МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НАУКОВО-ПРАКТИЧНИЙ ВИМІР В УМОВАХ ВОЄННИХ ВИКЛИКІВ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 26 квітня 2024 року

Одеса
«Фенікс»
2024

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 15.05.2024 р.)

За загальною редакцією ***С. В. Ківалова***

Відповідальний за випуск ***М. Р. Аракелян***

Є 24 **Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів** : матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2024. – 1000 с.
ISBN 978-617-8430-05-4

У збірнику відображено наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології в умовах повномасштабного військового вторгнення. Висвітлено питання загроз національній безпеці в їх конституційному вимірі у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов’язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики. Відображено наукові напрацювання у сферах адміністративного права та процесу, фінансового, морського та митного права, організації та вдосконалення судоустрою, прокуратури, інших правоохоронних органів, адвокатури. Висвітлено питання кримінального права, кримінально-процесуальних аспектів кримінального провадження та кримінологічних особливостей протидії злочинності в умовах воєнного стану, криміналістики, судової експертизи, психології та медицини у забезпеченні судочинства, цивільного та сімейного права, інтелектуальної власності та патентної юстиції, цивільного судочинства, господарського права та процесу. Розглянуто актуальні питання діяльності сучасних бібліотек у закладах вищої освіти, фізичної підготовки здобувачів вищої освіти.

Збірник розраховано на наукових і науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)»364»»20»(062.552)

Матеріали видано в авторській редакції

ISBN 978-617-8430-05-4

Лобода Юлія Геннадіївна
ГЕНЕРАЦІЯ НАБОРУ ДАНИХ ДЛЯ МАШИННОГО НАВЧАННЯ 860
Манаков Сергій Юрійович
ВІРТУАЛЬНІ ПОТОКИ JAVA ТА КОРУТИНИ KOTLIN 862
Чанишев Рашид Ібрагімович
ШТУЧНИЙ ІНТЕЛЕКТ ТА ПРАВО: ВИКЛИКИ ТА ПЕРСПЕКТИВИ РЕГУЛЮВАННЯ 864
Чикунов Павло Олександрович
ВІДСТЕЖЕННЯ ПОШИРЕННЯ ПО ПРОГРАМІ НЕПЕРЕВІРЕНИХ ЗОВНІШНІХ ДАНИХ 866
Щербина Юрій Володимирович
Казакова Надія Феліксівна
ДОСЛІДЖЕННЯ ПОТОЧНОГО ШИФРУ, ПОБУДОВАНОГОНА ОСНОВІ XORSHIFT-ГЕНЕРАТОРА 870
Грезіна Олена Миколаївна
ЦИФРОВА МАЙСТЕРНІСТЬ ТА ІННОВАЦІЇ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ – БЕЗПЕКОВІ ВИКЛИКИ ДЛЯ СФЕРИ ОСВІТИ 872
Соловйов Артем Сергійович
ПРОБЛЕМАТИКА ФАЛЬСИФІКАЦІЇ СИСТЕМНИХ ЖУРНАЛІВ У ОПЕРАЦІЙНІЙ СИСТЕМІ LINUX 874
Дика Анастасія Іванівна, Трофименко Олена Григорівна
АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ЗАСОБАМИ CHATGPT ДЛЯ ТЕСТУВАННЯ БЕЗПЕКИ ВЕБЗАСТОСУНКІВ 876
Проданюк Назар Богданович
ДЕЯКІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ ЮРИДИЧНИХ ПОСЛУГ У ЦИФРОВУ ЕПОХУ 878
Світлічний Ігор Валерійович
Світлічна Дар'я Ігорівна
ЧИ МАЮТЬ МИМОБІЖНІ ПРЯМІ ПРАВО НА ПЕРЕТИН? ДЕЯКІ АСПЕКТИ ЗНАХОДЖЕННЯ ВІДСТАНІ МІЖ МИМОБІЖНИМИ ПРЯМИМИ 880

