рах людської діяльності було виявлено, що з роками ці системи стали простим та ефективним технічним засобом для автоматизації процесу виявлення проблем та ризиків за різними сценаріями під час реалізації виробничих проєктів і допомогли організаціям досягти успіху в бізнесі, почуватися комфортно в повсякденній роботі, але на даний момент багатьом важко їх використовувати і провести інтеграцію в свою сферу діяльності досить складно, що може бути викликано страхом навчання та впровадження нових технологій. Крім переваг, про які йшлося вище, системи підтримки прийняття рішень мають певні недоліки, тому результати, представлені системою, можуть не бути на 100 % правильними.

Список використаних джерел

1. Рудніченко М., Отрадська Т., Шибаєв Д., Петров І., Полікарпов М. Розробка системи підтримки прийняття рішень для менеджера з управління ІТ-проєктами. *Інформаційні технології та суспільство*. 2021. № 2 (2). С. 50-57.

2. Бідюк П., Тимощук О., Коваленко А., Коршевнюк Л. Системи і методи підтримки прийняття рішень. 2020. № 4. С. 230-234.

Науковий керівник: доц. Чепурна О. Є.

Сопільняк Карина Олександрівна
студентка 1-го курсу судово-адміністративного факультету
Національного університету «Одеська юридична академія»

ПИТАННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ВІЙНИ

Ще з початку епідемії COVID-19 як українці, так і увесь світ були змушені приймати нові виклики, навчатися жити в новому, дистанційному форматі. Обмеження через поширення вірусу торкнулися усіх сфер життя. Співробітники багатьох підприємств, компаній, фірм були вимушені працювати поза межами офісів та своїх постійних місць роботи. Вони користувалися домашніми інтернет-мережами, підключалися з пристроїв, які, на відміну від корпоративних, не були належним чином захищені. Величезна кількість даних опинилася без належного захисту. З часом ми певним чином призвичаїлися

до нових умов користування, але з початком повномасштабного вторгнення Російської Федерації всі українські державні сайти, банківські сервіси, системи та інфраструктура зазнали величезної кількості ворожих кібератак та збоїв [1].

Почалися атаки на сайти Верховної Ради України, Кабінету Міністрів України, Міністерства закордонних справ України, Служби безпеки України, Міністерства оборони України, Міністерства України з питань реінтеграції тимчасово окупованих територій, ПриватБанку, Ощадбанку та великої кількості інших установ [2].

Сучасні форми гібридних війн демонструють залучення інформаційних атак на серйозні вірусні програми на сервери державного та транскорпораційного рівня, які серйозно підривають політичну та економічну стабільність у країні та регіоні загалом [5].

Загалом, кібератаки націлені на приховане викрадення важливої інформації, ймовірно, для надання Росії стратегічної переваги на полі бою. Все це відбувається для того, аби здійснити психологічний тиск на громадян, дестабілізувати ситуацію всередині країни, посіяти паніку та хаос, паралізувати засоби комунікації та зв'язку у державі. Такого роду атаки стали можливими лише через те, що не був забезпечений надійний та досконалий захист інформаційних ресурсів такої важливої сфери діяльності держави, як національна кібербезпека.

Саме тому, можна зробити висновок, що, оскільки Україна прагне бути повноцінним суб'єктом міжнародної політики, а не пасивним глядачем, урядом повинна бути сформована детальна стратегія щодо національної безпеки в інформаційному просторі.

Це обумовлено тим, що ефективний захист кіберпростору допоможе зменшити рівень маніпуляції з боку суб'єктів політики, а це допоможе підвищити рівень політичної культури серед політичних діячів та рівень політичної свідомості серед пересічних громадян [5].

Достатньо велика кількість дослідників та учених приділяє цьому питанню значну увагу у своїх дослідженнях. Зокрема, якщо узагальнити різні точки зору, то можна виділити певні аспекти, умови, з урахуванням яких повинна формуватися подальша державна стратегія у галузі кібербезпеки:

1. Керівництво нашої держави повинне усвідомити, що на сучасному етапі кіберпростір є не просто тлом протистоянь, а новим полем геополітичного суперництва. Відповідно, це і змушує державу на ви-

ділення значних коштів та витрати для удосконалення інформаційної безпеки.

