані з соціальною інженерією, можуть мати серйозні наслідки, такі як фінансові втрати, витік конфіденційної інформації, порушення конфіденційності та втрата репутації. У цьому контексті для окремих користувачів, організацій та урядів стало дуже важливо розробляти та впроваджувати методи та заходи захисту від соціальної інженерії.

З огляду на активну діджиталізацію суспільства та зростання кількості цифрових атак, важливим завданням є вивчення цього питання та розробка відповідних заходів захисту. Зосередившись на цих аспектах разом, ми зможемо забезпечити вищий рівень інформаційної безпеки та допомогти користувачам краще захистити свою інформацію.

Соціальна інженерія (social engineering, социнжиніринг) – це метод маніпулювання думками та вчинками людей. Він базується на психологічних особливостях особистості та закономірності людського мислення [1].

В контексті соціальної інженерії, "інженери" використовують психологічні методи, маніпулювання та обман, щоб переконати людей робити певні дії або розкривати конфіденційну інформацію.

Основною ідеєю соціальної інженерії є використання соціальних навичок та знань про психологію для маніпулювання людьми з метою отримання користі або доступу до конфіденційної інформації. Соціальні інженери можуть виглядати як довірливі співробітники, колеги або навіть друзі, але їхня мета завжди полягає в обмані та зловживанні довіри.

Психологічні аспекти соціальної інженерії включають в себе різні аспекти поведінки та ментального стану користувачів, які використовуються соціальними інженерами для досягнення своїх цілей. Важливим є розуміння

цих аспектів, оскільки вони визначають, наскільки успішно інженер може маніпулювати особою або організацією [7].

Ключові психологічні аспекти соціальної інженерії:

1. Довіра: спроможність соціальних інженерів завоювати довіру користувачів є важливим аспектом. Вони можуть виглядати довірливими особами, які вселяють віру та переконують відкрити конфіденційну інформацію або виконати певні дії.
2. Вразливість: знання психологічних слабкостей та вразливостей користувачів, таких як страхи, амбіції, споживчі побажання, може допомогти соціальним інженерам вибудувати ефективну стратегію маніпуляції.
3. Соціальний інженеринг та вплив на почуття важливості: часто соціальні інженери створюють ситуації, де користувачі відчувають себе важливими, що стимулює їх до виконання запитаних дій.
4. Маніпулювання соціальними нормами: вони можуть використовувати норми та цінності, загальні для конкретної спільноти, щоб переконати осіб дотримуватися певних вимог.
5. Емоційна маніпуляція: здатність викликати певні емоції у користувачів, такі як страх, або зацікавленість, є ефективним інструментом впливу.
6. Авторитет і доручення: соціальні інженери можуть видача себе за авторитетних осіб, що мають повноваження, щоб вплинути на користувачів.

Вплив соціальної інженерії на користувачів полягає в тонкому мистецтві маніпуляції психологією людей. За допомогою цього підходу зловмисники можуть викликати бажану реакцію або отримати доступ до конфіденційної інформації, використовуючи соціальні інженерні методи. Вони можуть представляти себе як надійні особи або використовувати психологічний тиск, щоб переконати користувачів виконати певні дії або розкрити інформацію. Такі атаки можуть бути дуже ефективними, оскільки вони не вимагають використання складних технічних засобів, а замість цього базуються на психологічних слабкостях людей.

Вплив соціальної інженерії на користувачів є важливою проблемою в сучасному цифровому світі. Зловмисники постійно шукають нові способи маніпуляції та використовують соціальну інженерію для досягнення своїх цілей. Тому розуміння методів та заходів захисту від соціальної інженерії є надзвичайно важливим для забезпечення безпеки та конфіденційності в інтернеті.

Метод соціальної інженерії охоплює сукупність прийомів (фішинг, вішинг, претекстінг тощо), застосування яких можливе лише щодо особи, яка взаємодіє з кіберпростором шляхом використання електронно-цифрових приладів (комп'ютера, планшета, мобільного телефону тощо) [2].

Соціальна інженерія може призвести до серйозних психологічних та фінансових наслідків для користувачів та організацій. Користувачі, які стають жертвами атак соціальної інженерії, можуть відчувати страх, невпевненість та втрату довіри до інтернет-користувачів. Вони можуть сумніватися у своїй здатності розпізнавати атаки та стати більш обачливими щодо відомих та невідомих контактів.

Фінансові втрати також можуть бути серйозними. Зловмисники можуть шахрайством отримати доступ до банківських рахунків, кредитних карт, а також використовувати обман для вимагання грошей або викрадення фінансових даних.

Один із наслідків атак соціальної інженерії – це поширення конфіденційної інформації. Зловмисники можуть використовувати соціальну інженерію для отримання конфіденційної інформації про користувачів або організації, в наслідок чого психологічні та фінансові наслідки атак соціальної інженерії можуть бути дуже серйозними і можуть мати потенціально велику шкоду для жертв.

У кіберсередовищі загрози, пов'язані із соціальною інженерією, мають свої особливості:

1.Анонімність: зловмисники можуть легко залишати анонімні сліди в інтернеті та використовувати фальшиві профілі, що робить їх важко відстежити.

2.Глобальний доступ: завдяки інтернету соціальна інженерія може атакувати користувачів та організації з будь-якої точки світу, що робить цю загрозу глобальною.

3.Збільшені ризики онлайн спілкування: в інтернеті користувачі часто довіряють інформації та людям, з якими вони спілкуються, навіть якщо ці інформація та люди є ненадійними.

4.Соціальні мережі та онлайн-профілі: зловмисники можуть використовувати інформацію з соціальних мереж та онлайн-профілів для створення переконливих атак.

5.Застосування психології: соціальна інженерія включає в себе використання психологічних та маніпулятивних методів для досягнення мети, що робить її особливо небезпечною в онлайн-середовищі.

Соціальна інженерія є складним та хитрим видом кібератак, який базується на психологічних маніпуляціях та обмані. Вплив соціальної інженерії на поведінку користувачів та організацій є значним, призводячи до психологічних негараздів, фінансових втрат та розповсюдження конфіденційної інформації. Користувачі повинні бути уважними та освіченими щодо можливих атак та методів захисту. Організації повинні вдосконалювати свої стратегії та

заходи захисту, а також навчати свій персонал розпізнавати атаки соціальної інженерії.

Запобігання атакам соціальної інженерії вимагає комплексного підходу, що включає в себе технічні заходи захисту, освіту та навчання користувачів та співробітників, а також постійне оновлення стратегій та заходів захисту відповідно до змінюючогося кіберсередовища. У світі, де кіберзагрози постійно зростають, ефективний захист від соціальної інженерії стає надзвичайно важливим завданням для користувачів та організацій.

Список використаних джерел:

1. Соціальна інженерія. Інтернет джерело. URL: https://ukeywaf.com/baza/soczialna-inzheneriya/
2. Козицька О. Г. Використання методу соціальної інженерії в процесі виявлення, розкриття та розслідування кримінальних правопорушень. Юридична психологія. Випуск № 1(28). 2021.
3. Горбатенко О. А. Використання соціальної інженерії в кіберзлочинах: аналіз та заходи захисту. Юридичний журнал. Випуск № 3(37). 2017.
4. Іванова О. В., Петренко В. С. Сучасні аспекти соціальної інженерії в кіберпросторі. Інформаційні технології та комп'ютерна інженерія. Випуск № 5(65). 2019. С. 67-74.
5. Кузнєцов Д. Ю. Соціальна інженерія: психологічні методи атаки та захисту від них. Організаційна психологія. Випуск № 8(1). 2018. С 64-81.
6. Литвиненко О. П., Савченко І. В. Засоби захисту від соціальної інженерії для організацій в Україні. Інформаційні технології та комп'ютерна інженерія. Випуск № 4. 2020.
7. Тетяна Савчук. Соціальна інженерія. Інтернет джерело. URL: http://surl.li/hsung

Ключові слова: соціальна інженерія, психологічні аспекти, кіберсередовище, кіберзагрози, кібератаки.
Keywords: social engineering, psychological aspects, cyber media, cyber threats, cyber attacks.

Науковий керівник: к. ф.-м. н., доцент Чепурна О.Є.

СУЧАСНИЙ ПІДХІД ДО УПРАВЛІННЯ ФІНАНСОВИМИ РИЗИКАМИ

Шамес Владислава

студентка 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Діяльність фірми, саме фінансова діяльність, пов'язані з різними видами ризиків, які впливають її результати. Такі ризики, що супроводжують фінансову діяльність фірми, поєднують у спеціальну групу, назва якої – фінансові ризики. У загальному портфелі ризиків фірми ця група ризиків займає особливу, головну роль.

Фінансовий ризик - імовірнісна характеристика події, яка у віддаленій перспективі може призвести до виникнення втрат, неотримання доходів, недоотримання чи отримання додаткових доходів, внаслідок усвідомлених дій кредитної організації під впливом зовнішніх та внутрішніх факторів розвитку в умовах невизначеності економічного середовища [1, с.42-43].

У діяльності, що з управлінням фінансовими ризиками, вивчаються такі чинники, які впливають рівень ризиків фірми. Аналіз цих факторів проводиться з метою виявлення рівня керованості фінансовими ризиками та встановлення способів їхнього зниження. Усі чинники, які впливають на рівень фінансових ризиків, можна поділити на зовнішні та внутрішні, які розглянуті нижче у таблиці 1 [2, с. 123].

Таблиця 1. Фактори, що впливають на рівень фінансових ризиків

Зовнішні фактори	**Внутрішні фактори**
Рівень економічного розвитку країни	Основні напрямки фінансової стратегії
Державне регулювання фінансової складової діяльності фірми	Наявність фінансових коштів у фірми
Темпи інфляції у країні	Розмір власного капіталу фірми
Кон'юнктура попиту та пропозиції на фінансовому ринку	Склад активів, що використовуються
Рівень конкуренції у готельних сегментах фінансового ринку	Раціональність використання фінансових ресурсів
Економічний стан у галузі діяльності	Види фінансових інструментів, що використовуються фірмою
Рівень криміногенної обстановки у регіоні діяльності	Рівень кваліфікації фінансових менеджерів фірми

Джерело: [3].