СЕКЦІЯ 24. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

Горбаченко Станіслав Анатолійович, Дикий Олег Вікторович
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕСІ МАРКЕТИНГОВОГО ЦІНОУТВОРЕННЯ 883
Казакова Надія Феліксівна, Кулешова Євгенія Романівна
ВИБІР ТИПУ ХМАРНИХ ПОСЛУГ ТА РИЗИК ВИТОКУ ЧУТЛИВОЇ ІНФОРМАЦІЇ 885
Ахмаметьєва Ганна Валеріївна
ПРОБЛЕМИ РОЗПОВСЮДЖЕННЯ ФЕЙКОВИХ МУЛЬТИМЕДІА В МЕРЕЖІ INTERNET 887
Бойко Віктор Дмитрович
БІБЛІОТЕКА NUMPY – ОСНОВА ІНСТРУМЕНТАЛЬНОГО СТЕКУ НАУКОВИХ РОЗРАХУНКІВ SCIPY 888
Кухаренко Сергій Вікторович
ПОЛІТИКИ ТА ПРОЦЕДУРИ РЕАГУВАННЯ НА ПОРУШЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ 891
Чепурна Олена Євгенівна
КІБЕРЗАГРОЗИ ДЛЯ БІЗНЕС-СЕРЕДОВИЩА ТА СУЧАСНІ ЗАХОДИ ПРОТИДІЇ 893
Черевко Євген Володимирович
ШТУЧНИЙ ІНТЕЛЕКТ ТА ЙОГО ЗАСТОСУВАННЯ У ФУНДАМЕНТАЛЬНИХ ДОСЛІДЖЕННЯХ 895
Овчинников Микола Юрійович
ОСОБЛИВОСТІ ВБУДОВУВАННЯ ПРИХОВАНОЇ ІНФОРМАЦІЇ У ФАЙЛИ ФОРМАТУ MP3 898
Разінкін Нікіта Сергійович
КІБЕРЗАХИСТ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВІЙНИ 902
Саврацький Олександр Олександрович
ОСОБЛИВОСТІ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ В УМОВАХ ВІЙНИ 905

СЕКЦІЯ 25. ПИТАННЯ МЕТОДИКИ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ, ТЕОРІЇ ТА ПРАКТИКИ ПЕРЕКЛАДУ ЯК ЗАСОБУ НАЛАГОДЖЕННЯ КОМУНІКАЦІЇ

Томчаковська Юлія Олегівна
СТРАТЕГІЇ І ТАКТИКИ МЕДІЙНОГО ДИСКУРСУ 908
Строченко Леся Василівна
ПЕРЕКЛАД У ВІЙСЬКОВІЙ ГАЛУЗІ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ 910
Варєшкіна Наталія Володимирівна
ДО ПРОБЛЕМИ ВИКЛАДАННЯ АНГЛІЙСЬКОЇ МОВИ ЗА ПРОФЕСІЙНИМ СПРЯМУВАННЯМ 911
Дихта Наталя Миколаївна, Явдощук Анастасія Андріївна
НАВЧАННЯ ФОНЕТИЦІ АНГЛІЙСЬКОЇ МОВИ 913

рі [4, 5] та інших нормативних документах аналізуючи які можливо запропонувати наступні елементи, які повинні забезпечити реагування на інциденти:

1. Швидке та ефективне реагування та відновлення після інцидентів.

2. Забезпечення захисту від кібератак, витоків даних та інших загроз, що можуть призвести до фінансових втрат та втрат інформаційних активів.

3. Добре розроблений план реагування на інциденти з використанням безпечних методів, які спроможні мінімізувати наслідки інцидентів для подальшої безпечної роботи.

4. Управління наслідками порушення безпеки, збір доказів та вжиття заходів для запобігання подальшим атакам.

5. Мінімізація наслідків інцидентів безпеки та запобігання його повторенню з часом.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII у ред. від 01.01.2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Перелік категорій кіберінцидентів. Державна служба спеціального зв'язку та захисту інформації України. URL: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv

3. Реагування на інциденти. URL: https://cqr.company/ua/service/reaguvannya-na-incidenty/

4. Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : постанова КМУ від 04.04.2023 р. № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text

5. Методичні рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : наказ Адмін. Держ. служби спец. зв'язку та захисту інформації України від 03.07.2023 р. № 570. URL: https://ips.ligazakon.net/document/FN077992

Ключові слова: кібербезпека, кіберінцидент, політика безпеки, захист інформації, захист даних, кібератака.
Keywords: cyber security, cyber incident, security policy, information protection, data protection, cyberattack.

