ЧЕРЕП Алла Василівна,
д-р екон. наук, професор,
академік НАН ВО України,
Запорізький національний університет
ORCID ID: 0000-0001-5253-7481

ВОРОНКОВА Валентина Григорівна,
д-р філос. наук, професор,
академік НАН ВО України,
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету
ORCID ID: 0000-0002-0719-1546

НІКІТЕНКО Віталіна Олександрівна,
д-р філос. наук, професор,
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету
ORCID ID: 0000-0001-9588-7836

ЧЕРЕП Олександр Григорович,
д-р екон. наук, професор,
Запорізький національний університет
ODCID ID: 0000-0002-3098-0105
Україна

СТРАТЕГІЇ ПРОТИДІЇ КІБЕРЗАГРОЗАМ ЯК ФАКТОР ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ У ЦИФРОВУ ЕПОХУ

Стратегії протидії кіберзагрозам як фактор забезпечення стійкості національної безпеки у цифрову епоху пов'язані з трансформацією загроз цифрової та кібербезпеки і відноситься до процесу адаптації національних стратегій безпеки до сучасних викликів цифрової ери. Це означає визнання того, що загрози та вразливості в галузі кібербезпеки стають все більш важливими для національної безпеки країни. Така трансформація включає в себе розробку та впровадження стратегій, політик, законодавства та технологічних рішень, спрямованих на захист інформації, критичних інфраструктур та інших важливих об'єктів від кіберзагроз. Вона також передбачає співпрацю з іншими країнами, міжнародними організаціями та приватним сектором для обміну інформацією та спільних заходів з кібербезпеки. Ця трансформація також може включати зміни в організаційній структурі та культурі владних органів та військових структур, щоб ефективно впоратися

з новими викликами, які представляють цифрові загрози. У цьому контексті важливо розуміти, що кібербезпека стає не лише технічним питанням, але й складовою національної стратегії безпеки в цілому[1].

Цифрова безпека – це сукупність заходів, спрямованих на захист інформації, комп'ютерних систем, мереж та інших цифрових ресурсів від несанкціонованого доступу, руйнування, зміни чи втрати. Це дуже важливий аспект в сучасному світі, оскільки зростання залежності від технологій вимагає збільшення уваги до захисту цифрових даних. Заходи цифрової безпеки включають у себе широкий спектр дій, таких як використання сильних паролів, шифрування даних, застосування програмного та апаратного забезпечення для виявлення та запобігання вторгненням, а також навчання персоналу з питань безпеки. Крім того, важливо постійно оновлювати концепцію політики національної безпеки як чинник забезпечення стабільності та захисту інтересів держави з метою усунення небезек, та вразливостей.

Цифрова безпека є ключовим аспектом для захисту приватності, фінансових активів, корпоративної інформації та національної безпеки. Зростання загроз від кібератак та кіберзлочинності підкреслює необхідність надійних заходів цифрової безпеки для всіх користувачів та організацій. Крім основних заходів цифрової безпеки, існують і спеціалізовані напрямки захисту, такі як мережева безпека, захист від вірусів і шкідливих програм, кібербезпека в області IoT (інтернет речей), захист персональних даних та багато інших. З розвитком технологій зростає і складність загроз, тому цифрову безпеку важливо постійно вдосконалювати і адаптувати до нових викликів[2].

Кібербезпека концентрується на захисті від цифрових загроз, як-от злом, віруси та шахрайство, з акцентом на мережеві системи, комп'ютерне обладнання та програмне забезпечення. З іншого боку, інформаційна безпека – це ширше поняття, що охоплює захист усіх форм інформації, чи то друковані, електронні, чи то інші дані, включно з фізичною безпекою та політиками обробки інформації. Тоді як

1 Воронкова В. Г., Череп А. В., Нікітенко В. О., Череп О. Г. Політика національної безпеки як чинник забезпечення стабільності та захисту інтересів держави // Contemporary ukrainian science: theoretical and practical achievements : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2024. С. 40–55. URL : https://doi.org/10.51587/9798-9866-95952-2024-018

2 Череп А .В., Воронкова В. Г. Соціально-економічна безпека як чинник забезпечення конкурентоспроможності економіки. Методологія сучасних наукових досліджень : збірник наукових праць за результатами XIX Міжнародної науково-практичної конференції 23–24 лютого 2023 року. Харків, 2023. Вид-во Харківського національного педагогічного університету імені Г. С. Сковороди, 2023. С. 238–241.

кібербезпека фокусується переважно на технічному аспекті захисту, інформаційна безпека займається ширшим діапазоном навичок і знань. Обидва напрямки відіграють ключову роль у забезпеченні безпеки інформаційних ресурсів організації[3].

Одним з ключових напрямків в цифровій безпеці є кіберзахист, який включає в себе заходи з попередження, виявлення та реагування на кібератаки. Кіберзахист вимагає використання спеціальних технологій, таких як системи виявлення вторгнень, антивірусне програмне забезпечення, мережеві брандмауери та інші засоби, які допомагають виявляти та блокувати шкідливі дії. Для великих організацій та урядових установ важливо мати цілісну стратегію цифрової безпеки, яка охоплює всі аспекти захисту від кіберзагроз. Це включає в себе розробку політик безпеки, регулярне навчання персоналу, аудит безпеки, а також реагування на інциденти та відновлення після їхніх наслідків. Одним із важливих аспектів є також співпраця між суб'єктами цифрової безпеки, включаючи організації, урядові структури та академічні установи, для обміну інформацією про нові загрози та виявлення кращих практик в області формування стратегії кібербезпеки в умовах глобалізації[4].