До особливо важливих зовнішніх факторів можна віднести: зміну відсоткових та податкових ставок, мит, інфляцію, різні зміни у трудовому законодавстві тощо. Вплив внутрішніх факторів, таких як помилки у діяльності керівництва та персоналу, також небезпечно впливають на діяльність фірми. Зарубіжні експерти зробили висновок, що близько 90% невдач фірм, насамперед, пов'язані з малим досвідом керівництва в управлінні персоналом, а також невмінням пристосовуватися до умов середовища, що швидко змінюються. Все це призводить до збільшення помилок у прийнятті рішень та, відповідно, до зниження позицій фірми на ринку.

До внутрішніх чинників також можна віднести і суб'єктивний чинник ставлення ризику. Готовність ризикувати у всіх людей є різною. Деякі керівники готові постійно ризикувати, а інші, своєю чергою, з обережністю підхо-

дять до ризику або зовсім не хочуть ризикувати. Вибір тієї чи іншої стратегії у діяльності підприємства залежить від поведінки людей. Ті керівники, які обирають стратегію, яка не схильна до ризику, обирають постійний стабільний дохід. Керівники, які абсолютно нейтрально ставляться до ризиків, розраховують на той дохід, який очікують, незважаючи на ймовірні збитки. Керівники, які готові ризикувати, зазвичай хочуть отримати найбільший прибуток [4, с. 245-147].

Введення системи ризик-менеджменту у практичну діяльність компанії дає можливість стабільного розвитку, підвищення ухвалення обдуманих рішень у ситуаціях схильних до ризику, а також розвинути фінансове становище за рахунок контролю усіх видів діяльності. Отож, пропонуємо виділити чинники, що впливають величину ступеня ризику, можна розділити на об'єктивні і суб'єктивні (рис. 1).

До об'єктивних чинників ставляться причини, що у зовнішньому середовищі підприємства, тобто які залежить від діяльності фірми [5, с. 66-76; 6]. Суб'єктивні чинники пов'язані з внутрішнім середовищем фірми та характеризують її діяльність.

Зовнішні фактори ризиків виникають поза господарюючим суб'єктом і можуть істотно впливати на його діяльність. Чинники, що виникають у соціально-економічній сфері, призводять до зміни ситуації на ринку і викликають появу нових конкурентів, нових товарів.

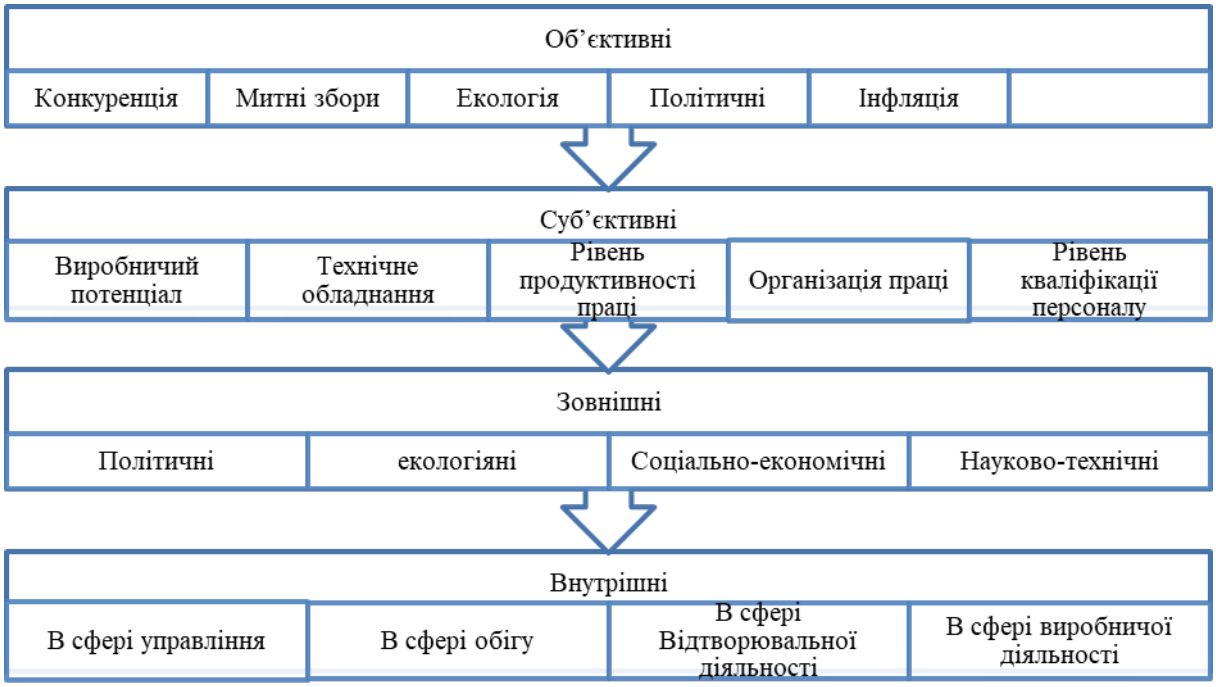


Рисунок 1 - Ключові фактори ризику

Джерело: Складено автором

Управління фінансовими ризиками базується на таких ключових постулатах ризик-менеджменту: ризики незалежні та нейтралізуються індивідуально, у всіх випадках можна знайти рішення, яке забезпечує компроміс між загрозою втрат та очікуваною вигодою.

У процесі управління фінансовими ризиками використовуються різноманітні зовнішні та внутрішні механізми їхньої нейтралізації. При цьому першорядне значення мають саме внутрішні механізми та методи, що розробляються та здійснюються самим суб'єктом підприємницької діяльності. Система управління фінансовими ризиками має значний арсенал прийомів та методик нейтралізації, мінімізації та компенсації ризиків.

Одним із поширених методів управління фінансовими ризиками є їхня диверсифікація. Під диверсифікацією розуміється розсіювання фінансового ризику з допомогою розподілу активів, капіталу між різними об'єктами вкладення [7].

Механізм диверсифікації застосовується насамперед з метою нейтралізації негативних наслідків, пов'язаних з дією внутрішніх факторів фінансового ризику (специфічні, несистематичні ризики). Дані види ризиків можуть бути обумовлені недооцінкою деяких напрямів фінансової діяльності, неефективною структурою активів та капіталу, некваліфікованим управлінням та іншими причинами. Залежно від об'єкта розрізняють диверсифікацію в масштабі діяльності суб'єкта підприємництва та диверсифікацію в масштабі окремих видів ризикових активів (інструментів) при їхньому розподілі між різними об'єктами вкладення.

Створення сучасної та ефективної системи ризик-менеджменту, що відповідає всім вимогам післяреформеного конкурентного ринку, є одним із першорядних факторів комерційного успіху компанії. Особливо важливо це для українського ринку в лібералізованому середовищі, реструктуризація якого призводить до значних змін та появи нових фінансових ризиків для його учасників, де кожна компанія має самостійно обирати прийнятний функціональний рівень для своєї системи ризик-менеджменту [8].

Таким чином, існує велика різноманітність методів та мінімальних вимог для управління фінансовими ризиками в компаніях з метою досягнення головних завдань фінансової політики будь-якої компанії – недопущення високої ймовірності банкрутства та отримання найбільшого прибутку з наданням високоякісних послуг.

Вибір методів управління фінансовим ризиком підприємства передбачає використання як стереотипного, і оригінального рішення, що містить економічно обґрунтовані рекомендації та заходи, створені задля зменшення стартового рівня фінансового ризику до прийнятного рівня.

Список використаних джерел:

1. Боровик М. В. Ризик-менеджмент : конспект лекцій для студентів магістратури усіх форм навчання спеціальності 073 Менеджмент. М. В. Боровик ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2018. 65 с.
2. Скакальський Ю.С. Контролінг фінансових ризиків підприємств: дис. канд. ек. наук: 08.00.08. Київ, 2018. 231 с.
3. Фінансовий менеджмент : підручник за ред. д-ра екон. наук, проф. М. І. Крупки. Львів : ЛНУ імені Івана Франка, 2019. – 440 с.
4. Управління фінансовими ризиками: навч. посіб. С. Г. Шклярук. Київ : ДП «Вид. дім «Персонал», 2019. 494 с.
5. Бездітко О. Є. Управління фінансовими ризиками підприємства. Таврійський науковий вісник. Серія: Економіка. 2020. Вип. 3. С. 43–49
6. Орлик О. В. Фінансові ризики в системі забезпечення фінансово-економічної безпеки підприємства. Інноваційна економіка. 2016. № 5–6 [63]. С. 218–223.
7. Бєлоусова С. В. Механізм управління фінансовими ризиками промислових підприємств. Проблеми і перспективи економіки та управління. 2019. № 3 (19). С. 277–293
8. Ковальчук Н.О., Федишин М.П., Жаворонок А.В. Теоретичні аспекти аналізу складу, структури активів та джерел їх фінансування. Інвестиції: практика та досвід. 2019. № 23. С. 64–69. DOI: https://doi.org/10.3 2702/2306-6814.2019.23.64 (дата звернення: 07.11.2023).

Ключові слова: управління, ризики, кібербезпека.
Keywords: governance, risks, cybersecurity.

Науковий керівник: к. ф.-м. н., доцент Черевко Є.В.

ОСНОВНІ ФОРМИ ПРОФІЛАКТИКИ РИЗИКІВ НА ПІДПРИЄМСТВІ

Муль Валерій

студента 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Постійні загрози, з якими зазвичай зіштовхуються підприємства, важливо мати чіткий розуміння щодо основних форм профілактики ризиків. Забезпечення безпеки та стабільності в організації може бути досягнуто за допомогою різноманітних стратегій. Серед таких форм профілактики ризиків на підприємстві можна виділити систематичний аналіз ризиків, впровадження ефективних політик з безпеки, навчання персоналу з питань безпеки та охорони праці, а також впровадження технологічних заходів для захисту даних та інформації. Ці стратегії сприяють не лише запобіганню можливих проблем, але й створенню здорової та безпечної робочої атмосфери, що сприяє стійкому розвитку підприємства в довгостроковій перспективі[1].

Основні форми профілактики ризиків на підприємстві з'явилися внаслідок потреби у забезпеченні безпеки та стабільності в робочих умовах. Історія цих форм профілактики пов'язана з розвитком індустрії та зростанням усвідомлення ризиків, які можуть впливати на діяльність підприємств.