2. Варто не очікувати на реальну заборону кібервійн на міжнародному рівні відповідними міжнародними договорами, а посилювати свій потенціал в сфері кібероборони. В цьому випадку варто навести наступний приклад зі світової історії. Якщо під час «холодної війни» СРСР та США відбувалося певне стримування, обмеження озброєння, то у галузі інформаційної оборони жодних дієвих обмежень не передбачається.

3. Необхідно переглянути наявну в Україні модель інформаційного суспільства, зокрема, звернути увагу на посилення цифрового суверенітету держави. Під цифровим (інформаційним) суверенітетом зазвичай розуміють здатність держави незалежно, самостійно забезпечувати національні інтереси у кіберсфері, самостійно розпоряджатися власними цифровими (інформаційними) ресурсами та національною інформаційною інфраструктурою. Це дозволить гарантувати інформаційну, кібернетичну безпеку як державі загалом, так і окремо кожному громадянину.

4. На законодавчому рівні у зовнішньо- та внутрішньополітичній стратегії політика держави повинна бути спрямована на більш чітке визначення подальшого розвитку кіберпростору у державі. Зокрема, сюди можна віднести комплексний огляд вітчизняного сектору кібербезпеки, прийняття Стратегії забезпечення кібернетичної безпеки України.

5. Крім того, важливим є формування загальнонаціональних структур, які будуть здатні погоджувати та координувати діяльність різних силових відомств для розслідування злочинів у кіберпросторі, та створення ефективної системи захисту вітчизняного кіберпростору (зокрема у військовій сфері).

6. Кібербезпековий простір повинен бути належним чином забезпечений ресурсами. До них можна віднести не тільки фінанси, а і матеріальне, кадрове, технічне забезпечення [6].

Крім того, надзвичайно великий вплив на формування справді захищеного інформаційного простору здійснює рівень політичної культури громадян. Саме тому важливим завданням користувачів мережі Інтернет (як суб'єктів політики, так і пересічних громадян) є дотримання нормативно-урегульованих правил користування Інтернетом [5].

Таким чином, на завершення роботи, можна зробити висновок, що з огляду на ту зовнішньополітичну загрозу, від якої наразі потерпає не лише кіберпростір нашої країни, а й усі сфери життєдіяльності громадян України, держава має приділяти більшу кількість уваги кібербезпековій сфері, зокрема визначенню та закріпленню на законодавчому рівні термінів та понять, що регулюють дану галузь.

Звісно, не можна не відмітити те, що у зв'язку із багаторічною кіберзагрозою з боку країни-агресора, український кіберпростір значно просунувся у розвитку та вже є на значно вищому рівні, аніж на початку російсько-української кібервійни, але світ розвивається у шаленому темпі, ми повинні відповідати рівню розвинутих країн і вміти себе захистити не тільки на полі бою, а і у кіберпросторі.

Список використаних джерел

1. Щодо кібератак на сайти державних органів. *Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/news/shodo-kiberatak-na-saiti-derzhavnikh-organiv
2. Щодо кібератаки на сайти військових структур та державних банків. *Офіційний веб-сайт Кабінету Міністрів України.* URL: https://www.kmu.gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-ta-derzhavnih-bankiv
3. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»: Закон України від 23.02.2006 № 3475-15. *Відомості Верховної Ради України*. 2006. № 30. Ст. 258.
4. База даних «Законодавство України». *Офіційний веб-сайт Верховної ради України*. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text
5. Закон України «Про основні засади забезпечення кібербезпеки України»: Закон від 05.10.2017 № 2163-19. *Відомості Верховної Ради.* 2017. № 45. Ст. 403.
6. Завгородня Ю. В. Кібербезпека як інноваційний захист у політичному просторі України. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* 2021. № 4 (52). URL: http://visnyk-psp.kpi.ua/article/view/248130/245405
7. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с. URL: https://niss.gov.ua/sites/default/files/2015-02/Dubov_mon-89e8e.pdf

Науковий керівник: к.політ.н., доц. Завгородня Ю. В.