Ми виокремлюємо різноманітні напрями стратегії протидії кіберзагрозам як фактор забезпечення стійкості національної безпеки у цифрову епоху:

1) Використання штучного інтелекту та машинного навчання для виявлення та аналізу поведінки загроз, розробки прогностичних моделей для передбачення інцидентів та автоматизації процесів реагування на кібератаки. Штучний інтелект може використовуватися для аналізу великих обсягів даних і виявлення аномальних патернів, які можуть свідчити про кібератаки або інші загрози. Машинне навчання допомагає адаптувати системи кібербезпеки до нових видів загроз та вчить їх розрізняти шкідливу діяльність від нормального трафіку[5].

3 Кібербезпека: актуальні загрози та методи захисту. URL : https://lemon.school/blog/kiberbezpeka-aktualni-zagrozy-ta-metody-zahystu

4 Воронкова В. Г. Формування концепції стратегії кібербезпеки в умовах глобалізації: економічні засади // Scientific trends: modern challenges. Volume 1 : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2021. С.46–60. URL : https://doi.org/10.51587/9781-7364-13302-2021-004-46-60

5 Cherep A.V., Voronkova V.H. Bekhter L.A., Cherep O.H., Lyshchenko E.G. (2023). Minimization of information secutiry risks amid the challenges of digital society // Artificial intelligence: an era of new threats or opportunities? monograph. Edited by Irina Tatomyr, Liubov Kvasnii. Praha: Oktan print, 260 p. P. 190–201. URL : https://doi.org/10.46489/aiaeont-23-23

2) Блокчейн використовується для створення розподілених та недійсних журналів транзакцій, що робить їх майже неможливими до зміни або втручання. Це може забезпечити безпеку даних та транзакцій у різних областях, включаючи фінансові транзакції та обмін даними між користувачами. Використання блокчейну для забезпечення надійності та цілісності даних, а також для створення розподілених систем ідентифікації та автентифікації[6].
3) Розробка заходів безпеки для мобільних пристроїв, застосунків та мобільних мереж, включаючи захист від шкідливих додатків, зловмисного коду та атак на мобільні пристрої. З ростом популярності мобільних пристроїв і додатків, кіберзлочинці також активно використовують їх для здійснення атак. Заходи безпеки мобільних пристроїв включають в себе захист від вірусів, шифрування даних, аутентифікацію користувачів та контроль доступу до даних.
4) Розробка квантових криптографічних алгоритмів та систем шифрування, які стійкі до атак з використанням квантових комп'ютерів. Квантова криптографія використовує принципи квантової механіки для забезпечення безпеки комунікаційних каналів і шифрування даних. Це дозволяє створювати криптографічні системи, які залишаються стійкими навіть в умовах квантового обчислення.
5) Забезпечення безпеки для хмарних інфраструктур та послуг, включаючи захист від витоку даних, атак на віртуалізацію та інші загрози, що виникають в хмарних середовищах. Хмарні сервіси надають доступ до даних і обчислювальних ресурсів через мережу Інтернету, тому заходи безпеки для них включають в себе шифрування даних в покої, автентифікацію користувачів та контроль доступу.
6) Розробка стандартів та протоколів безпеки для підключених пристроїв, захист від атак на IoT мережі та застосунки, а також забезпечення конфіденційності та цілісності даних, що збираються та оброблюються IoT пристроями. Збільшення кількості підключених

6 Воронкова В.Г., Череп А.В., Череп О.Г. Концепція блокчейн-економіки як економіки нового типу в умовах цифровізації // Modern scientific strategies of development". Modern scientific strategies of development : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2022. 349 p. P. 54–61. URL : https://doi.org/10.51587/9781-7364-13395-2022-008-54-61

пристроїв створює нові вектори атак для кіберзлочинців. Кібербезпека в області IoT включає в себе захист від атак на підключені пристрої, захист від витоку конфіденційної інформації та захист мережі IoT від зловмисних атак[7].

Ці напрями представляють лише деякі з важливих аспектів розвитку цифрової безпеки, які постійно еволюціонують у відповідь на зростаючі загрози та виклики в сфері кібербезпеки. я даних в покої, автентифікацію користувачів та контроль доступу. Ці напрями є лише кількома з багатьох аспектів цифрової безпеки, які постійно розвиваються і адаптуються до зростаючих загроз та нових технологічних викликів[8].

Цифрова безпека та кібербезпека стали надзвичайно важливими аспектами національної безпеки в сучасному технологічному ландшафті. З розвитком інформаційних технологій і швидким поширенням цифрових систем з'явилися нові загрози, які можуть торкнутися як державні структури, так і приватний сектор. Однією з основних загроз є кібератаки, які можуть бути спрямовані на різноманітні об'єкти: від урядових систем до фінансових установ і навіть критично важливих інфраструктур, таких як електростанції або транспортні мережі. Ці атаки можуть мати серйозні наслідки, включаючи втрату конфіденційної інформації, фінансові втрати, порушення роботи систем і навіть загрозу життю людей[9].

Для забезпечення національної безпеки у цифровому середовищі необхідно вживати комплексних заходів, включаючи наступні стратегії: 1) Кіберзахист, в основі якого розробка і впровадження технічних та організаційних заходів для захисту інформаційних систем від несанкціонованого доступу, вірусів, вторгнень та інших кіберзагроз. 2) Моніторинг і реагування, що включає постійний моніторинг кіберпростору для виявлення потенційних загроз і швидке реагування на них для запобігання або мінімізації збитків. 3) Співпраця між

7 Мар'єнко В. Ю. Безпека даних в епоху великих даних як стратегічний ресурс країни. Стратегічні пріоритети розвитку підприємництва, торгівлі та біржової діяльності: матеріали IV-ої Міжнародної науково-практичної конференції, 10-11 травня 2023 року / За заг. редак. проф. А. М. Ткаченко Запоріжжя : НУ «Запорізька політехніка», 2023. С. 76–80.