У давні часи, особливо в традиційних суспільствах, збереження безпеки на робочому місці вважалося менш пріоритетним, оскільки більший наголос робився на продуктивності. Проте з поширенням промисловості у 19-20 століттях та збільшенням складності технологічних процесів з'явилася потреба у систематичному підході до управління ризиками.

Згодом, у 20 столітті зростання усвідомлення про шкоду для людського здоров'я та довкілля, що може бути спричинена несправними промисловими процесами, призвело до встановлення правил та норм безпеки на робочому місці. Це стало основою для розвитку законодавства та стандартів щодо безпеки праці.

З появою комп'ютерів та інших інформаційних технологій у 20 столітті з'явилися нові виклики у забезпеченні кібербезпеки, що прискорило розвиток стратегій профілактики ризиків в цьому секторі.

Сьогодні форми профілактики ризиків на підприємстві продовжують розвиватися та адаптуватися до сучасних викликів, що створюється швидким темпом технологічного прогресу та зростанням світового бізнесу.

Зважаючи на постійну зміну умов діяльності підприємств, основні форми профілактики ризиків стають все більш складними та розширеними. Ось більш докладний огляд цих стратегій:

1. Систематичний аналіз ризиків: Цей процес передбачає не тільки ідентифікацію можливих загроз, але й оцінку ймовірності їх виникнення та потенційних наслідків. Це включає аналіз внутрішніх і зовнішніх факторів, які можуть впливати на діяльність підприємства, і розробку стратегій для управління цими ризиками.

2. Ефективні політики безпеки: Розробка чітких і комплексних політик безпеки, які охоплюють широкий спектр аспектів, таких як охорона праці, здоров'я та безпека, пожежна безпека, кібербезпека та захист інтелектуальної власності. Ці політики повинні бути інтегровані в усі сфери діяльності підприємства, щоб забезпечити високий рівень безпеки.

3. Навчання та тренінги з безпеки та охорони праці: Організація регулярних навчальних курсів та тренінгів для персоналу з питань безпеки, процедур запобігання нещасним випадкам та екстрених ситуацій. Це дозволяє персоналу ефективно реагувати на можливі небезпеки та запобігати їх виникненню.

4. Використання передових технологій для захисту даних та інформації: Впровадження сучасних систем кібербезпеки, шифрування даних, бе-

капів та інших технологічних заходів для захисту від кібератак, витоку конфіденційної інформації та інших кіберзагроз. Ці стратегії не тільки забезпечують безпеку та захищеність підприємства, але й сприяють підвищенню довіри споживачів та партнерів і підвищенню конкурентоспроможності підприємства на ринку.

Висновуючи, основні форми профілактики ризиків на підприємстві є невід'ємною складовою успішного та стійкого управління. Ці стратегії допомагають підприємствам уникати можливих небезпек, забезпечуючи безпеку та стабільність діяльності в умовах постійних змін і несприятливих факторів зовнішнього середовища[2].

Систематичний аналіз ризиків дозволяє виявити та оцінити потенційні загрози, що можуть впливати на підприємство, тоді як ефективні політики безпеки забезпечують створення безпечного та здорового робочого середовища для співробітників. Навчання персоналу з питань безпеки та використання передових технологій для захисту даних інтегруються в загальний план заходів, спрямованих на запобігання негативним наслідкам ризиків[3].

Застосування цих стратегій допомагає підприємствам підтримувати конкурентоспроможність, забезпечуючи сталість бізнес-процесів та надійність у взаємодії з клієнтами та партнерами. Тим самим, вони створюють підґрунтя для сталого розвитку та процвітання підприємства в сучасному конкурентному середовищі.

Список використаних джерел:

1. Кривов'язюк І. В., Смерічевський С. Ф., Кулик Ю. М. Ризик-менеджмент логістичної системи машинобудівних підприємств : монографія. Київ : Кондор, 2018. 200 с.
2. Миколайчук І. П. Формування організаційно-економічного механізму управління ризикозахищеністю підприємства. Академічний огляд. 2018. № 2(49). С. 45–52. DOI: https://doi.org/10.32342/2074-5354-2018-2-49-4
3. Koev S. R., Tryfonova O., Inzhyievska L., Trushkina N., Radieva M. Management of Domestic Marketing of Service Enterprises. IBIMA Business Review. 2019. Vol. 2019. P. 1–13. DOI: https://doi.org/10.5171/2019.68170938. Trushkina N. Dev

Ключові слова: управління, ризики, кібербезпека.
Keywords: governance, risks, cybersecurity.

Науковий керівник : к. ф.-м. н., доцент Черевко Є.В.

СУЧАСНІ ПРОБЛЕМИ ВЗАЄМОДІЇ ЛЮДИНИ І КІБЕРСЕРЕДОВИЩА

Руденко Каріна

студентка 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасний світ переживає революцію інформаційних технологій, яка впливає на всі сфери нашого життя. У життя сучасної людини активно впроваджуються інформаційно-комунікативні технології, які не мають аналогів у минулому[2]. Кіберсередовище стає все більш невід'ємною частиною нашої повсякденності, перетворюючи спосіб, яким ми спілкуємося, навчаємося, працюємо та відпочиваємо. Проте цей розвиток також викликає велику увагу до питань управління та соціально-психологічних аспектів цього кібернетичного простору. Під кіберпростором розуміється середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення (ПЗ) і послуг в Інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі[3].

Кіберсередовище не обмежується лише технічними аспектами, воно також формує соціальні та психологічні реалії нашого сучасного світу. Управління цим простором вимагає не лише технологічної експертизи, але і розуміння впливу цифрового середовища на суспільні відносини та психологію індивідів.

Управлінські та соціально-психологічні аспекти кіберсередовища є ключовими для розуміння сучасного світу, і їх вивчення допомагає сформувати більш повне уявлення про те, як ми функціонуємо у цьому цифровому столітті.

Соціально-психологічні аспекти кіберсередовища визначають спосіб, яким ми взаємодіємо в цифровому світі, впливають на нашу психологію. З одного боку, інтернет створює можливості для спілкування та співпраці, допомагає збирати та обмінюватися інформацією. З іншого боку, це середовище може призводити до проблем, таких як кібербулінг, інтернет-залежність та порушення приватності.

Співвідношення між онлайн та офлайн життям стає предметом соціальних та психологічних досліджень. Питання про вплив соціальних мереж, віртуальної реальності та онлайн-ігор на психіку та емоційний стан особистості стають все важливішими.

Стає зрозумілим, що на даному етапі розвитку людства, існування особистості поза взаємодією з комп'ютерними системами вже важко уявити. Проведення індивідами в мережі все більшої кількості часу, як виразна тенденція надання переваги мережевій комунікації та використання послуг кі-

берпростору з метою віртуальної самореалізації, підтверджують надзвичайну актуальність цього питання.

Один з ключових аспектів кіберсередовища є управління цим середовищем. Висока швидкість розвитку технологій та об'єм інформації, що генерується в інтернеті, створюють виклики для бізнесу, уряду та громадянського суспільства.

У цих умовах актуальною є проблема визначення змісту терміна “кібернетична безпека”. Кібербезпека - це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах [1]. Зростання кількості кібератак та загроз вимагає розробки стратегій та заходів для захисту інформації, інформаційних систем та мереж. Організації повинні вдосконалювати свої підходи до кібербезпеки та навчати персонал виявляти й реагувати на ці загрози.

Психологічний вплив кіберсередовища на людину не може бути недооцінений. Онлайн-середовище впливає на наші ставлення, спосіб спілкування та сприйняття світу. Спілкування у соціальних мережах може впливати на формування самооцінки та ставлення до інших.

Кіберпростір також створює виклики для соціальних відносин. Питання етики та правил спілкування в інтернеті стають важливими, оскільки цифровий світ дозволяє анонімність і може призводити до негативних проявів, таких як кібербулінг та онлайн-гонитви.

Співвідношення між реальним та віртуальним життям стає предметом соціальних досліджень. Вирішення проблематики негативних проявів кіберпростору, є надзвичайно важливим завданням, оскільки ці явища можуть значущо впливати на психологічний стан та добробут індивідів. Нижче наведено кілька способів вирішення цієї проблематики:

- Просвітницькі заходи: Один з ключових шляхів боротьби з кібербулінгом та онлайн-гонитвами - це посилення освіти та усвідомлення проблеми серед дітей, підлітків та їх батьків. Школи та організації повинні надавати інформацію про небезпеки цифрового світу та способи виявлення та запобігання кібербулінгу.
- Створення безпечних онлайн-середовищ: Платформи та соціальні мережі повинні приділяти особливу увагу виявленню та блокуванню користувачів, які здійснюють кібербулінг чи онлайн-гонитви. Технологічні рішення, такі як алгоритми виявлення образливих коментарів, можуть бути корисними.
- Підтримка та консультування: Важливо створити середовище, де жертви кібербулінгу та онлайн-гонитв можуть шукати допомогу та підтримку. Психологічна підтримка та консультування можуть допомогти жертвам подолати емоційні та психологічні труднощі.

Отож, кіберсередовище стало необхідною складовою сучасного світу, і його управління вимагає особливої уваги та підходів. Управління кібербезпекою стає надзвичайно важливим завданням у цифровому світі. Організації повинні розробляти стратегії та заходи для захисту інформації та інформаційних систем від кіберзагроз.

Список використаних джерел:

1. Баранов, О. А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика, 2014, 2.42: 54-62.
2. Данильян, О. Г.; дзьобань, о. П. Віртуальна реальність і кіберпростір як атрибути сучасного суспільства. Інформація і право, 2020, 4 (35): 9-21.
3. Завгородня, Ю. В. Кіберпростір як сучасна платформа для політичних конфліктів. Publishing house “baltija publishing”, 2021.

Ключові слова: кіберпростір, кіберсередовище, кібербезпека, онлайн середовище
Keywords: cyberspace, cyber environment, cybersecurity, online environment

Науковий керівник : к. ф.-м. н., доцент Черевко Є.В.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УПРАВЛІННІ ПЕРСОНАЛОМ

Снігур Ксенія

студентка 4-го курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

У сучасному світі очевидним є факт що підприємства не можуть ефективно працювати без застосування нових технологій в своїй діяльності. Тому поширення інформаційних технологій стає невід’ємною частиною управлінської діяльності.