Чепурна Олена Євгенівна
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат фізико-математичних наук, доцент

КІБЕРЗАГРОЗИ ДЛЯ БІЗНЕС-СЕРЕДОВИЩА ТА СУЧАСНІ ЗАХОДИ ПРОТИДІЇ

В умовах сучасної гібридної війни, що охопила Україну, кіберпростір став ареною жорстоких зіткнень, які не менш значимі, ніж традиційні воєнні дії. Військові конфлікти тепер не обмежуються лише фізичним простором; вони проникають у віртуальний світ, де битви за інформаційний простір і безпеку даних стають вирішальними. Для бізнес-середовища в Україні, як і для всього суспільства, кіберзагрози в цей період набули особливої актуальності.

Кібератаки, фішинг, злом баз даних – це лише деякі з викликів, з якими зіткнулися українські компанії. У таких умовах, коли віртуальний фронт стає таким же важливим, як і фізичний, питання кібербезпеки виходить на перший план. Воно вимагає негайної уваги та координації зусиль на всіх рівнях – від окремих користувачів до великих корпорацій та державних структур.

Стратегічне планування, освіта та постійне оновлення заходів безпеки стануть ключовими в забезпеченні стійкості українського бізнесу та суспільства в цілому перед обличчям кіберзагроз воєнного часу [1].

Кіберзагрози для бізнес-середовища під час війни в Україні стали особливо актуальними та різноманітними, враховуючи збільшення кібератак та спроб злому інформаційних систем. Деякі ключові кіберзагрози, з якими може зіткнутися бізнес в Україні під час воєнних дій:

1. Фішингові атаки та соціальна інженерія – ці методи часто використовуються для отримання конфіденційної інформації, такої як паролі та фінансова інформація, через обман користувачів.

2. Розповсюдження шкідливого програмного забезпечення – включає віруси, трояни та шпигунські програми, які можуть бути спрямовані на крадіжку даних, знищення інформації або використання комп'ютерних систем жертви для розповсюдження малвар.

3. DDoS-атаки (Атаки розподіленого відмови в обслуговуванні) – спрямовані на перевантаження систем або мережі так, щоб вони стали недоступними для своїх легітимних користувачів.

4. APT (Advanced Persistent Threats – Розширені Тривалі Загрози) – це цілеспрямовані атаки, які зазвичай проводять державні або інші великі організації з метою шпигунства або саботажу.

5. Ransomware (Вимагацькі програми) – шкідливі програми, що блокують доступ до системи або файлів і вимагають викуп за їх розблокування.

6. Зломи баз даних та крадіжка інформації – несанкціонований доступ до баз даних з метою викрадення конфіденційної інформації, такої як персональні дані клієнтів або внутрішньої корпоративної інформації.

7. Маніпулювання інформацією або дезінформація – спроби вплинути на громадську думку або корпоративні рішення через розповсюдження фальшивої або вводять в оману інформації [2].

У зв'язку з цими загрозами, важливо для бізнесу в Україні впроваджувати комплексні заходи безпеки, включаючи навчання персоналу методам розпізнавання та запобігання фішинговим атакам, встановлення антивірусного програмного забезпечення, регулярне оновлення систем і програм, використання сильних паролів та багатофакторної аутентифікації, а також створення резервних копій важливих даних.

Сучасні заходи протидії кіберзагрозам включають широкий спектр стратегій та технологій, які допомагають захищати бізнес та індивідуальних користувачів від різноманітних видів кібератак. Основою цих заходів є не лише застосування передових технологічних рішень, але й формування культури кібербезпеки, постійне навчання та адаптація до змінюваних умов кіберпростору. До сучасних заходів протидії можна віднести:

1. Багатофакторна аутентифікація (MFA) – використання додаткових методів перевірки ідентичності користувачів, окрім пароля, таких як одноразові паролі, біометричні дані або спеціальні мобільні додатки.