8 Кивлюк О. П., Воронкова В. Г. Філософська рефлексія інформаційної безпеки у цифровому середовищі: проблеми, ризики, правове забезпечення. // Innovative resources of modern science : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2022. P.160–172. URL : https://www.eo.kiev.ua/resources/zmist/mono9/Monograph_9-160-172.pdf

9 Череп А., Воронкова В., Андрюкайтене Р., Денисенко М. (2023). Соціально-економічна безпека у контексті міжнародного економічного клімату задля забезпечення конкурентоспроможності економіки. *Acta Academia Beregsasiensis. Economics*. V. 3. 2023. P. 172–179. URL : https://doi.org/10.58423/2786-6742/2023-3-172-179

секторами, між урядовими органами, приватним сектором і академічною громадськістю для обміну інформацією про потенційні загрози та розробки спільних стратегій захисту. 4) Навчання та освіта, що включає підвищення рівня обізнаності індивідів та організацій щодо кібербезпеки шляхом навчання та проведення освітніх кампаній. 5) Законодавчі заходи, що включають прийняття відповідного законодавства для регулювання діяльності в кіберпросторі і покарання тих, хто порушує ці правила. Усі ці заходи спільно сприяють створенню стійкого та надійного цифрового середовища, що є важливою складовою національної безпеки в сучасному світі[10].

Взаємодія та взаємовплив між різними аспектами цифрової безпеки та кібербезпеки в сучасному технологічному ландшафті національної безпеки дуже глибока і складна. Розвиток нових технологій може створювати як можливості для покращення безпеки, так і нові загрози. Наприклад, використання шифрування та біометричних методів аутентифікації може підвищити безпеку, але водночас розвиток квантових комп'ютерів може загрожувати стійкості сучасних шифрів[11]. Кібератаки та інші кіберзагрози можуть впливати на ефективність заходів з цифрової безпеки. Виявлення нових загроз та розробка заходів протидії їм часто відбувається через взаємодію між урядовими органами, приватним сектором та академічною громадськістю. Кібератаки можуть мати серйозний вплив на економіку країни, зокрема на фінансову стійкість, конфіденційність бізнес-даних та споживчу довіру. Заходи з покращення кібербезпеки можуть сприяти збереженню економічного процвітання[12].

Кібербезпека – це широке поняття, яке охоплює різноманітні концепції, стратегії та методи, спрямовані на захист комп'ютерних систем, мереж і даних від кіберзагроз.

Ключові концепції кібербезпеки у контексті стратегій протидії кіберзагрозам у цифрову епоху: 1) Захист інформації включає в себе

10 Кивлюк О. П., Воронкова В. Г. Філософська рефлексія інформаційної безпеки у цифровому середовищі: проблеми, ризики, правове забезпечення. // Innovative resources of modern science: collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2022. P. 160–172. URL : https://www.eo.kiev.ua/resources/zmist/mono9/Monograph_9-160-172.pdf

11 Воронкова В. Г., Нікітенко В. О. Кібергеополітика як важлива сфера геополітичних відносин цифрової ери. Соціокультурні засади економіки і політики: взаємо- зв'язки, тренди, суперечності: тези доп. Всеукр. наук.-практ. конф. (Київ, 16 листоп. 2023 р.) / відп. ред. Н. В. Крохмаль. Київ : Держ. торг.-екон. ун-т, 2023. С. 220–224. URL : https://doi.org/10.31617/k.knute.2023-11-16

12 Там само.

заходи, спрямовані на захист конфіденційності, цілісності і доступності інформації. 2) Ідентифікація і аутентифікація – контроль доступу до систем та даних за допомогою методів ідентифікації користувачів (логінів, паролів, біометричних даних тощо). 3) Мережева безпека – захист мережевої інфраструктури від несанкціонованого доступу, атак і перехоплення даних. 4) Кіберзахист програмного забезпечення – виявлення, запобігання та виправлення вразливостей програмного забезпечення, які можуть бути використані для атак. 5) Інцидентні реагування та відновлення - системи та процедури, спрямовані на реагування на кіберінциденти, відновлення роботи після атак і відновлення пошкоджених даних. 6) Шифрування даних – використання алгоритмів шифрування для захисту конфіденційної інформації від несанкціонованого доступу. 7) Соціальна інженерія і освіта користувачів – заходи для підвищення свідомості користувачів про кіберзагрози та практики безпеки в Інтернеті для запобігання атакам, пов'язаним із соціальною інженерією. 8) Моніторинг і аналіз загроз – системи, які виявляють, аналізують і реагують на потенційні кіберзагрози шляхом використання різноманітних даних і алгоритмів. 9) Інформаційна безпека у Інтернеті речей (IoT) – захист вбудованих систем та пристроїв, які з'єднані з Інтернетом, від кіберзагроз. 10) Хмарна безпека – захист даних, додатків та інфраструктури, що знаходяться в хмарних сервісах.

Ці концепції використовуються в різних комбінаціях залежно від потреб і контексту організації чи користувача, які прагнуть забезпечити безпеку своєї інформації та інфраструктури[13].

Кібератаки можуть бути використані для впливу на політичну ситуацію в країні або в світі в цілому. Це може означати спроби вплинути на вибори, маніпулювати громадською думкою або підірвати авторитет уряду. Кібербезпека тісно пов'язана з національною обороною. Критично важливі інфраструктури, такі як енергетика, транспорт та оборонні системи, можуть стати об'єктами кібератак, що ставить під загрозу національну безпеку. Цифрова безпека та кібербезпека в сучасному технологічному ландшафті національної безпеки взаємодіють і взаємовпливають на багато рівнів, і успішне керування цими аспектами вимагає комплексного та координованого підходу.