Неможливість управління традиційними методами на більшості підприємств, це пов’язано зі значним зростанням обсягу різного виду інформації. З кожним роком кількість керуючих відділів на підприємствах зростає. Для ефективного функціонування бізнесу керівництву підприємства необхідно оперативно приймати рішення з управління, які базуються на повноті інформації, кваліфікації персоналу та можливості вирішення різноманітних завдань в автоматизованих системах різного рівня та призначення. У цьому контексті, завдання управління людськими ресурсами (human recourses, HR) набуває пріоритетного значення для будь-якої організації.

Системи управління людськими ресурсами (Human Resource Management, HRM) або системи інформації про людські ресурси (Human Resources Information System, HRIS) представляють собою CRM-системи, що

сприяють ефективному управлінню персоналом. Це комплексні системи автоматизації, які спрощують процеси найму, відбору, залучення персоналу, забезпечують орієнтацію, навчання і розвиток, оцінюють їх роботу, визначають винагороди та надають пільги, мотивують, підтримують належні відносини з кожним членом команди та забезпечують безпеку роботи за рахунок застосування програм для HR і HR-аналітики. Як обов'язковий атрибут сучасного підприємства, вони давно широко впроваджуються на українських підприємствах.

У корпоративному процесі ключовим етапом є вибір підходящої програми щодо управління персоналом і системи HR – менеджерів. У сучасних умовах практично усі компанії обирають програмне забезпечення для автоматизації функцій у сфері HR. Вже недостатньо лише мати переліки працівників та їхніх заробітних плат, а також використовувати Excel-таблиці для відстеження відпусток і лікарняних. Важливо мати можливість вести облік робочих годин, відпусток і лікарняних в єдиній системі.

Сучасні технології змінили підхід до керування повсюдними процесами у сфері HR, надаючи зручне програмне забезпечення для HR-менеджерів та працівників компаній. Системи управління людськими ресурсами (HRM / HRIS) допомагають у виведеній бюрократії та оптимізації численних організаційних процесів.

В обов'язки відділу кадрів входить моніторинг історії, навичок, здібностей, заробітних плат та досягнень співробітників. Заміна певних процесів високого рівня системи HRM для HR може перерозподілити обов'язки з управління інформацією. Розглянемо головні задачі автоматизованих процесів управління персоналом за допомогою HRM-систем:

Рис. 1. HRM-система [2].

Також розглянемо як HRM-системи сприяють досягненню ключових бізнес-цілей, наведено в таблиці:

Таблиця

Ключова роль HRM-систем у досягненні бізнес-цілей

Ціль	Сутність
Ефективне управління персоналом	Оптимізація процесів з найму, розвитку, оцінки та звітності полегшує управління персоналом.
Автоматизація рутинних процесів	Зменшення навантаження на рутинні адміністративні завдання через автоматизацію, що дозволяє персоналу більше уваги приділяти стратегічним завданням.
Покращення комунікації	Забезпечення ефективного обміну інформацією між високими рівнями управління та працівниками для підвищення комунікації та співпраці.
Аналіз та звітність	Забезпечення точної аналітики та звітності для прийняття стратегічних управлінських рішень на основі даних про персонал.
Розвиток та навчання	Підтримка процесів навчання та розвитку працівників для підвищення їх професійного рівня та адаптації до нових вимог.
Управління талантами	Виявлення та утримання ключових талантів, підвищення мотивації та розвиток кар'єри працівників.
Забезпечення відповідності	Виконання законодавчих вимог та нормативів, що регулюють управління персоналом та робочими відносинами.

Безпека відіграє критичну роль у виборі систем HRM, оскільки дані, що зберігаються в них, мають високий ступінь конфіденційності, включаючи корпоративну інформацію та персональні дані співробітників. Компаніям необхідно вибирати рішення, які використовують безпечні методи передачі, такі як SSL. Це надає можливість шифрувати дані під час роботи з Інтернетом.

Інформація на підприємствах захищена паролями з різними рівнями доступу, що відповідають робочим потребам. Незважаючи на те, що більшість компаній дозволяють своїм робітникам мати доступ до окремих частин своїх HRM-рішень, співробітники повинні усвідомлювати важливість збереження цілісності системи та захисту інформації, яка в ній міститься (наприклад, заборону спільного використання паролів).

Крім того, повинні бути вжиті заходи для швидкого відмовлення у доступі до системи звільненим працівникам. Таким чином, безпека є важливим аспектом при виборі та використанні систем HRM. Враховуючи все вищезазначене зробимо слідуючі висновки:

1. Ефективність HRM-систем. HRM-системи, як інструменти інформаційних технологій, можуть значно підвищити ефективність управління персоналом, автоматизуючи рутинні процеси та забезпечуючи точні дані для прийняття рішень.
2. Досягнення бізнес-цілей. Завдяки підвищеній ефективності, HRM-системи можуть допомогти організаціям досягти своїх ключових бізнес-цілей, зокрема збільшення продуктивності, зниження витрат та підвищення задоволеності персоналу.
3. Роль інформаційних технологій. Інформаційні технології відіграють важливу роль в сучасному управлінні персоналом. Вони не лише спрощують процеси управління, але й надають можливість для стратегічного планування та аналізу.
4. Інтеграція HRM-систем. Інтеграція HRM-систем з іншими бізнес-системами може допомогти організаціям отримати більш повне розуміння своєї роботи та виявити можливості для подальшого розвитку.
5. Навчання та розвиток персоналу. Інформаційні технології, такі як HRM-системи, можуть сприяти навчанню та розвитку персоналу, надаючи доступ до онлайн-ресурсів та платформ.
6. Виклики та можливості. Незважаючи на переваги, використання цифрових технологій в управлінні персоналом також ставить перед нами нові виклики, такі як захист даних, конфіденційність та потреба в постійному оновленні технологій.

Отже, використання HRM-систем та інших інформаційних технологій щодо управління персоналом відіграє важливу роль у досягненні ключових бізнес-цілей. Проте, для успішного впровадження та використання цих технологій потрібно враховувати ряд викликів та проблем.

Список використаних джерел:

1. Що таке HRM і навіщо потрібна оптимізація HR-процесів? Інтернет-ресурс. URL: https://peopleforce.io/uk/blog/shho-take-hrm-i-navishho-potribna-optimizatsiya-hr-protsesiv
2. Седікова І.О, Козак К.Б., Седіков Д.В., Управління персоналом в умовах глобальних інформаційних процесів. Економіка харчової промисловості. Том 14, Випуск 2/2022. С.51-57.
3. Бардадим С. А. Діджиталізація HR-процесів в організації / С. А. Бардадим, С. М. Невмержицька, Т. Р. Цалко // Інноватика в освіті, науці та бізнесі: виклики та можливості : матеріали II Всеукраїнської конференції здобувачів вищої

освіти і молодих учених, м. Київ, 18 листопада 2021 року. Т. 2. Київ : КНУТД, 2021. С. 54-59.

Ключові слова: HRM-системи, бізнес-цілі, інформаційні технології, управління персоналом, цифрові виклики
Keywords: HRM systems, business goals, information technologies, personnel management, digital challenges

Науковий керівник: д.е.н., професор Слободянюк О.В.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В АНАЛІЗІ ФІНАНСОВОГО СТАНУ ПІДПРИЄМСТВ

Кедік Олена
студентка 4-го курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Сучасні інформаційні технології набувають великого значення в житті сучасної людини, але у цій статті ми розглянемо їх з точки зору економічної ефективності й сучасного менеджменту. За допомогою інформаційних програм ми можемо спрогнозувати витрати, поліпшити фінансові результати підприємства.

Фінансове планування є однією з найважливіших складових системи фінансового управління підприємством, оскільки кожне підприємство, починаючи свою діяльність, зобов'язане чітко уявляти потребу у фінансових, трудових і матеріальних ресурсах та джерела їх формування. [1] Тому у сучасному бізнесовому середовищі важливість забезпечення не лише високого рівня фінансової стійкості підприємств, але й розробка та впровадження ефективних інструментів для аналізу та управління фінансовим станом є надзвичайно актуальною.

Використання інформаційних технологій в аналізі фінансового стану підприємств включа' використання програмних пакетів для статистичної обробки даних, програмних засобів для оцінки екологічних параметрів економічної діяльності, програмних продуктів для аналізу безпеки технічних систем, та програмних пакетів для оцінки фінансових параметрів підприємств. [2] Також Застосування ІТ дозволяє автоматизувати процес збору фінансової інформації, роблячи його точнішим і ефективнішим. Інформаційні технології надають можливість проводити аналіз фінансового стану підприємств в режимі реального часу, що дозволяє оперативно реагувати на зміни та вчасно коригувати стратегію. Використання ІТ-інструментів дозволяє створювати точні фінансові моделі та прогнози на основі різноманітних сценаріїв, що сприяє більш точному розумінню можливих ризиків та вигід. Застосування

сучасних технологій гарантує високий рівень безпеки фінансової інформації, забезпечуючи конфіденційність та запобігаючи несанкціонованому доступу. Фінансові інтегровані платформи, інтелектуальний аналіз даних, електронна звітність та документообіг є прикладами IT-рішень у фінансовому аналізі.

Наведемо декілька програмних продуктів, які використовують підприємства при аналізі фінансового стану:

1. Програмні пакети для статистичної обробки даних. Ці інструменти допомагають аналізувати великі набори даних і виявляти тенденції та закономірності, які можуть бути непомітними при поверхневому огляді.
2. Програмні засоби для оцінки екологічних параметрів економічної діяльності. Ці інструменти можуть допомогти підприємствам визначити вплив їхньої діяльності на навколишнє середовище, що може мати важливе значення для їхньої репутації та фінансового стану.
3. Програмні продукти для аналізу безпеки технічних систем. Ці інструменти можуть допомогти підприємствам виявити потенційні ризики та вразливості в їхніх технічних системах, що може допомогти їм уникнути великих витрат у майбутньому.
4. Програмні пакети для оцінки фінансових параметрів підприємств. Ці інструменти можуть допомогти підприємствам аналізувати такі параметри, як прибуток, витрати, дохід та інші ключові фінансові показники. [3]

Таким чином використання сучасних інформаційних технологій в аналізі фінансового стану підприємств може допомогти підприємствам поліпшити їх фінансові результати шляхом прогнозування даних. Це включає в себе використання різних програмних пакетів та інструментів для аналізу різних аспектів фінансового стану підприємства і не лише сприяє ефективному управлінню, але і забезпечує підвищення точності та достовірності результатів.. А завдяки використанню інформаційних технологій в аналізі фінансового стану підприємств підприємства досягають не лише ефективності управління, але й підвищують рівень точності та достовірності отриманих результатів. Технологічний прогрес є ключовим інгредієнтом для сучасного фінансового аналізу, дозволяючи компаніям вирішувати виклики із вищою точністю та швидкістю, а також ключовим фактором для сучасного фінансового аналізу, забезпечуючи точніше та швидше вирішення викликів.