2. Ендпойнт захист – встановлення антивірусного програмного забезпечення, антималварних рішень та систем запобігання вторгненням на всіх кінцевих точках мережі, включаючи мобільні пристрої та портативні комп'ютери.

3. Шифрування даних – застосування технологій шифрування для захисту конфіденційності даних під час їх зберігання та передачі.

4. Резервне копіювання та відновлення даних – створення регулярних резервних копій важливих даних для забезпечення можливості їх відновлення у випадку втрати або пошкодження.

5. Мережева сегментація – розділення мережевої інфраструктури на окремі сегменти для обмеження розповсюдження потенційних загроз та спрощення управління доступом.

6. Освітні програми для співробітників – проведення регулярних тренінгів з кібербезпеки для підвищення обізнаності персоналу про загрози та навчання безпечній поведінці в мережі.

7. Проведення пенетраційного тестування – регулярне виконання контрольованих атак на системи та мережі з метою виявлення вразливостей до їх використання зловмисниками.

8. Розробка плану реагування на інциденти – підготовка детального плану дій для ефективного реагування на кіберінциденти, що дозволяє швидко виявляти, локалізувати та усувати наслідки атак.

9. Співпраця з експертами з кібербезпеки – налагодження партнерства з професійними організаціями та службами кібербезпеки для обміну інформацією про загрози та кращі практики захисту.

В умовах сучасного цифрового світу, де кіберзагрози еволюціонують із кожним днем, захист інформації та систем стає невід'ємною частиною стратегії будь-якого бізнесу. Ефективна кібербезпека вимагає комплексного підходу, який об'єднує технологічні рішення, освітні програми для співробітників, регулярне тестування на вразливості та чіткий план реагування на інциденти. Інвестиції у заходи безпеки та неперервна увага до кіберзагроз не лише захищають від потенційних атак, але й сприяють створенню довіри з боку клієнтів та партнерів.

Значення освіти та обізнаності в області кібербезпеки не можна недооцінювати, адже людський фактор часто виявляється слабкою ланкою в системі захисту. Підвищення кваліфікації співробітників і формування в них відповідального ставлення до кібергігієни може суттєво знизити ризик успішних кібератак.

Важливою складовою є розробка та дотримання плану реагування на інциденти, що дозволяє оперативно локалізувати та усунути наслідки атак, мінімізувавши потенційні втрати. Співпраця з професійними організаціями і службами кібербезпеки надає додаткові переваги завдяки доступу до актуальної інформації про загрози та ефективні методи захисту.

Список використаних джерел

1. Буров О. Ю. Кібербезпека в мережах прийняття рішень: стан і тенденції. *Питання інтелектуальної власності* : зб. наук. пр. 2021. Вип. 18. С. 75–81.

2. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни. *Економіка та суспільство*. 2022. Вип. 44. URL: https://doi.org/10.32782/2524-0072/2022-44-21

3. Кібербезпека бізнесу під час війни. URL: https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny

Ключові слова: кіберзагрози, бізнес-середовище, заходи протидії, фішинг, безпека.
Keywords: cyber threats, business environment, countermeasures, phishing, security.

Черевко Євген Володимирович
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат фізико-математичних наук, доцент

ШТУЧНИЙ ІНТЕЛЕКТ ТА ЙОГО ЗАСТОСУВАННЯ У ФУНДАМЕНТАЛЬНИХ ДОСЛІДЖЕННЯХ

Глобальним проблемам, що виникають при застосуванні штучного інтелекта було присвячено [5]. Серед рецептів, як людству уникнути небезпеки знищення штучним інтелектом, є рекомендація доручати ШІ лише частинні задачі, бо розв'язуючи глобальну задачу, наприклад, поліпшити екологію – ШІ може дійти до очевидного висновку: щоб остаточно розв'язати проблему – треба знищити людство [1–2].

Отже, в даному випадку ми вирішили присвятити роботу ШІ саме для частинного випадку, а саме, інтегральному численню. ШІ виступав у особі відомого ChatGPT. Для початку