13 Воронкова В. Г. Глобальні політико-правові проблеми в умовах невизначеності та непередбачуваності. Соціально-гуманітарні виміри правової держави : матеріали Міжнародної науково-практичної конференції (м. Дніпро, 27 жовтня 2022 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2022. С. 58–63.

Це може включати різні види кібернетичних нападів, такі як вторгнення в комп'ютерні системи урядових установ, політичних партій, а також маніпулювання інформацією в мережі для впливу на громадську думку і рішення політичних лідерів. Наприклад, кібератаки можуть включати в себе хакерські вторгнення в системи голосування або електронні системи підрахунку голосів під час виборів, щоб змінити результати голосування або порушити довіру до виборчого процесу. Також можуть проводитися кібератаки з метою викриття конфіденційної інформації про політичних діячів або державні таємниці з метою шантажу або дискредитації. Ці кібератаки можуть мати серйозні наслідки для політичної стабільності та безпеки країн і навіть змінювати геополітичний ландшафт, тому що вони можуть створити хаос і посилити людську безпеку як чинник людського розвитку та досягнення прогресу[14].

Стратегія захисту суспільства та особистості у протидії кіберзлочинності

Ми живемо у взаємопов'язаному світі, у якому всі ми є уразливими, так як кіберзлочинність заполонила ін формаційний простір[15]. Злочинці розробили цілий арсенал методів для отримання прибутків, надавши перевагу цифровому інтелекту перед людським, і опинилися осередками між реальністю і цифровими даними, що контролюються шахраями, у результаті чого виникла загальна загроза достовірності інформації та її втрати, яка накопичується під час «революції великих даних». Взаємопов'язаність та повсюдність уразливих за своєю суттю комп'ю терних систем свідчить про те, що ураган технологічної небезпеки, що насувається, більше не можна ігнорувати[16].

Розвиток транснаціональної організованої кіберзлочинності. Транснаціональна організована злочинність – це сьогодні величезний бізнес,

14 Череп А. В., Нікітенко В. О., Воронкова В. Г. Становлення і розвиток концепції людської безпеки як чинник людського розвитку та досягнення прогресу. Соціально-гуманітарні виміри правової держави : матеріали Міжнародної науково-практичної конференції (м. Дніпро, 14 квітня 2023 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2023. С. 103–107.

15 Воронкова В. Г. Напрями захисту суспільства та особистості у протидії кібезлочинності. Матеріали конференції «Публічне управління у цифровому суспільстві» 25 червня 2020 року / Аспекти публічного управління. Спеціальний випуск 1. Дніпро: Дніпропетровський регіональний інститут державного управління Національної академії державного управління. 2020. Т. 8. С.25–27. URL : www.aspects.org.ua https://aspects.org.ua/index.php/journal/article/view/750

16 Voronkova V., Nikitenko V., Metelenko N. AGILE-economy as a factor in improving the digital society. *Baltic Journal of Economic Studies*. Riga, Latvia : "Baltija Publishing", 2022. Vol. 8, N. 2. P. 51–58.

який заробляє 2 трильйони доларів на рік: гроші надходять від торгівлі наркотиками, крадіжок інтелектуальної власності, торгівлі людьми, дитячої порнографії, викрадення особистих даних, кіберзлочинності, руху людей та кон трабандних товарів, отримання доступу до приватних облікових записів поштового сервісу Gmail, доступу до системи паролів, яка дозволяла користувачам входити у низку служб Google і успішно зламувати базу даних по всьому світу, які вважалися найвпливовішими компаніями епохи Інтернету. «Ця система була найважливішим об'єктом інтелектуальної власності, яку розробники вважали «коштовним каменем у короні» вихідних кодів компанії»[17].

Компанія неодноразово опинялася під прицілом спритних хакерських компаній, у результаті чого хакери ще у 2010 році викрали текст програми для системи управління паролями, яка дозволяла користувачам одночасно заходити у різні додатки Google. Крадіжка викликала паніку серед вищого керівництва Google – компанії, яка пишається власною системою безпеки користувачів та їхніх персональних даних і яка вибудувала собі репутацію, гарантуючи цю безпеку. Агентство проводить політику купівлі інформації про вразливості і платить за це найвищу ціну, а також проводить наступальні кібероперації, що можуть нанести ураження кібероперація м.

Як вважають експерти даного питання, до створення кіберармії підштовхують масштабні шпигунські операції, спрямовані проти оборонних підприємств. Загалом, організована злочинність, яка формує сучасні корпоративні структури, створює від 15 до 20% світового ВВП[18]. Локальні кримінальні мережі та угрупування, що швидко збираються і підлаштовуються, щоб використати будь-які незаконні можливості і канали для своєї незаконної діяльності, добре структуровані та саморегулюються, створюють клірингові центри (по- середників, фінансових організацій, що пропонують різноманітні послуги із взаєморозрахунків), гарантують незаконні продукти або викрадену інформацію. Злочинні корпорації мають онлайн-підручники з усіх найважливіших питань та навичок: від проблем з подоланням фаєрволів до клонування кредитних карток. Злочинці-початківці мають доступ до створених корпораціями онлайн-курсів, де вони навчаються запускати компанії з «фішингу», поширювати

17 Шейн Г. Війн@ : битви в кіберпросторі. Київ : Ніка-Центр; Львів: Видавництво Анетти Антоненко, 2019. С. 199.
18 Гудмен, М. Злочини майбутнього. Харків: Фабула, 2019.