Список використаних джерел:

1. Свистун Л. А. Перспективи використання сучасних інформаційних технологій при здійсненні фінансового планування на підприємстві. Економіка і регіон. 2016. № 3. С. 13-21.

2. Левченко Л.О.,. Кілянчук О.П, Повханич О.Ю. Огляд програмних продуктів фінансово-економічного аналізу діяльності енергопідприємств URL: https://urss.knuba.edu.ua/files/zbirnyk-8/121-127.pdf
3. Л.І. Дробот. Етапи виконання та інформаційна база фінансово-економічного аналізу господарської діяльності підприємства URL: Етапи виконання та інформаційна база фінансово-економічного аналізу господарської діяльності підприємства.pdf (uzhnu.edu.ua)

Ключові слова: фінансовий аналіз, інформаційні технології, підприємства, автоматизація, аналіз в реальному часі, прогнозування та моделювання, безпека інформації
Keywords: financial analysis, information technologies, enterprises, automation, real-time analysis, forecasting and modeling, information security

Науковий керівник: д.е.н., професор Слободянюк О.В.

КІБЕРКУЛЬТУРА: СТІЙКІСТЬ В УМОВАХ СЬОГОДЕННЯ

Горбанець Катерина

студентка 4-го курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Корпоративна культура відіграє важливу роль у формуванні стійкості підприємства, особливо в умовах кризи. Вона створює сприятливий клімат на підприємстві, що спонукає працівників намагатися виправдати очікування керівника, виконуючи покладене ними завдання у необхідному обсязі та у строк.

Сьогодні менеджмент компаній визнає, що корпоративна культура стає активом, який вимагає обережного та цілеспрямованого управління. Фірми з розвиненою культурою виграють у тому числі за рахунок людського капіталу: компанії, які вкладають більше коштів у своїх співробітників за часів стабільності, мають вищу продуктивність праці в умовах кризи, тому що в таких компаніях співробітники сильніше мотивовані та продуктивніші. Ця теза знаходить обґрунтування в результатах, отриманих PwS під час глобального дослідження «Корпоративна культура: час діяти» 3, проведеного в 2021 році шляхом глобального опитування 3243 керівників та співробітників із 42 країн [1-2].

У сучасному світі, де кіберсередовище стає все більш поширеним, корпоративна культура повинна адаптуватися до цього нового контексту. Це може включати в себе розробку нових стратегій та підходів до мотивації, комунікації та управління в умовах віддаленої роботи. Соціально-психологічні аспекти кіберсередовища, такі як взаємодія в команді, мотивація та віддалена робота, можуть впливати на корпоративну культуру. Наприклад, підпри-

ємства можуть використовувати ці аспекти для підвищення ефективності діяльності підприємства та зростання трудового потенціалу. [3].

Слід вивчати кращі зарубіжні практики компаній, виявляти каталізатори, що використовуються ними для зміцнення корпоративної культури, і гнучко застосовувати їх у своїх компаніях. Найчастіше згадуваними каталізаторами виступають: культурні риси та позитивні приклади моделей поведінки вищого керівництва, суттєва підтримка співробітників з боку вищого керівництва, технології та інструменти проактивної взаємодії в колективі, премії, компенсації та винагороди за внесок у бізнес-результати, можливості для особистісного та професійного зростання співробітників та проведення відповідних тренінгів, формальна комунікація, взаємопідтримка співробітників, залучення та залучення співробітників, комунікація на основі зворотного зв'язку та прийняття відповідних управлінських рішень. Зі зростанням числа використовуваних каталізаторів зміцнення корпоративної культури істотно підвищується її здатність виступати джерелом сили та конкурентної переваги, забезпечувати швидшу адаптацію компанії до змін. [4].

На сьогоднішній день підприємства з інноваційною корпоративною культурою мають максимальне конкурентне перевагу, оскільки вони характеризуються великою адаптивністю, що дуже важливо в умовах постійно мінливої довкілля. Працівники мають високий професійний рівень, відчувають турботу і підтримку менеджменту, що сприяє розвитку почуття причетності до спільної справи та спільних проблем. На підприємствах реалізуються оригінальні проекти, що забезпечують їм конкурентні переваги.

А корпоративна культура та кіберсередовище взаємопов’язані, і обидва вони відіграють важливу роль у стійкості підприємства в умовах кризи. Ефективне управління цими двома аспектами може допомогти підприємствам краще адаптуватися до змін та подолати виклики.

Список використаних джерел:

1. Global Culture Survey 2021. URL: https://www.pwc.com/gx/en/issues/upskilling/global-culture-survey-2021.html.
2. М. В. Орлик, І. О. Царенко. Роль корпоративної культури в системі фінансово-економічної безпеки. 2016. С. 301.
3. Ворожбит В. В. Система цінностей у корпоративній культурі як засіб підтримки економічної безпеки підприємства. URL: http://www.repository.hneu.edu.ua/jspui/handle/123456789/2652
4. Зеліч В.В. Роль та місце корпоративної культури та її вплив на розвиток підприємства. URL: http://market-infr.od.ua/journals/2017/6_2017_ukr/6.pdf
5. Краснокутська Н.С., Кришталєва О.В. Розвиток корпоративної культури в умовах віддаленого режиму роботи URL: 11.pdf (vernadskyjournals.in.ua)

Ключові слова: кіберкультура, стійкість, кіберсередовище, цифровий світ, технологічні зміни, соціальна адаптація, інформаційне суспільство
Keywords: cyberculture, resilience, cyberspace, digital world, technological changes, social adaptation, information society

Науковий керівник: д.е.н., професор Слободянюк О.В.

МЕТОДОЛОГІЧНІ ПІДХОДИ ДО УПРАВЛІННЯ РИЗИКАМИ

Музика Герман
студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У процесі управління ризиками ключове завдання полягає в прийнятті стратегічних рішень, які спрямовані на зменшення негативного впливу внутрішніх та зовнішніх чинників на операції компанії, а також на зниження потенційних збитків від непередбачених подій. Першочерговим завданням є попередження ситуацій, що можуть призвести до фінансових втрат та інших небажаних наслідків для підприємства. Процес управління ризиками включає оцінку ризиків, аналіз технічних і технологічних можливостей фірми, її економічний потенціал, умови робочого середовища та прогнозування майбутніх змін у законодавчому полі. У цьому контексті використовуються економічно-математичні моделі, маркетингові дослідження та інші інструменти.

Додатково, процес управління ризиками включає розроблення стратегії та тактичних планів. Основні принципи, які мають бути враховані при формуванні та впровадженні стратегії управління ризиками в організації, включають системний підхід, постійність процесу, розподіл відповідальності та ініціатив, використання аналітичних та евристичних методів для оцінювання ризиків, розгляд альтернативних сценаріїв та активне прогнозування [1].

Сучасні науковці пропонують різноманітні методики оцінки ризиків. Узагальнюючи їх підходи, можна виокремити наступний алгоритм. На етапі "Збір та аналіз інформації" визначаються ключові фактори ризику, вплив яких на діяльність компанії потрібно мінімізувати. Головною ціллю "аналізу ризику" є встановлення максимально прийнятного рівня ризику для різних ситуацій, а для відомих ризиків - визначення їх меж прийнятності. Важливо відрізняти якісний та кількісний аналіз ризиків на підставі зібраної інформації. Методики аналізу ризиків представлені на рисунку 1.

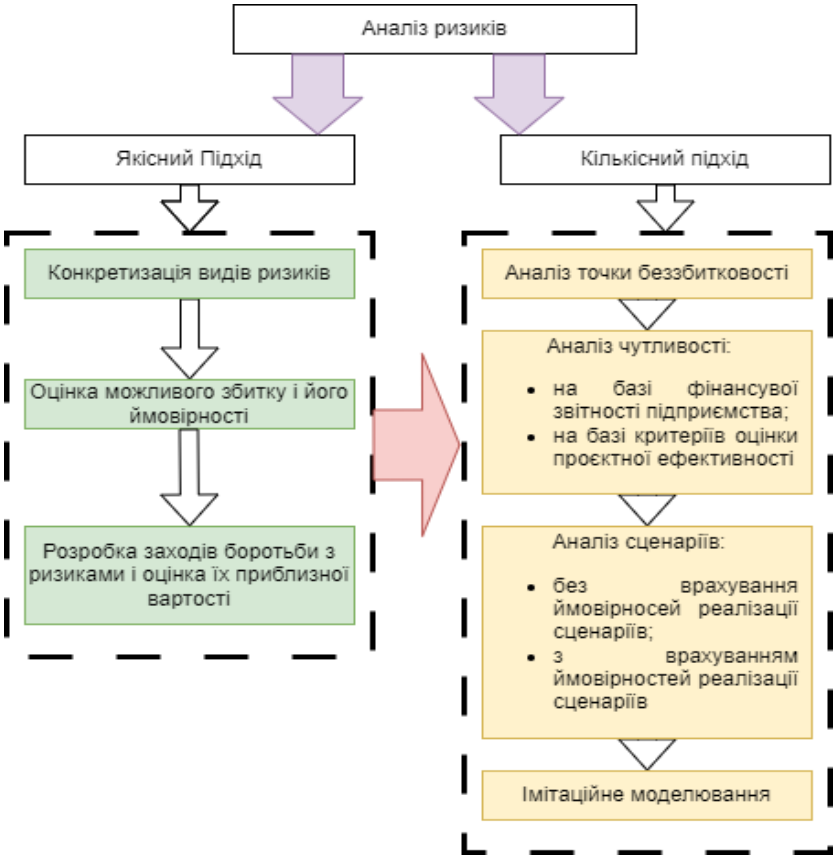


Рис. 1 – Процедура аналізу ризиків

Основна характеристика якісного підходу до аналізу ризиків полягає у послідовності кроків: спершу ідентифікуються потенційні ризики, а потім здійснюється оцінка їх можливих наслідків та розробляються стратегії їх контролю. Такий аналіз рекомендовано виконувати на стадії планування проекту. У той час як кількісний аналіз грунтується на застосуванні методів теорії імовірностей та математичної статистики, зосереджуючись на числовій оцінці впливу ризикових чинників на результативність проекту, доповнюючи при цьому якісний аналіз.