спам, а також користуватися заготівками для створення шкідливого програмного забезпечення, засвоюючи «ремесло» цифрової злочинності та кібер шахрайства.

У кіберпідпільному світі створені своєрідні «вікіпедії», що містять докладні посилання, розбиті за категоріями – як зламувати всі наявні пристрої, програмне забезпечення та операційні системи. Кіберзлочинці є набагато потужнішими і далекогляднішими, є більш успішнішими і технологічно підготовленішими кримінальними командами, які забезпечують себе високими прибутками за відносно малих ризиків. Судові розслідування кіберзлочинів є надзвичайно рідкісними, тому що вироки за ними складають менше тисячної частки відсотка серед усіх кримінальних покарань, які продовжують здійснювати агресивні кібероперації, спрямовані на викрадення інформації, причому найактивніше хакерські контратаки здійснюються у банківській сфері.

Розквіт організованої кіберзлочинності. Розквіт організованої кіберзлочинності - це тема, яка вимагає уваги та заходів для протидії. Організовані злочинні групи використовують інформаційні технології для вчинення різноманітних злочинів, включаючи крадіжку даних, шахрайство, фінансові маніпуляції та інші види кіберзлочинності. Для протидії цьому явищу потрібна співпраця між правоохоронними органами, урядовими установами, приватними компаніями та громадськістю. Важливо розвивати технологічні та правові засоби для виявлення, запобігання та розслідування кіберзлочинності. Також важливо підвищувати рівень свідомості серед користувачів Інтернету про загрози кібербезпеки та заходи їх уникнення[19].

Кримінальні підприємства створюють власні структури, завжди користуються власною юрисдикцією офшорних зон або країн із слабким управлінням, нестабільними політичними режимами, які за певну плату ладні закривати очі на нелегальну діяльність кримінальних структур. У межах цих злочинних синдикатів існують відділи праці та управління поставками, керівники відділів, зовнішні консультанти та команди виконавців. Хакери вдосконалюють та демонструють власну майстерність у використанні технологій, продовжуючи постійний пошук нових можливостей, кількість кіберзлочинів зростає, у той час

19 Звіт CROWDSTRIKE 2024 : аналіз глобальних кіберзагроз. URL : https://iitd.com.ua/news/zvit-crowdstrike-2024-analiz-globalnih-kiberzagroz-ta-strategii-zahistu/

як компанії не мають технічного ресурсу, щоб захистити себе. Існує ринок для кібернайманців, які розробляють і продають шпигунське ПЗ і хакерські інструменти, що не поступаються державним розробкам США кількарічної давності. Шпигунська програма учасників кіберпідпілля, здатна контролювати комп'ютер, копіювати файли та записувати кожне слово, набране користувачем, замаскована під оновлення популярного застосунку iTunes.

Технологічні інновації, що виходять з підпільного світу, процвітають, а «колективний злочинний інтелект» упевнено бере гору над антивірусними компаніями, продавцями технологій безпеки та правоохоронними органами. Наприклад, уряди можуть встановлювати строгі закони та санкції проти кіберзлочинців, сприяти обміну інформацією між країнами для спільного розслідування кіберзлочинності та підтримувати програми навчання та підвищення кваліфікації фахівців з кібербезпеки. Приватні компанії також мають велику відповідальність у забезпеченні кібербезпеки. Вони можуть інвестувати у технології захисту, вдосконалювати свої системи безпеки та робити регулярні аудити для виявлення слабких місць у своїх мережах. Нарешті, громадськість може бути важливим інструментом у протидії кіберзлочинності. Популяризація знань про безпеку в Інтернеті, вчасне повідомлення про підозрілу діяльність та участь у програмах спільного спостереження можуть сприяти виявленню та припиненню кіберзлочинності[20].

Збитки від програмного забезпечення

Збитки від програмного забезпечення можуть бути значними як окремих користувачів, так і організацій. Ось деякі з найпоширеніших видів збитків: 1) Втрата даних, так як неправильно спроектоване або неналежно використовуване програмне забезпечення може призвести до втрати важливих даних. Це може бути через помилки в програмному коді, атаки зловмисників або некоректну роботу системи. 2) Витрати на відновлення, в основі яких втрата даних або виникнення інших проблем через програмне забезпечення , що може призвести до необхідності проведення робіт з відновлення, що може бути дуже витратним.

20 Гайдук О., Звєрєв В. Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. 3 (23), 225–236. URL : https://doi.org/10.28925/2663-4023.2024.23.225236

3) Збої в роботі бізнесу: якщо бізнес покладається на програмне забезпечення для свого функціонування, будь-які збої або проблеми з цим програмним забезпеченням можуть призвести до припинення роботи і втрати прибутку. 4) Порушення безпеки: вразливості в програмному забезпеченні можуть бути використані зловмисниками для викрадення даних, введення в організаційні мережі або інших злочинних дій, що може призвести до фінансових втрат і втрати довіри клієнтів. 5) Витрати на оновлення та підтримку, так як деяке програмне забезпечення може вимагати постійних витрат на оновлення та підтримку, особливо якщо його виробник припиняє підтримку старих версій. 6) Штрафи та судові витрати: якщо організація порушує законодавство через використання неліцензійного або піратського програмного забезпечення, вона може стати об'єктом штрафів або судових позовів.

Організації та користувачі повинні приділяти увагу якості та безпеці програмного забезпечення, а також підтримці та оновленню для зменшення ризику виникнення таких збитків.Сьогодні, коли ми стикаємося з фактом поганого стану світового програмного забезпечення, програмісти говорять, немає ідеального програмного забезпечення, оскільки воно буде зламане, яким би воно не було, а користувачі прагнуть мати потужне багато- функціональне програмне забезпечення, визначаючи безпеку пріоритетом і ключовим компонентом надійних обчислень. Ця проблема зростає у міру того, що все більше і більше пристроїв починають спілкуватись один з одним і всі помилки у ПЗ та дефекти безпеки мають кумулятивний характер в контексті глобальної інформаційної мережі і саме через це 75% комп'ютерних систем можуть бути зламані за лічені хвилини.

Враховуючи, що ПЗ керує глобальною економікою та усіма критичними інфраструктурами, – від електрики до телефонних мереж, - ми не маємо права гаяти час. Ми маємо допомогти компаніям зрозуміти, що, з огляду на довгострокову перспективу, в їхніх інтересах створювати більш безпечне і стабільне ПЗ, необхідне для нашого технологічного майбутнього і що відмова робити це матиме для них важкі наслідки, тому необхідне правове регулювання нашої глобальної кібербезпеки[21].

21 Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. Підприємництво, господарство і право. 2017. Вип. 5. С. 174–180.

Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України

Національна система кібербезпеки в Україні відіграє важливу роль у забезпеченні національної безпеки країни в умовах сучасних кіберзагроз. Вона складається з різноманітних елементів, які спільно працюють для захисту інформаційних та кіберних ресурсів країни від потенційних загроз[22]. Основні складові національної системи кібербезпеки України включають:

1) Стратегічне управління, в основі якого розробка та впровадження стратегічних документів, таких як національна стратегія кібербезпеки, що визначає основні напрями дій у сфері кібербезпеки на рівні держави.
2) Нормативно-правове забезпечення, в основі якого прийняття та впровадження законів, нормативних актів та стандартів, які регулюють сферу кібербезпеки та встановлюють відповідальність за порушення кіберзаконодавства.
3) Технічні засоби захисту, що включають розробку та впровадження технічних рішень для захисту інформаційних систем від кіберзагроз, таких як системи виявлення та запобігання вторгнень, антивірусні програми, фаєрволи тощо.
4) Інцидентні реагування та реагування в кризових ситуаціях, що включає створення механізмів реагування на кіберінциденти та кризові ситуації, включаючи створення національних центрів кібербезпеки, розвиток процедур співпраці з приватним сектором та міжнародними партнерами.
5) Співпраця з іншими країнами та міжнародними організаціями, Україна активно співпрацює з іншими країнами та міжнародними організаціями у сфері кібербезпеки для обміну інформацією, проведення спільних навчань та розробки міжнародних стандартів у цій галузі.
6) Свідомість та освіта, в основі якої залучення громадськості та підвищення рівня освіти про кібербезпеку, зокрема шляхом проведення інформаційно-просвітницьких заходів, навчання та тренінгів.

22 Про «План реалізації Стратегії кібербезпеки України». URL : https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

Ці складові спільно формують національну систему кібербезпеки, яка має на меті забезпечення стійкості інформаційного простору України та захист національних інтересів в кіберпросторі[23].

Через усвідомлення і визнання цих загроз, що несуть технології для всього людства, слід започаткувати зміни, необхідні для зміцнення фундаменту нашого технологічного майбутнього. Необхідно посилення державного контролю у сфері кіберзлочинності, рівень активності якої зростає у мережах, та компаніям необхідно підвищувати стандарти безпеки й гарантувати кібербезпеку. Якими б складними не були технології чи інтернет-сервіси, учасники цифрового підпілля вже напоготові, щоб на власний розсуд використати новомодні засоби та орієнтуватися перш за все на гроші за рахунок більш масштабних, але точно вивірених крадіжок, здатних кинути виклики владі та йти на порушення правил та законів, створюючи зловмисне програмне забезпечення, прагнучи стимулювати інновації та створювати нові напрямки злочинного бізнесу, розробляючи нові види кіберафер, тому держава повинна запобігти хакерським атакам, щоб створити перепони для них.

Держава повинна розробити різноманітні технічні, організаційні, освітні рекомендації щодо державної політики, спрямованої на зменшення ризиків, пов'язаних з технологіями, як застосовувати ті чи інші інструменти для отримання максимально можливої користі при мінімізації негативних наслідків, і тільки так ми зможемо витримати випробування прогресом[24].

Для сучасного суспільства й економіки довіра до кіберпростору вкрай важлива, оскільки загроз сьогодні збільшилося, хакери щодня викрадають дані, а держава не в змозі їх захистити, тоді як компанії не мають технічного ресурсу, щоб самостійно захиститися. Сьогодні необхідне посилення державного контролю у сфері захисту суспільства та особистості у протидії кіберзлочинності, щоб спонукати підвищити стандарти безпеки й гарантувати посилення кібероборони та запобігання атакам на критично важливі об'єкти державної інфраструктури. Держава повинна сформувати ефективну концепцію національної безпеки,

23 6 трендів кібербезпеки в 2024 році. URL : https://wezom.com.ua/ua/blog/6-trendiv-kiberbezpeki-v-2024-rotsi

24 Єдині стандарти кібербезпеки: Міноборони зміцнює захист інформаційних систем. URL: https://armyinform.com.ua/2024/04/21/yedyni-standarty-kiberbezpeky-minoborony-zmicznyuye-zahyst-informaczijnyh-system/

оприлюднювати інформацію про хакерів і посилювати контроль, щоб захисти тися від хакерських злочинних атак[25].