Головні методи якісного та кількісного аналізу викладені у таблиці 2. Якісний аналіз відіграє ключову роль у виявленні всіх потенційних ризиків, встановленні ризикових факторів та визначенні послідовності подій, що можуть призвести до цих ризиків.

З іншого боку, кількісний аналіз зосереджується на визначенні обсягу потенційних збитків від різноманітних ризиків. Він аналізує причини та джерела ризику, а також оцінює ймовірність настання можливих наслідків. Наприклад, система контролю та діагностики банкрутства є аналогічною до аналізу фінансових ризиків, використовуючи схожі фінансово-економічні індикатори для визначення фінансового стану підприємства [2].

На даний момент існує багато методів оцінки ризиків, включаючи двофакторну модель, коефіцієнти Альтмана, чотирьохфакторну модель Таф-

флера, експертні судження, аналіз ефективності витрат та інші. Однак, слід зазначити, що використання виключно математичного підходу, заснованого на первинних даних, може бути недостатнім для повного розуміння масштабу та ймовірності ризику.

Статистичний метод оцінки ризиків аналізує інформаційну базу збитків та прибутків підприємства, визначаючи розмір і частоту виникнення ризикових подій, та на цій основі формує прогнози майбутнього стану системи.

Таблиця 2 – Методи якісні та кількісні методи аналізу

Метод	Суть	Особливості
Якісні методи аналізу ризиків		
Конкретизація видів ризиків	Передбачає збір та детальне вивчення інформації про майбутній проект та притаманні йому ризики.	Вимагає часових і фінансових затрат на отримання інформації
Метод аналогій	Передбачає порівняння зарядом ознак майбутнього проекту з раніше втіленими проєктами.	Вимагає повнити інформації для розуміння ступеня її застосовності у конкретній ситуації
Причинно-наслідковий аналіз	Передбачає евристичне виділення ризикових подій формальний логічний аналіз їх можливих причин і розробку антикризових заходів	Застосовується на передінвестиційній стадії стимулює пошук варіантів підвищення надійності проекту в цілому
Метод “Подій - наслідки”	Передбачає поділ проекту на елементи і виявлення ризиків для кожного з них	Застосовується для виявлення специфічних ризиків
Кількісні методи аналізу ризиків		
Коригування норми дисконтування	Передбачає збільшення ставки дисконтування відповідно до сукупності ризиків, що впливають на «проект».	Не враховує зміни рівня ризику в ході реалізації «проекту».
Метод достовірних еквівалентів	Передбачає експертне коригування грошових потоків залежно від суб'єктивної оцінки рівня ризику.	Небезпека методу полягає в суб'єктивності експертної оцінки та відсутності обґрунтованих методів розрахунку безризикових еквівалентів.
Аналіз показників ефективності	Розглядає запас міцності проекту і виявляється відносними показниками.	Надає лише агреговану оцінку всіх проектних ризиків.

Аналіз чутливості	За допомогою внесення почергових одиночних змін до техніко-економічних параметрів «проекту» виявляються найбільш впливаючі ризики.	Дозволяє оцінити ступінь відхилення параметра, при якому «проект» стає збитковим.
Метод сценаріїв	За допомогою одночасного внесення змін до низки техніко-економічних параметрів формуються альтернативні сценарії розвитку «проекту».	Усуває обмеження по кількості факторів порівняно з аналізом чутливості.
Імітаційне моделювання	Передбачає побудову фінансової моделі і багаторазовий розрахунок сценаріїв «проекту», з урахуванням кореляції між його параметрами.	Вимагає спеціального програмного забезпечення та додаткових досліджень; складний у використанні.
Методи, що поєднують кількісний та якісний аналіз		
Методи експертних оцінок	Центральною фігурою цього методу являється експерт що проводить оцінки за допомогою логічних і статистичних методів	Перевагою даного методу являється відсутність необхідності в точних вигідних даних і дороговартісних програмних засобах для обліку впливу різноманітних факторів використовується досвід експерта
Створення профілю ризиків або картки ризиків	Передбачає оцінку ризиків проекту за рядом параметрів і відображення їх на групи відповідних шкал. Отриманий профіль порівнюється з еталонним.	Являється інструментом візуалізації структури ризиків і оцінки відповідності проекту політиці організації у сфері ризику

Експертні аналізи забезпечують можливість інтегрувати різні точки зору експертів для оцінки ймовірності ризиків з метою встановлення прийнятних рівнів ризику або оцінки потенційних втрат. Так, експертам пропонують оцінити шанси на виникнення ризиків за спеціальною шкалою, де нуль означає мінімальний ризик, а сто - абсолютну неминучість ризикованої ситуації [3].

Серед відомих методик збору експертних оцінок вирізняють такі: метод "Делфі" (досягнення консенсусу серед експертів через опитування, інтерв'ю та групові обговорення); метод "Снігової кулі" (аналіз усіх можливих альтернатив та ймовірностей, що призводить до "лавиноподібного" зростання обсягу інформації) [4].

Метод "Дерева цілей" (структурування цілей до рівня планованих та контрольованих дій); метод "Круглого столу" (обговорення різних підходів до вирішення проблем для вибору найкращого рішення); метод евристичного прогнозування (створення прогностичної моделі та застосування евристичних підходів і логічного аналізу для отримання оцінок); матричний метод (аналіз доцільності витрат, побудова кривих ризиків або проведення аналогій) [5].

Таким чином, існують численні методи оцінювання потенційних ризиків, які допомагають визначити загальний обсяг ризиків для компанії. Компанії можуть уникати прийняття ризикованих рішень, використовуючи ці методики як на етапі попереднього аналізу, так і під час діяльності для коригування в разі підвищення ризиків. На сьогодні існує багато способів для мінімізації ризиків.

Список використаних джерел:

1. Економічні, соціальні та психологічні аспекти сучасних маркетингових технологій / В.А. Фалович [та ін.] ; за ред. д.е.н, доц. В.А. Фаловича. – Тернопіль: ФО-П Шпак В. Б., 2019. – 231 с. (дата звернення: 04.11.2023)
2. Шурда К.С. Методи якісного та кількісного аналізу ризиків. Український науковий центр екології моря (УкрНЦЕМ), Ukraine № 4 (2020) URL: https://orcid.org/0000-0003-0385-7731 (дата звернення: 04.11.2023)
3. Турінський О.В., Демідов Б.О., Гриб Д.А., Хмелевська О.О. Науково-методологічні аспекти управління ризиками у системі державного оборонного замовлення. Наука і техніка Повітряних Сил Збройних Сил України. 2020. № 2(39). С. 37-46. (дата звернення: 04.11.2023)
4. Цифрове суспільство: фінанси, економіка, управління: матеріали Міжнародної науково-практичної конференції. Дніпро : Університет митної справи та фінансів, 2020. 315 с. (дата звернення: 04.11.2023)
5. Сучасний рух науки: тези доп. XI міжнародної науково-практичної інтернет-конференції, 8-9 жовтня 2020 р. – Дніпро, 2020. – Т.1. – 440 с. (дата звернення: 04.11.2023)

Ключові слова: підхід, якісний метод, кількісний метод, ризик.
Keywords: approach, qualitative method, quantitative method, risk.

Науковий керівник: к.т.н., доцент Ахмаметьєва Г.В.

ПЕРЕФОРМАТУВАННЯ IT-СЕКТОРУ УКРАЇНИ В УМОВАХ ВІЙНИ

Баланюк Ростислав

студент 3-го курсу факультету адвокатури і антикорупційної діяльності Національного університету «Одеська юридична академія»

Останніми роками IT-індустрія є двигуном розвитку вітчизняної економіки чи не за всіма показниками: від експортної виручки до середньогалузевої виручки. І навіть під час війни більшість IT-компаній зберегло не лише потенційних, а й поточних клієнтів і контракти, незважаючи на такі ризики, як: затримки проекту через війну, мобілізація ключових інженерів, нестабільність у країні, фізична безпека даних, кіберзагрози, відсутність Інтернету, неможливість працювати з розробниками під час активних військових дій.

Кількісно, за даними першого кварталу 2022 року, вітчизняна IT-індустрія забезпечила за час війни рекордні 2 мільярди доларів, експортні надходження США.

Адже аналогічний показник у 2021 році становив 1,44 мільярда доларів США. Так, обсяг IT-експорту зріс на 28%. У галузі працює близько 300 тис. осіб. спеціалістів і 70% з них змінили місце проживання з початку 2022 року. Крім того у березні 2022 року українська IT-галузь зберегла 96% експорту IT-послуг (522 млн дол.) порівняно з аналогічним періодом минулого року (546 дол. США) мільйонів доларів США), що довело свій запас міцності в умовах нестабільності та підвищених ризиків.

Паралельно український IT-бізнес припинив співпрацю з РФ. Зокрема, там мали офіси 3 з 10 найбільших вітчизняних IT-компаній (EPAM, Luxoft, DataArt). І хоч не відразу після початку війни, але всі вони заявили про ліквідацію бізнесу в країні-агресорі. [1]

Основні економічні побоювання, пов'язані з роботою IT-сектору у військових умовах, зводяться передусім до двох пунктів: втрата клієнтів, проектів, і, отже, масове переміщення робочих місць і спеціалістів за кордон. Дійсно, в першому місяці війни близько 5-7% фахівців втратили роботу внаслідок активних бойових дій. Надалі оптимізація бізнесу почала визначатися процесами за рахунок зниження активності. Але такі компанії як Rozetka, EVO, Нова Пошта змогли зберегти свій бізнес з перших днів і до сьогодні ці компанії мають прибуток.