Практичні аспекти цифрової безпеки та кібербезпеки

Цифрова безпека охоплює заходи та політики, спрямовані на захист комп'ютерних систем, мереж і даних від зловмисників. Кібербезпека займається захистом інформаційних систем від кіберзагроз, таких як хакерство, кібершпигунство, кібертероризм. Для мінімізації ризиків у Європі в 2018 році набрали чинності закони про захист даних. Вони передбачають різке підвищення штрафів за розголошення або втрату персональних даних, що змусить компанії вже в цьому році переглянути свої підходи і стандарти щодо забезпечення інформаційної та кібернетичної безпеки, в тому числі ввести окрему посаду відповідального за захист інформації та кібернетичну безпеку. Масові відключення електроенергії, телефонного зв'язку та Інтернету, труднощі з обслуговуванням клієнтів і проведенням банківських операцій, реальні фінансові збитки — це те, що використовує ворог. Використовуючи кіберпростір, хакери можуть зламати захищені мережі та отримати необхідну інформацію, тому ми мусимо спрямувати зусилля на захист своїх мереж і забезпечити їх безпеку, використовуючи різні рівні захисту інформації. Висновок, який ми повинні зробити для себе, - це збільшення інвестування в кібербезпеку, щоб запобігати атакам на великі державні й приватні компанії і протистояти намірам дестабілізувати суспільство [26].

Великі порушення безпеки можуть призвести до втрати конфіденційної інформації, фінансових збитків, порушення приватності та навіть загрози для національної безпеки. Заходи безпеки включають у себе встановлення міцних паролів, використання антивірусного програмного забезпечення, регулярні оновлення програмного забезпечення тощо. Уряди розробляють кіберстратегії для захисту національних інтересів в кіберпросторі, включаючи захист критично важливих інфраструктур. Кібербезпека стає глобальною проблемою, тому міжнародне співробітництво в цій сфері є ключовим для

25 Кібербезпека як важлива складова всієї системи захисту держави. URL: https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html

26 Про основні засади забезпечення кібербезпеки України URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

ефективного захисту від загроз. Розуміння і впровадження цих аспектів допоможе забезпечити національну безпеку в умовах сучасного цифрового середовища[27].

Практичні аспекти цифрової безпеки та кібербезпеки полягають в тому, що вони впливають на безпеку держави, бізнесу та громадян. Вони включають: 1) Захист інформаційних систем уряду та критично важливої інфраструктури, в основі якої забезпечення безпеки державних систем і критично важливих інфраструктур, таких як енергетика, транспорт, банківська система, є важливим завданням для уряду. Це включає в себе розробку та впровадження технологічних заходів безпеки, регулярні аудити безпеки та планування реагування на інциденти. 2) Захист бізнесу, так як підприємства, організації, установи також повинні приділяти значну увагу кібербезпеці, оскільки вони також стають мішенню для кібератак. Захист корпоративних мереж, даних клієнтів і фінансових операцій є критичним для забезпечення стабільності та успішності бізнесу в умовах глобального управління[28]. 3) Захист особистої інформації громадян, так як у світі, де особиста інформація зберігається і обробляється в онлайн-середовищі, захист персональних даних громадян є надзвичайно важливим.

Це стосується як державних програм збирання інформації, так і приватних компаній, що опрацьовують особисті дані, вивчаючи технології інформаційного забезпечення менеджменту[29]. 4) Протидія кіберзлочинності, в основі якої відслідковування, викриття та переслідування кіберзлочинців, що є ключовими аспектами забезпечення кібербезпеки. Це вимагає співпраці між правоохоронними органами, міжнародної співпраці та розвитку спеціалізованих технологічних засобів для виявлення та відповіді на кіберзлочинність. 5) Забезпечення безпеки в Інтернеті для громадян, так як підвищення освіти та навичок в галузі кібербезпеки серед громадян може допомогти у запобіганні кібератак, шахрайства та інших форм кіберзлочинності. Також важливою є роль уряду та громадських організацій у підтримки для збільшення кібербезпеки серед

27 Кібербезпека – це важливо в сучасному світі. URL : https://foxminded.ua/kiberbezpeka-tse/

28 Воронкова В. Г., Нікітенко В. О. Концепція глобального управління: характеристика та напрями розвитку. Соціально-гуманітарні виміри правової держави: матеріали Міжнародної науково-практичної конференції (м. Дніпро, 14 квітня 2023 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2023. С. 113–118.

29 Воронкова В. Г. Технології інформаційного менеджменту в державному управлінні. Вісник Національного університету цивільного захисту України : зб. наук. пр. Харків : Вид-во НУЦЗУ, 2021. Вип. 2 (15). С.70–79. URL : http://vdu-nuczu.net/ua/8-ukr/141-vipusk-2-15-2021

громадян і оптимізації фінансової безпеки промислового підприємства в епоху цифровізації.

Важливо аналізувати сучасні тенденції в кіберпросторі та ідентифікувати потенційні загрози для національної безпеки. Це може включати кібератаки на державні установи, критичну інфраструктуру, а також кібершпигунство та кібертероризм. Національні уряди повинні розробляти та впроваджувати стратегії і політики з кібербезпеки, які охоплюють всі сфери суспільства, включаючи державні установи, приватний сектор та громадян. Ці стратегії повинні бути гнучкими та реагувати на змінюючіся умови у кіберпросторі. Національні уряди повинні активно захищати критичну інфраструктуру від кібератак, оскільки її порушення може мати серйозні наслідки для економіки, безпеки та життєвого середовища. Кіберзагрози часто перетинають національні кордони, тому міжнародне співробітництво в цій сфері набуває великого значення.

Держави повинні співпрацювати у сфері обміну інформацією, розробки міжнародних стандартів та норм, а також спільних заходів з кібербезпеки. Важливо підвищувати рівень освіти та свідомості серед громадян щодо кібербезпеки. Це може включати навчання кібергігієни, безпеки в Інтернеті та виявлення шахрайства. Загалом, трансформація загроз цифрової та кібербезпеки в рамках національної безпеки вимагає комплексного підходу, який об'єднує технологічні, політичні, організаційні та освітні заходи[30].