Якщо говорити про внутрішні територіальні зміни та географію під ча війни то найменше постраждали підприємства та спеціалісти у Львові, Тернополі та Івано-Франківську. Перший місяць війни було дуже важко в Києві та Одесі, але потім ситуація дещо вирівнялася. Найбільше постраждало IT-середовище у м. Дніпро, Харків і Запоріжжя.

Український надає допомогу IT-сектору для підтримки його діяльності шляхом тимчасового звільнення IT-фахівців від мобілізації, що має особливе значення для бізнесу. За оцінками фахівців, які працюють в IT-середовищі, частка мобілізованих не перевищує 5%, плюс додатковий відсоток складають волонтери.

Особливості IT-сектору дозволяють перенести в інші країни не тільки розробку програмних продуктів, але й обслуговування клієнтів, більшість IT-послуг і багато допоміжних бізнес-процесів. Тому, щодо аспектів переїзду, увага роботодавців зосереджується насамперед на безпеці працівників та швидкому переїзді зі східної частини країни у безпечне місце – на захід чи за кордон.

Звичайно, значна кількість IT-спеціалістів виїхала з України, і зазначений процес посилився з самого початку 2022 року. Серед країн, які відвідали IT-спеціалісти лідирує Польща (35%) та Німеччина (10%). Так само працюють команди в Ірландії, Болгарії та Португалії. Слід зазначити, що понад 90% IT-спеціалістів роблять фінансові внески в армію, в благодійні фонди або самі є волонтерами.

У контексті внутрішньої релокації найбільше IT-спеціалістів переїхало до Львівської області (11%), Івано-Франківської області (6%) та Закарпаття (9%). Для переважної більшості IT-фахівців робоче навантаження не змінилося в результаті переведення. Середня заробітна плата на всіх поточних посадах становить приблизно (у квітні 2022 року) 86,5 тис. грн. Найбільше пропозицій роботи з місячною винагородою 44,2 тис. грн. (36%). Ще в чверті вакансій зарплата становить від 77,5 тис. грн. [2]

Практика показує, що найпростіше знайти нову роботу керівникам проектів, розробникам, а також фахівцям DevOps/SRE, QA, Data Scientist і HR. Найважче для менеджерів з продажу, системних адміністраторів, спеціалісти технічної підтримки, дизайнери та маркетологи. Однак, незважаючи на те з точки зору складності, частка IT-фахівців, які все ще шукають роботу, не є такою великою і не перевищує 5%.

Таким чином, у нових умовах IT-індустрія залишається фінансово стабільною, забезпечує регулярне надходження валюти в економіку та державний бюджет України. Для подальшого розвитку вітчизняного IT-сектору в умовах воєнного часу необхідно зробити наступні додаткові кроки.

1. Створення умов для масової підготовки та перепідготовки IT-спеціальностей (певні кроки в цьому напрямку вже зроблені, адже такі компанії, як Genesis, EPAM, Beetroot вже або розробили нові курси для легшого входження в професію, або зробили власні курси безкоштовними).

2. Розробка пропозицій для великих іноземних компаній (з використанням державної підтримки) щодо залучення вітчизняних спеціалістів до умови аутсорсингу, можливо, у формі державного агентства зайнятості.

3. Перехід від великих офісів до мобільних бригад, це легше реалізувати як оперативне перенесення.

Список використаних джерел:

1. Українська IT-Індустрія: перезавантаження в умовах війни. URL: https://itukraine.org.ua/ukrainian-it-industry-reboot-in-wartime.html (Дата звернення : 16.11.2022).
2. Як війна вплинула на IT-сферу: зарплати, вакансії, локації. URL: https://minfin.com.ua/ua/2022/04/06/83259219/ (Дата звернення : 16.11.2022).

Ключові слова: IT-індустрія, зарплата, локація, пропозиція, підготовка IT-спеціалістів, аутсорсинг.
Keywords: IT industry, salary, location, proposal, training of IT specialists, outsourcing.

Науковий керівник: д.е.н., професор Слободянюк О.В.

ЗМІСТ

ПЕРЕДМОВА 4

Секція 1. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ ЯК ОСНОВА СУЧАСНОГО СУСПІЛЬСТВА…….....6

ТЕНДЕНЦІЇ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ: СУЧАСНІ ВИКЛИКИ
Дикий Олег 6

РОЛЬ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ В СЬОГОДЕННІ: ПРОБЛЕМАТИКА, ВИКЛИКИ ТА ЗАХОДИ ЗАХИСТУ
Ісмайлов Карен 8

АНАЛІЗ СУЧАСНИХ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ
Самойлов Станіслав 11

ДОСЛІДЖЕННЯ АЛГОРИТМУ ФОРМУВАННЯ СТЕГАНОГРАФІЧНОГО КЛЮЧА ДЛЯ ПОБУДОВИ ЗМІННИХ КРИПТОГРАФІЧНИХ S-БЛОКІВ
Ахмаметьєва Ганна 13

ВПЛИВ КІБЕРЗАГРОЗ НА ЕФЕКТИВНІСТЬ УПРАВЛІННЯ ПІДПРИЄМСТВОМ
Пунченко Наталія, Златова Марія…….....17

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ
Кухаренко Сергій…….....21

ДОСЛІДЖЕННЯ КІБЕРЗАГРОЗ ТА ОЦІНКА РИЗИКІВ КІБЕРБЕЗПЕКИ ЗАСОБАМИ IPYTHON / JUPYTERLAB
Бойко Віктор…….....24

ОГЛЯД МЕТОДІВ ВБУДОВУВАННЯ ІНФОРМАЦІЇ В ЗВУКОВІ ФАЙЛИ
Овчинников Микола……..……....27

УРАЗЛИВОСТІ СТЕКА ХАМРР
Стаднік Денис…….....30

ТЕХНОЛОГІЇ ПРИХОВУВАННЯ ПРИСУТНОСТІ В СИСТЕМІ
Соловйов Артем…….....33

БЕЗПЕЧНЕ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ БОЙОВИХ ДІЙ
Спесівцев Микола 35

ВИДИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ
Орел Анастасія 38

СПОСОБИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ЗА ДОПОМОГОЮ ЛОГ-ФАЙЛІВ
Раєв Олександр 41

АВТОМАТИЗАЦІЯ ПЕНТЕСТИНГУ ВЕБ-САЙТІВ ЗА ДОПОМОГОЮ МОВИ PYTHON
Жук Максим 44

КІБЕРБЕЗПЕКА ЯК ФАКТОР ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА
Тишко Ілонна 46

ВИЯВЛЕННЯ ЗЛОВМИСНОЇ АКТИВНОСТІ В КОРПОРАТИВНИХ ЛОКАЛЬНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ АНАЛІЗУ DNS-ЗАПИТІВ
Гуренко Марк 49

ДОСЛІДЖЕННЯ MALWARE З ВИКОРИСТАННЯМ МЕТОДІВ ВКЛАДЕНОЇ ВІРТУАЛІЗАЦІЇ
Величканич Юрій 51

HOLOMORPHIC IMMERSIONS OF COMPLEX MANIFOLDS
Josef Mikeš Professor 53

БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ В АРХІТЕКТУРІ СИСТЕМИ ОРКЕСТРАЦІЇ КЛАСТЕРІВ
Астахов Даниїл 57

ШЛЯХИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ
Кіфа Константин 59

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
Вінник Мирослава 62

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІННОВАЦІЙНИХ ПРОЕКТІВ В УМОВАХ СЬОГОДЕННЯ
Громов Ігор 66

БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ
Чеховський Андрій 69

THE STRESS-ENERGY TENSOR AND LCK-MANIFOLDS RESPECT TO CONFORMAL MAPPINGS
Patrik Peška, Olena Chepurna 71

КРИТИЧНА ІНФРАСТРУКТУРА ЯК ОБ'ЄКТ КІБЕРЗАХИСТУ
Саврацький Олександр....76

СТАНДАРТ АВТЕНТИФІКАЦІЇ FIDO2
Даниловська Каріна....78

БЕЗПАРОЛЬНА АВТЕНТИФІКАЦІЯ (PASSWORDLESS AUTHENTICATION)
Сіянко Кіріл....81

КРИТИЧНИЙ АНАЛІЗ МЕТОДОЛОГІЧНИХ ПІДХОДІВ ДО ОЦІНКИ КІБЕРРИЗИКІВ
Грезіна Олена....85

CYBER SECURITY CHALLENGES AND ITS EMERGING TRENDS ON LATEST TECHNOLOGIES
Paige Nikita Andrew....87

ЗАХИСТ ІНФОРМАЦІЇ ЩОДО УПРАВЛІННЯ ПЕРСОНАЛОМ: ВАЖЛИВИЙ ФАКТОР ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМСТВА
Шатунова Ксенія....90

ГЕНДЕРНІ АСПЕКТИ У КІБЕРБЕЗПЕЦІ: РОЛЬ СТАТЕВИХ СТЕРЕОТИПІВ У СВІДОМОМУ ТА БЕЗПЕЧНОМУ КОРИСТУВАННІ ІНФОРМАЦІЙНИМИ ТЕХНОЛОГІЯМИ
Осадчук Анастасія....92

ARTIFICIAL INTELLIGENCE: CHALLENGES AND HOW WE COULD DEAL WITH
Yevhen Cherevko, Yevheniia Kuleshova....95

КІБЕРПРОСТІР В УМОВАХ ВІЙНИ
Парамонова Юлія....97

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ
Арнаут Аліна....100

ВИКОРИСТАННЯ БІБЛІОТЕКИ SCAPY ДЛЯ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ
Дрига Артем....102

Секція 2. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В УМОВАХ ВІЙНИ 105

АНАЛІЗ ПОТЕНЦІЙНИХ ВИТОКІВ ДАННИХ В ПРИСТРОЯХ КОМУНІКАЦІЇ
Задерейко Олександр, Логінова Наталія, Троянський Олександр 105

СУЧАСНІ ІНСТРУМЕНТИ UI/UX ДИЗАЙНУ
Манаков Сергій 108

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ У СИСТЕМАХ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
Грезіна Олена 110

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ В РІЗНИХ СФЕРАХ ДІЯЛЬНОСТІ
Задерейко Олександр, Толокнов Анатолій, Черненко Олександра 113

GEOINT: МОЖЛИВОСТІ ГЕОПРОСТОРОВОЇ РОЗВІДКИ
Задерейко Олександр, Долінко Ксенія 118

ДОСЛІДЖЕННЯ ПОТУЖНОСТЕЙ МНОЖИН НЕЛІНІЙНИХ ПЕРЕТВОРЕНЬ ІЗ ЗАДАНИМИ ЗНАЧЕННЯМИ ПЕРІОДІВ ПОВЕРНЕННЯ У ВИХІДНИЙ СТАН
Баландіна Наталія 123

РОЗПОДІЛЕНІ МЕРЕЖІ ТА ЇХ РОЛЬ У БЛОКЧЕЙН-ТЕХНОЛОГІЯХ
Сметана Владислав 127

ЧИСЛА, ЩО НЕ ПІДДАЮТЬСЯ НАУКОВОМУ ПОЯСНЕННЮ
Шляхтицький Дмитро 131

СУЧАСНІ МЕТОДИ ДОСЛІДЖЕННЯ ТА ОЦІНКИ DDOS-АТАК
Щербина Юрій, Казакова Надія 136

МОЖЛИВОСТІ МОВИ C# ДЛЯ ОРГАНІЗАЦІЇ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ
Чикунов Павло 140

ШТУЧНИЙ ІНТЕЛЕКТ У ВІЙСЬКОВІЙ СФЕРІ
Трофименко Олена, Яремчук Максим 144

АЛГОРИТМИ У BACK-END ЗАСОБАМИ JAVA
Трофименко Олена, Старіков Ігор 148

ПРОГРАМНІ ЗАСОБИ ДЛЯ ARDUINO
Усатенко Ярослав 152

ПРОЕКТИ ОБРОБКИ ВІЗУАЛЬНИХ ДАНИХ
Пучков Владислав 155

РОЛЬ СИСТЕМНОГО АНАЛІЗУ В РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ
Ревацький Олександр 158

ДИСТАНЦІЙНИЙ КОНТРОЛЬ СИСТЕМ ЕНЕРГОЗАБЕЗПЕЧЕННЯ СЕРВЕРНОГО ОБЛАДНАННЯ ЗА УМОВ ЗБОЇВ ЕНЕРГОПОСТАЧАННЯ
Пшеничний Євгеній 161

ЦИФРОВА ТРАНСФОРМАЦІЯ ОСВІТНЬОГО ПРОЦЕСУ В ЗВО ПІД ЧАС ВІЙНИ
Кульбабський Анатолій 164

ЗАСТОСУВАННЯ МАТЕМАТИКИ В ПРОГРАМУВАННІ
Ковальський Олександр 168

СТВОРЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗА ДОПОМОГОЮ AGILE
Гурін Євген 170

ШТУЧНИЙ ІНТЕЛЕКТ У ВЕБРОЗРОБЦІ: РЕВОЛЮЦІЯ ПЕРСОНАЛІЗАЦІЇ КОРИСТУВАЧА
Дика Анастасія, Максименко Артем 174

РЕАЛІЗАЦІЯ АЛГОРИТМІВ MACHINE LEARNING У БАЗАХ ДАНИХ СІМЕЙСТВА NOSQL
Лобода Юлія 176

ХАРАКТЕРИСТИКА ФРЕЙМВОРКІВ ДЛЯ КРОСПЛАТФОРМНОЇ РОЗРОБКИ
Касян Павло 179

ВИКОРИСТАННЯ КОЛЕКЦІЇ TIDYVERSE В АНАЛІЗІ ДАНИХ
Сітько Анастасія 182

ВЕБРОЗРОБКА ЗАСОБАМИ ASP.NET CORE
Солом’яний Олексій 185

АНАЛІЗ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ УПРАВЛІННЯ
Фомічов Дмитро 187

РОЗРОБКА ЧАТ-БОТА ДЛЯ ПОШУКУ НЕРУХОМОСТІ
Петрушенко Мілєна 190

Секція 3. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ КІБЕРПРОСТОРУ 193

ЩОДО ОБОВ'ЯЗКОВОСТІ РЕЄСТРАЦІЇ ЮРИДИЧНИХ ОСІБ ПРИВАТНОГО ПРАВА В ЕЛЕКТРОННОМУ СУДУ
Купенко Артем 193

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ В ПРОЦЕСІ МЕДІАЦІЇ
Блатін Стівен 195

ІНФОРМАЦІЙНА ПОСЛУГА У СФЕРІ ГОСПОДАРЮВАННЯ: ПОНЯТТЯ ТА ОЗНАКИ
Деренюк Ангеліна 197

ЩОДО КІБЕРБЕЗПЕКИ ГОСПОДАРСЬКИХ ПРАВОВІДНОСИН
Ляховецький Олександр 201

ДЕЯКІ АСПЕКТИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ЗМІН
Грезіна Олена 204

ВИКОРИСТАННЯ АЛГОРИТМІВ YOUTUBE ДЛЯ ОРГАНІЗАЦІЇ ТЕРОРИСТИЧНИХ НАПАДІВ.
Динту Валерія 206

THE BLETCHLEY DECLARATION ТА ПРОБЛЕМИ МІЖНАРОДНОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ
Чанишев Рашид.....209

ПРАВОВА ПРИРОДА ШТУЧНОГО ІНТЕЛЕКТУ
Бааджи Наталія 213

СУЧАСНІ ПРОБЛЕМИ ВЗАЄМОДІЇ ЛЮДИНИ І КІБЕРСЕРЕДОВИЩА
Руденко Каріна 218

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ У СИСТЕМІ МІСЦЕВОГО САМОВРЯДУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ
Холостенко Світлана, Ровинська Катерина 220

Секція 4. УПРАВЛІНСЬКІ ТА СОЦІАЛЬНО-ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРСЕРЕДОВИЩА 223

ПАРИТЕТ ТРАНСПАРЕНТНОСТІ ТА КІБЕРБЕЗПЕКИ У ХОЛОКРАТИЧНІЙ МОДЕЛІ УПРАВЛІННЯ БІЗНЕСОМ
Горбаченко Станіслав 223

ІНТЕГРАЦІЯ КРИТИЧНИХ КОМПОНЕНТІВ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВОДНОГО ТРАНСПОРТУ
Пунченко Наталія 225

СТРАТЕГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ ТА ІННОВАЦІЙНОГО УПРАВЛІННЯ ДЛЯ СТАЛОГО РОЗВИТКУ СУСПІЛЬСТВА
Котлубай Вячеслав.....229

ЗАСТОСУВАННЯ ІНСТРУМЕНТІВ КІБЕРБЕЗПЕКИ В ЕКОНОМІЦІ ЗАМКНУТОГО ЦИКЛУ
Клєвцєвич Наталія 232

ВИКОРИСТАННЯ КОМПЛЕКСНИХ ЧИСЕЛ У РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ
Гурін Євген 236

ОСОБЛИВОСТІ ПРОСУВАННЯ БРЕНДІВ В КІБЕРСЕРЕДОВИЩІ
Рева Аніта 238

КІБЕРРИЗИКИ ФУНКЦІОНУВАННЯ ЕЛЕКТРОМОБІЛЬНОЇ ІНФРАСТРУКТУРИ
Разінкін Нікіта.....242

ПЕРСПЕКТИВИ РОЗВИТКУ СЕГМЕНТУ ГЕЙМДЕВ В УКРАЇНІ
Скідан Владислав.....246

СУЧАСНІ ТРЕНДИ ІНТЕРНЕТ-МАРКЕТИНГУ
Науменко Аліна 250

КІБЕРБЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ ШЛЯХОМ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ
Грезіна Олена 254

СУТНІСТЬ ТА НЕОБХІДНІСТЬ УПРАВЛІННЯ РИЗИКОМ
Дем’янова Тетяна 256

ВПЛИВ ІНФОРМАЦІЙНИХ ВІЙН НА СОЦІАЛЬНУ ПСИХОЛОГІЮ СУЧАСНИХ СУСПІЛЬСТВ
Чепурна Олена, Козловський Ігор....260

СТРАТЕГІЯ УПРАВЛІННЯ РИЗИКАМИ ПІД ЧАС ВОЄННОГО СТАНУ
Ничипорук Анастасія....262

ВПЛИВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ПОВЕДІНКУ КОРИСТУВАЧІВ: АНАЛІЗ МЕТОДІВ ТА ЗАХОДІВ ЗАХИСТУ
Нігуренко Аміна....265

СУЧАСНИЙ ПІДХІД ДО УПРАВЛІННЯ ФІНАНСОВИМИ РИЗИКАМИ
Шамес Владислава....268

ОСНОВНІ ФОРМИ ПРОФІЛАКТИКИ РИЗИКІВ НА ПІДПРИЄМСТВІ
Муль Валерій....272

СУЧАСНІ ПРОБЛЕМИ ВЗАЄМОДІЇ ЛЮДИНИ І КІБЕРСЕРЕДОВИЩА
Руденко Каріна....275

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УПРАВЛІННІ ПЕРСОНАЛОМ
Снігур Ксенія....277

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В АНАЛІЗІ ФІНАНСОВОГО СТАНУ ПІДПРИЄМСТВ
Кедік Олена....281

КІБЕРКУЛЬТУРА: СТІЙКІСТЬ В УМОВАХ СЬОГОДЕННЯ
Горбанець Катерина....283

МЕТОДОЛОГІЧНІ ПІДХОДИ ДО УПРАВЛІННЯ РИЗИКАМИ
Музика Герман....285

ПЕРЕФОРМАТУВАННЯ ІТ-СЕКТОРУ УКРАЇНИ В УМОВАХ ВІЙНИ
Баланюк Ростислав....290

ЗМІСТ....293

КІБЕРПРОСТІР В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: ТЕОРІЯ ТА ПРАКТИКА

МАТЕРІАЛИ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

24 листопада 2023 року
м. Одеса

Відповідальній редактор: О.В. Дикий

Дизайн та верстка:
М.Ю. Овчинников

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАТЕРІАЛИ МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

КІБЕРПРОСТІР В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: ТЕОРІЯ ТА ПРАКТИКА

24 листопада 2023 року, м. Одеса