Стратегії протидії кіберзагрозам як фактор забезпечення стійкості національної безпеки у цифрову епоху, коли інформаційні технології стають невід'ємною частиною нашого повсякденного життя. Назвемо деякі ключові аспекти, які варто враховувати: 1) Використовувати унікальні та складні паролі для кожного облікового запису, а також активувати двофакторну аутентифікацію, де це можливо. Це ускладнює життя хакерам. 2) Регулярно оновлювати всі програми та операційну систему на вашому пристрої. Виробники постійно випускають патчі для закриття вразливостей. 3) Встановити надійний антивірусний захист на всі свої пристрої та регулярно сканувати їх на наявність загроз. 4) Захищати свою домашню мережу за допомогою паролів для

30 ТОП-9 трендів кібербезпеки у 2024 році: як захистити свій веб-сайт від зловмисників? URL : https://web-promo.ua/ua/blog/top-9-trendiv-kiberbezpeki-u-2024-roci-yak-zahistiti-svij-veb-sajt-vid-zlovmisnikiv/

Wi-Fi, обмеженням доступу до пристроїв, використанням захищеного протоколу шифрування. 5) Навчити себе та інших членів родини про основні правила цифрової безпеки, наприклад, уникання небезпечних веб-сайтів та поштових вкладень, розпізнавання фішингових атак. 6) Регулярно створювати резервні копії важливих даних та зберігати їх в захищеному місці. Це допоможе відновити важливу інформацію в разі її втрати через кібератаку або несправність пристрою. 7) Регулярно перевіряти свої фінансові виписки та операції, щоб вчасно виявити можливі аномалії або шахрайські дії. 8) Уникати надання особистої інформації в ненадійних джерелах, таких як сумнівні веб-сайти або недостовірні електронні повідомлення. 9) Налаштувати свої соціальні медіа та інші онлайн-профілі на рівень приватності, щоб обмежити доступ сторонніх осіб до вашої особистої інформації. Ці практичні заходи допоможуть забезпечити безпеку інформації та захистити від кіберзагроз.

Стратегії протидії кіберзагрозам як фактор забезпечення стійкості національної безпеки у цифрову епоху мають важливе практичне значення в сучасному світі, оскільки цифрові технології стають все більш важливим елементом суспільства, економіки та політики[31]. Тож відтепер усі системи, сервіси, застосунки та цифрові інструменти відомства матимуть єдині правила кібербезпеки. В Міноборони кажуть, що вони враховуватимуть найкращі підходи НАТО та міжнародні стандарти. Для багатьох країн цифрова і кібербезпека стають однією з найважливіших складових національної безпеки через наступні причини: 1) Економічна безпека: злочинці та зловмисники можуть використовувати кібератаки для крадіжок, шахрайства, викрадень грошей та конфіденційної інформації.

Це може призвести до значних економічних втрат для країни. 2) Політична безпека: кібератаки можуть бути спрямовані на вплив на політичний процес, включаючи втручання в виборчі кампанії, маніпулювання голосуванням або розповсюдження дезінформації з метою підриву демократичних інститутів. 3) Військова безпека: кібератаки можуть бути використані для ведення кібервійни, включаючи напади на важливі військові системи, комунікаційні

31 Міноборони України переходить на єдині правила кібербезпеки. URL : https://espreso.tv/viyna-z-rosiyeyu-minoboroni-ukraini-perekhodit-na-edini-pravila-kiberbezpeki

мережі та інфраструктуру. 4) Загрози критичній інфраструктурі: критична інфраструктура, така як енергетичні системи, транспорт, медичні системи тощо, може бути піддається кібератакам, що може призвести до серйозних наслідків для безпеки і добробуту населення. 5) Конфіденційність та приватність: порушення конфіденційності та приватності в Інтернеті може мати серйозні наслідки для індивідуальних громадян та суспільства в цілому[32]. У зв'язку з цим, ефективне управління цифровою та кібербезпекою стає критично важливим завданням для кожної країни з метою забезпечення національної безпеки та захисту інтересів держави, суспільства, громадян.

Стратегії протидії кіберзагрозам як фактор забезпечення стійкості національної безпеки у цифрову епоху є важливим аспектом національної безпеки в цифрову епоху, тому що швидкість розвитку технологій та поширення цифрових засобів зв'язку зробили кіберпростір критичною сферою, яка потребує постійного вдосконалення заходів забезпечення безпеки. До цифрової інфраструктури входять енергетичні системи, фінансові установи, транспортні мережі, медичні заклади та інші сектори, які є критичними для нормального функціонування суспільства. Захист цих систем від кібератак та інших загроз є найважливішим завданням для забезпечення національної безпеки. Потрібно постійно вдосконалювати технології та методи захисту від кіберзагроз. Це включає в себе розробку механізмів виявлення, відповіді та відновлення після кібератак. Національна безпека потребує кваліфікованих кадрів у сфері кібербезпеки. Держави мають розвивати системи освіти та навчання, щоб забезпечити наявність спеціалістів, які здатні ефективно протистояти кіберзагрозам. Захист персональних даних та приватності користувачів є важливим аспектом національної безпеки, оскільки їх уразливість може бути використана для кібератак або інших зловмисних дій. Таким чином, стратегії протидії кіберзагрозам як фактор забезпечення стійкості національної безпеки у цифрову епоху вимагають комплексного підходу, який охоплює технологічні, правові, організаційні та міжнародні аспекти.

DOI: 10.51587/9798-9895-14649-2024-118-56-74

32 Кібератаки 2022–2023 : огляд найбільших інцидентів, та що нас чекає у 2024 році. URL : https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua