УДК 004.056:343.9
DOI https://doi.org/10.32782/2521-6643-2024-2-68.11

Рибальченко Л. В., кандидат економічних наук доцент,
доцент кафедри кібербезпеки та інформаційних технологій
Університету митної справи та фінансів
ORCID: 0000-0003-0413-8296

Габорець О. А., доктор філософії, доцент кафедри
оперативно-розшукової діяльності та інформаційної безпеки
факультету № 3 Донецького державного університету
внутрішніх справ
ORCID: 0000-0001-7791-6795

Прокопович-Ткаченко Д. І., завідувач кафедри кібербезпеки
та інформаційних технологій
Університету митної справи та фінансів
ORCID: 0000-0002-6590-3898

КІБЕРСТІЙКІСТЬ: ГЛОБАЛЬНІ ЗАГРОЗИ ТА НАЦІОНАЛЬНІ СТРАТЕГІЇ КІБЕРЗАХИСТУ

Стаття присвячена питанням захисту підприємств, установ та організацій від кіберзлочинності, яка створює глобальні загрози для національної безпеки. Розглядаються особливості застосування ефективних методів управління ризиками, проведення ретельного аналізу потенційних загроз та здійснення моніторингу рівня кібербезпеки.

Широке застосування інформаційних технологій призводить до численних злочинів та виникнення нових видів загроз, які ґрунтуються на використанні різних засобів, методів та елементів впливу на свідомість людини. Формування єдиного глобального інформаційного простору дало можливість кожній людині отримати доступ до інформації з різних частин світу.

Доведено, що дистанційне керування бізнесом, управління власними активами, проведення транзакції, спричиняє для злочинців нові засоби втручання до персональних даних громадян з метою їх заволодіння.

Метою статті є дослідження глобального інформаційного простору, який став безмежним місцем та інструментом для злочинів. Інформаційно-комунікаційні системи стали основним знаряддям злочину.

Досліджено, що застосування незаконних технічних засобів, створення вірусів, спамів, фішингових атак та інших засобів, дали кіберзлочинцям можливість отримати доступ до конфіденційної інформації, баз даних, інформації з обмеженим доступом, платіжних карток, банківських рахунків та автоматизованих систем управління із метою викрадення та заволодіння даними призводить до прояву різних форм шахрайства.

Доведено, що крадіжка персональних даних та комерційної інформації з метою заволодіння коштами клієнтів банку, навмисне пошкодження і псування інформаційних систем та комунікацій є невеликим переліком зловмисний дій сучасних шахраїв, які призводять до збитків підприємства, установи, організації та громадян.

З'ясовано, що застосування різних атак на інтернет-ресурси із використанням сучасних інформаційних технологій, які стрімко розвиваються, стали підґрунтям для кіберзлочинців щодо нанесення шкоди та збитків критичній інфраструктурі країни.

Встановлено, що в умовах війни кількість кіберзлочинів зросла в рази і здійснюється для дестабілізації держави, нанесення збитків, виведення з ладу обладнання, техніки та технологій, зв'язку та комунікацій. Хакерські атаки здатні здійснити контроль над особистими даними, базами даних великих підприємств та установ, стати загрозою для витоку даних та пошкодження мережі.

Ключові слова: *кібератаки, шахраї, критична інфраструктура, інформаційні технології, спами.*

Rybalchenko L. V., Haborets O. A., Prokopovych-Tkachenko D. I., Cyber resilience: global threats and national cyber defense strategies

The widespread use of information technologies leads to numerous crimes and the emergence of new types of threats based on the use of various means, methods and elements of influence on human consciousness. The formation of a single global information space has enabled everyone to access information from different parts of the world.

Remote management of business, management of personal assets, conducting transactions, provides criminals with new means of interfering with personal data of citizens in order to obtain them.

The purpose of the article is to study the global information space, which has become a limitless place and tool for crime. Information and communication systems have become the main instrument of crime.

The use of illegal technical means, creation of viruses, spam, phishing attacks and other means have enabled cybercriminals to gain access to confidential information, databases, restricted information, payment cards, bank accounts and automated management systems in order to steal and take possession of data, resulting in various forms of fraud.

The theft of personal data and commercial information to seize the funds of bank customers, deliberate damage and corruption of information systems and communications is a small list of malicious actions of modern fraudsters that cause losses to enterprises, institutions, organizations and individuals.

The use of various attacks on Internet resources with the help of rapidly developing modern information technologies has become the basis for cybercriminals to cause damage and losses to the country's critical infrastructure.

It has been established that in times of war, the number of cybercrimes has increased many times and is being committed to destabilize the state, cause damage, disable equipment, technology, communications and communications. Hacker attacks can gain control over personal data, databases of large enterprises and institutions, and become a threat to data leakage and network damage.

Key words: *cyberattacks, fraudsters, critical infrastructure, information technology, spam.*

Постановка проблеми. Кібербезпека є однією з ключових складових інформаційної безпеки, яка спрямована на захист конфіденційності, цілісності та доступності даних у цифровому середовищі. Однак, злочинність у кіберпросторі значно впливає на ефективність реалізації основних принципів кібербезпеки. До ключових принципів кібербезпеки, на які впливають злочинні дії, можна віднести:

Злочинні дії, такі як крадіжка персональних або корпоративних даних, безпосередньо підривають принцип конфіденційності. Атаки типу фішинг або зловмисне використання вразливостей у програмному забезпеченні призводять до несанкціонованого доступу до чутливої інформації, що є порушенням цього принципу. Наприклад, атаки на бази даних із персональною інформацією користувачів загрожують конфіденційності, оскільки отримана інформація може бути використана для подальших злочинних дій або продана на чорному ринку.

Злочинність у кіберпросторі може суттєво вплинути на цілісність даних шляхом їх модифікації або пошкодження. Зловмисники часто змінюють або маніпулюють даними з метою викривлення фактів, що особливо небезпечно у фінансовій сфері або при роботі з державними документами. Атаки, спрямовані на порушення цілісності даних, можуть бути пов'язані з використанням шкідливих програм або програмних помилок, що дозволяють змінювати інформацію без відома користувача.

Атаки типу DDoS (Distributed Denial of Service) є типовим прикладом злочинних дій, що спрямовані на порушення доступності інформаційних ресурсів. Внаслідок таких атак легітимні користувачі втрачають доступ до необхідних сервісів або систем. Злочинці також можуть використовувати програми-вимагачі (ransomware), які блокують доступ до систем або даних до моменту сплати викупу.

Злочинні дії, такі як використання вкрадених облікових даних або маніпуляції з системами багатофакторної аутентифікації, можуть призвести до порушення принципу аутентифікації. Несанкціонований доступ до облікових записів користувачів з використанням вкрадених паролів або компрометація інших методів аутентифікації, таких як біометричні дані, стає все більш поширеним явищем у контексті кіберзлочинності.

Здатність до відстежування дій у системі є ключовою для виявлення та протидії злочинності у кіберпросторі. Проте кіберзлочинці використовують складні методи приховування своїх дій, такі як анонімізація трафіку, використання шифрування та інших технологій, що ускладнюють ідентифікацію нападників і подальшу відповідальність за їхні дії.

Стан дослідження. Згідно даним World Economic Forum [1], глобальна вартість кіберзлочинів прогнозується на рівні 23,84 трлн доларів США до 2027 року, що свідчить про значне зростання з 8,44 трлн у 2022 році. Така динаміка пов'язана із зростанням використання інтернету для особистих та бізнес-операцій, що робить кіберпростір більш уразливим для атак. У 2023 році кількість кібератак сягнула понад 800 000 на рік.

Візуалізація різних аспектів кіберзлочинності у 2023 році представлена на рисунку 1, де фішингові атаки мають найбільший вплив і становлять 45%, програми-вимагачі – 30%, DDoS-атаки – 15% та 10% – інші кіберзагрози.

Стрімке зростання кількості кіберзагроз за 2020-2023 рр. характеризує глобальну небезпеку (рис. 2) для кожної країни світу та населення.

Вплив кібератак на різні галузі економіки у 2023 році вказує на те, що такі сектори економіки, як виробництво, сільське господарство, банківська діяльність та страхування, найбільше постраждали від кібератак (рис. 3).

Ці діаграми демонструють поточні тенденції та вплив кіберзлочинності на глобальну економіку і небезпеку.

Таким чином, злочинність у кіберпросторі має суттєвий вплив на основні принципи кібербезпеки, створюючи нові виклики для забезпечення надійного захисту інформаційних систем. Реагування на ці виклики потребує постійного вдосконалення технологій захисту, підвищення обізнаності користувачів та розвитку міжнародної співпраці у сфері кібербезпеки.

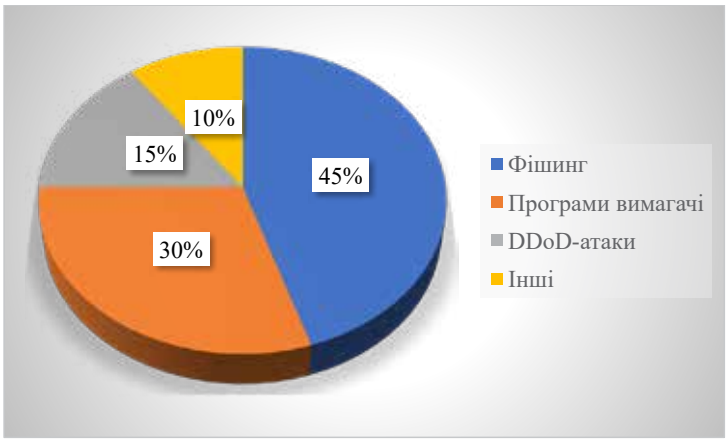

Рис. 1. Поширеність основних кіберзагроз у 2023 році

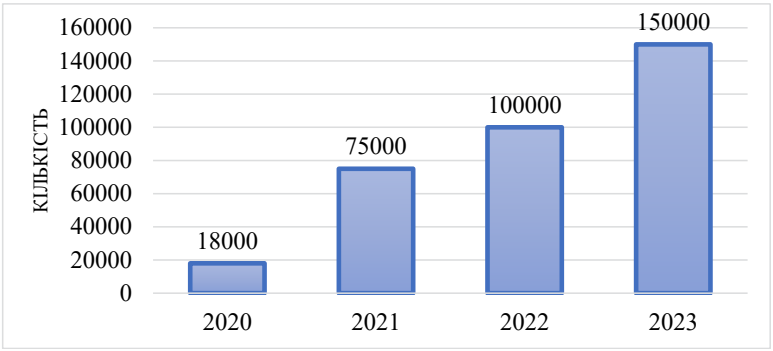

Рис. 2. Кількість кібератак у 2020-2023 роках.

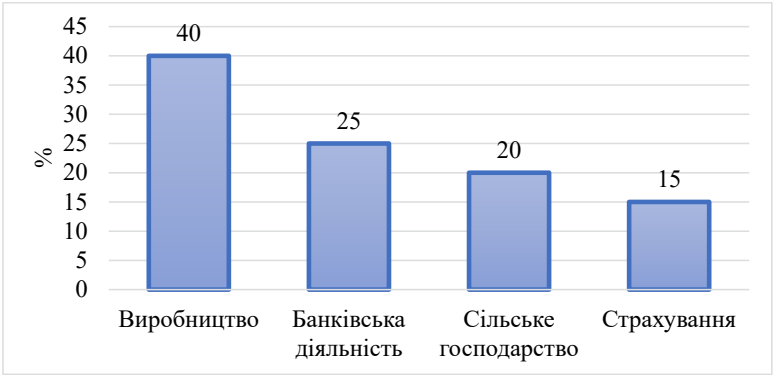

Рис. 3. Вплив кібератак на галузі економіки у 2023 році.

Метою статті є дослідження глобального інформаційного простору, який став безмежним місцем та інструментом для злочинів.

Виклад основного матеріалу. Кіберзлочинність на глобальному рівні демонструє стійку тенденцію до експоненційного зростання, при цьому її форми стають дедалі різноманітнішими, що створює суттєві загрози як для фізичних осіб, так і для підприємницьких структур та національної безпеки в цілому. Активне впровадження інформаційних технологій безпосередньо сприяє ескалації кіберзлочинів, які проникли у всі ключові сфери суспільного життя та економічної діяльності.

Багаточисленні збройні конфлікти та війни, що тривають у різних частинах світу, забезпечили ідеальні умови для розгортання технологічних війн у кіберпросторі. Зокрема, війна в Україні стала тестовим полігоном для апробації різноманітних типів кіберзлочинів, спрямованих на підрив інформаційного суверенітету держави та дестабілізацію її економічних секторів, таких як фінансовий, виробничо-промисловий та енергетичний.

Кожна держава реалізує власні стратегії щодо запобігання, нейтралізації та протидії різноманітним кіберзагрозам, використовуючи диференційовані методи та тактики кіберзахисту. У цьому контексті розробка інтегрованих підходів, гармонізованих методологій і нормативно-правових актів для зміцнення резильєнтності інформаційного простору є ключовим завданням для формування національної кіберстійкості. Це включає подолання негативних наслідків, спричинених кібератаками, що використовують складні інформаційно-комунікаційні технології.

Сфера підприємництва також стикається з ескалацією кіберризиків, що здатні призвести до значних втрат через витоки інформації, зокрема унаслідок таких загроз, як соціальна інженерія, кібершантаж, деструктивні кібератаки та порушення конфіденційності персональних і комерційних даних. Це безпосередньо впливає на зниження операційної ефективності бізнесу та скорочення прибутковості.

Зростання зусиль у протидії потенційним негативним наслідкам кіберзагроз варіюється залежно від рівня фінансових інвестицій, необхідних для впровадження передових рішень у сфері кібербезпеки, а також від підготовки висококваліфікованих спеціалістів у галузі інформаційної безпеки. Підготовка таких фахівців, включно з їх безперервною освітою та адаптацією до швидко мінливого технологічного середовища, є критично важливою для забезпечення надійної кіберзахищеності.

Близько 52% організацій заявляють про відсутність ресурсів та навичок для боротьби із кібершахрайством.

Фішинг, шкідливе програмне забезпечення, спам, шкідливі повідомлення та інші загрози є одними з найпоширеніших інструментів, які кіберзлочинці використовують для здійснення атак на підприємства. Окрім цих методів, зростає кількість атак із використанням програм-вимагачів (ransomware), які блокують доступ до даних та вимагають викуп за їхнє відновлення. Також поширеними стають DDoS-атаки, що спричиняють перевантаження серверів або систем компаній, порушуючи їхнє нормальне функціонування. Не менш небезпечними є атаки на ланцюги постачань, коли кіберзлочинці вражають систему постачальників чи партнерів з метою отримання доступу до цільових компаній. Особливу загрозу також становлять атаки, які використовують вразливості типу «zero-day», коли зловмисники експлуатують недоліки в програмному забезпеченні, які ще не були виявлені або усунені, що значно ускладнює захист від таких атак.

Великі підприємства в усьому світі показали значні успіхи щодо захисту своєї кіберстійкості у 2023 році, а малі підприємства значне зниження кіберстійкості на 30% у порівнянні із 2022 роком.

Кількість організацій, які постраждали від кіберзагроз за 2022 рік, становить 41%. Саме в цих організаціях загроза була спричинена третьою стороною. У 54% організацій загроза виникла через неперевірених та ненадійних партнерів і постачальників.

Керівники 64% організацій вважають, що кіберстійкість їх організації відповідає вимогам щодо захисту.

У 60% організацій, в яких керівники застосували заходи щодо упередження кіберзловживань через впровадження конфіденційності інформації, нормативно-правових актів, впровадження відеоспостережень, призвело до зниження ризиків на 21% у порівнянні з 2022 роком.

Аналітики стверджують, що впровадження новітніх технологій, таких як штучний інтелект (ШІ), значно підвищить кіберстійкість підприємств завдяки автоматизації процесів виявлення та реагування на кіберзагрози. ШІ здатен аналізувати великі обсяги даних у реальному часі, ідентифікуючи аномальні дії або поведінкові патерни, які можуть свідчити про кібератаки. Використання алгоритмів машинного навчання дозволяє не лише швидше реагувати на існуючі загрози, але й прогнозувати потенційні уразливості до того, як вони будуть використані зловмисниками. Це дає можливість підприємствам не лише захищати свої мережі від відомих атак, але й адаптуватися до нових загроз у міру їхнього виникнення, що робить захист більш ефективним і проактивним. Із стрімким освоєнням інформаційних технологій, громадськість, суспільство та організації, найчастіше застосовують принципи безпеки та захисту для своїх гаджетів, планшетів, комп'ютерів та даних.

Нові технології зараз широко використовуються для захисту інформації від кіберінцидентів, ніж і раніше. Галузі, які найчастіше потерпали від кіберзагроз, а саме промисловість (65%), сільське господарство (63%), банківська справа (56%) і страхування (56%), інформаційні технології та телекомунікації (52%), у 2023 році були найбільшими лідерами, які використали технологію штучного інтелекту для боротьби із кібервикликами.

В умовах розвитку кібербезпеки, боротьбі із економічними злочинами, виникає питання щодо попиту талановитих, висококваліфікованих кадрів щодо роботи у сфері кібербезпеки. Брак професіоналів та фахівців стає найчастіше питанням керівників для створення надійного захисту та кіберстійкості організації.

У 2022 році 6% керівників повідомили, що їм не вистачає фахівців для реагування на кіберінциденти, а у 2023 році, вже 12% керівників повідомили, що їм не вистачає таких фахівців. Що вказує на зростання загроз та викликів.

За попередніми опитуваннями керівників організацій щодо впливу кібератак на їх подальшу діяльність, необхідно зазначити, що керівники більше турбуються про збої в роботі після кібератак (39,5%), потім про фінансові втрати (36,05%), репутацію своєї організації (18,6%) і лише 5,81% на контроль регулятора їх діяльності (рис. 4).

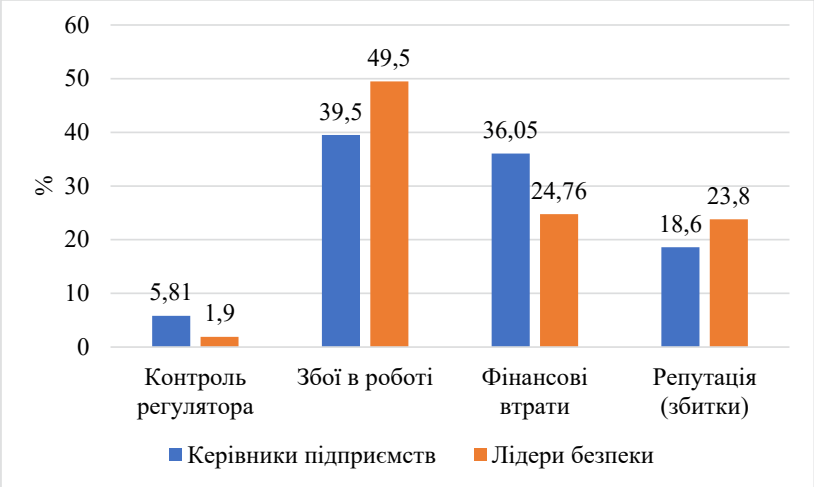

Рис. 4. Вплив кібератак на діяльність організації

Майже 50% кіберлідерів увагу приділяють нестійкості в роботі після кібератак, потім про фінансові втрати (24,76%), репутації організації (23,8%) і лише 1,9% контролю регулятора їх діяльності (рис. 4).

Для лідерів безпеки перешкодами для кіберстійкості в організаціях є прогалини в навичках (32%), є вартість щодо змін застарілих процесів (29%) та несприйняття змін серед керівників чи працівників (25%) (рис. 5).

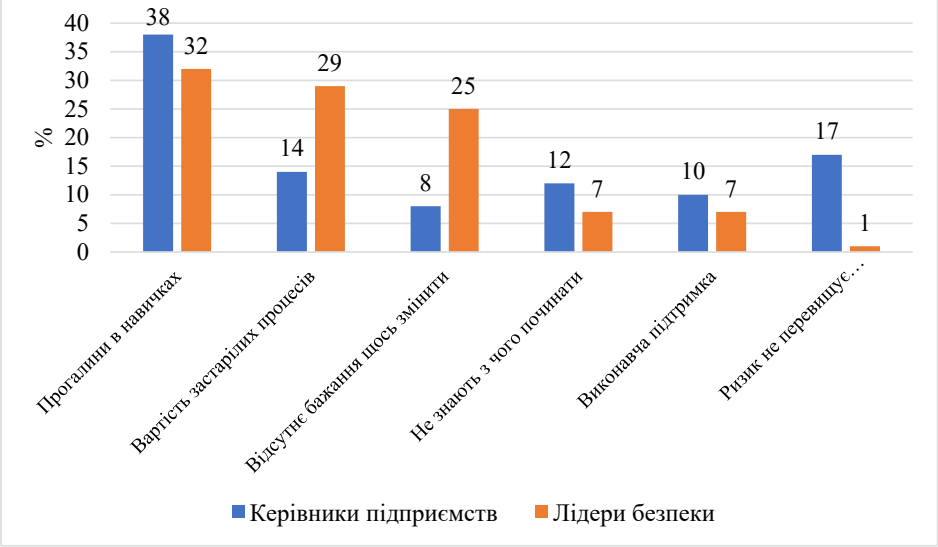

Рис. 5. Вплив кібератак на діяльність організації

Для керівників підприємств ключовими викликами залишаються прогалини у навичках та вартість модернізації застарілих процесів, що відображено у значних показниках – 38% і 32% відповідно. Це свідчить про те, що підприємства часто зіштовхуються з дефіцитом кваліфікованих кадрів, які можуть ефективно впроваджувати сучасні технологічні рішення для підвищення кіберстійкості. Натомість лідери безпеки також зазначають ці проблеми, але значно менше акцентують увагу на вартості процесів (14%) порівняно з прогалинами у навичках (32%).

Відсутність бажання до змін та невизначеність у тому, з чого починати, залишаються основними перешкодами для багатьох організацій, особливо коли йдеться про впровадження нових технологій. Це особливо проявляється серед лідерів безпеки, де 25% відзначають відсутність бажання змінювати процеси, тоді як серед керівників підприємств цей показник складає лише 8%. Така різниця може свідчити про те, що безпекові структури більш обережні у впровадженні змін, оскільки це може вплинути на їхню кіберстійкість.

Водночас впровадження штучного інтелекту посилює розрив між тими організаціями, які активно використовують новітні технології, і тими, хто не встигає за цими змінами. Повільна модернізація або

відсутність оновлення застарілих інформаційних систем призводить до зростання ризиків, що відображено у даних графіку, де 17% керівників підприємств бачать проблему у тому, що ризик не виправдовує інвестиційні витрати. Однак лідери безпеки оцінюють цей фактор значно нижче, лише на рівні 1%, що може свідчити про їхню більшу готовність до інвестицій в оновлення технологій.

Питаннями національного рівня є визначення кіберзагроз, заходів та можливостей кібербезпеки, розробка основних показників кібербезпеки, їх дослідження за певними ознаками та створення відповідних груп показників кібербезпеки для аналізу та розробки заходів щодо їх уникнення. Метою проведення такого дослідження є сприяння глобальній культурі кібербезпеки та поліпшення сфери захисту в усьому світі [3]. Забезпечення кібербезпеки можливо тільки за рахунок комплексного і безперервного застосування організаційно-правових та технічних методів захисту на різних рівнях реалізації [4].

Для формування безпечного інформаційного простору на національному рівні, спрямованого на мінімізацію кіберризиків, необхідно впроваджувати комплексні механізми та інструменти управління кібербезпекою. Ці механізми мають забезпечувати виявлення, ідентифікацію, оцінку та запобігання ризикам, що загрожують інформаційним системам, шляхом створення проактивних заходів захисту. Важливою складовою цього процесу є не лише технічний захист, але й стратегічне управління ризиками, що включає в себе ретельний аналіз потенційних загроз, розробку критеріїв оцінювання ефективності захисту, а також визначення ключових показників, за якими здійснюється моніторинг рівня кібербезпеки.

У сучасних умовах стрімкого зростання кіберзагроз для всіх секторів економіки стає очевидною необхідність значного посилення заходів з кібербезпеки в Україні. Це включає розробку стратегічних рішень, які забезпечать не лише кіберстійкість окремих підприємств, але й загальну стійкість бізнес-середовища. Особливої уваги потребують компанії, які надають послуги з безпеки, оскільки вони стають першою лінією оборони у випадку кібератак. Багато керівників організацій визнають, що інтеграція кіберстійкості в бізнес-стратегію є необхідним елементом для забезпечення довгострокової конкурентоспроможності та захисту від зростаючих ризиків у цифровому середовищі.

Розвиток цифрових технологій, попри їхні численні переваги, водночас створює нові можливості для злочинної діяльності, що загрожує глобальній безпеці. Сучасні технологічні досягнення надають злочинцям інструменти для проведення більш складних і масштабних кібератак, що впливають на критичну інфраструктуру, фінансові системи та державні установи.

Це особливо актуально для країн, які вже піддаються агресивним кібератакам, таких як Україна. У таких умовах, вирішення технічних, організаційних та правових питань кібербезпеки, стає критично важливим. Країни мають розробляти нові стратегії для посилення своєї кіберстійкості, включаючи впровадження ефективних технологічних рішень, удосконалення правових норм і регулювань, а також формування міцних організаційних структур, здатних протистояти постійно зростаючим загрозам у цифровому просторі.

Для забезпечення більш комплексного підходу до кіберстійкості необхідно зосередитися на розвитку інноваційних рішень у сфері кібербезпеки, що дозволить підвищити рівень захищеності інформаційних систем на всіх рівнях управління. Це передбачає не лише інвестування в новітні технології, але й створення ефективної системи підготовки кадрів, здатних оперативно реагувати на нові виклики та кіберзагрози [6].

Крім того, важливою складовою кіберстійкості є створення гнучкої регуляторної бази, яка б адекватно реагувала на сучасні виклики. Це включає вдосконалення законодавства у сфері захисту даних, відповідальності за кіберзлочини та регулювання використання новітніх технологій, таких як штучний інтелект і блокчейн. Важливо, щоб правові механізми відповідали сучасним тенденціям розвитку технологій і забезпечували захист не тільки державних, але й приватних підприємств та громадян.

Не менш важливим є міжнародне співробітництво, оскільки кібератаки рідко обмежуються національними кордонами. Спільні зусилля на глобальному рівні, включаючи обмін інформацією між державами та міжнародними організаціями, дозволять більш ефективно протистояти загрозам, що з’являються у цифровому просторі. Інтернаціоналізація зусиль з кіберзахисту стає ключовою у боротьбі з кіберзлочинністю, оскільки лише тісна співпраця дозволить своєчасно виявляти та блокувати загрози на глобальному рівні.

Висновки. Таким чином, з урахуванням усіх аспектів, кіберстійкість має стати не просто питанням технічних рішень, але й загальнонаціональною стратегією, яка передбачатиме залучення різних секторів – від урядових структур до приватних компаній та освітніх установ. Створення спільної екосистеми кібербезпеки дозволить не лише знизити рівень загроз, але й сприяти стійкому розвитку цифрової економіки та забезпеченню стабільного функціонування всіх інституцій в умовах постійно змінюваного кіберпростору.

Окремо необхідно підкреслити важливість освіти в сфері кібербезпеки. Підготовка ІТ-фахівців високого рівня та організація навчальних програм для керівників і співробітників підприємств з питань захисту інформаційних систем, є одним із пріоритетних завдань. Тільки таким чином можна гарантувати, що підприємства будуть підготовлені до зустрічі з новими викликами та загрозами, що виникають у цифровому середовищі.

Список використаних джерел:

1. World Economic Forum. Global Cybersecurity Outlook 2024. Insight Report January 2024. Режим доступу: URL: https://weforum.org

2. Rubalchenko L., Kosychenko O. Features of latency of economic crimes in Ukraine. Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. 2019. Special Issue № 1 (102). – p. 264-267. https://doi.org/ 10.31733/2078-3566-2019-5-264-268

3. Рибальченко Л.В. Кіберзлочинність в глобальному просторі. Науковий вісник Дніпропетровського державного університету внутрішніх справ. – 2022. – Спеціальний випуск № 2 (121). – С. 524-530. https:// doi.org/ 10.31733/2078-3566-2022-6-524-530

4. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посіб. – Дніпро: ДДУВС, 2020. – 144 с. https://scholar.google.com.ua/citations?user=WCRn9eAAAAAJ&hl=ru&oi=sra

5. Rybalchenko L.V., Kosychenko O.O., Klinitskyi I.I. Ensuring economic security of enterprises taking into account the peculiarities of information security. Philosophy, Economics and Law Review. Volume 2, no. 1, 2022 p. 96-107. https://doi.org/10.31733/2786-491X-2022-1-96-107

6. Haborets O. Ensuring cybersecurity of Ukraine against cyberterrorism threats: a systematic approach. Scientific innovations and advanced technologies. Issue № 11(25) 2023. p. 197–205. https:// doi.org/10.52058/2786-5274-2023-11(25)-197-205

References:

1. World Economic Forum. Global Cybersecurity Outlook 2024. Insight Report January 2024. Access mode: URL: https://weforum.org

2. Rubalchenko L., Kosychenko O. (2019). Features of latency of economic crimes in Ukraine. Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. Special Issue № 1 (102). – p.264-267. https:// doi.org/10.31733/2078-3566-2019-5-264-268

3. Rybalchenko L. (2022). Cybercrime in the global space / L. Rybalchenko // Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. – Special Issue № 2 (121). – C. 524-530. https:// doi.org/10.31733/2078-3566-2022-6-524-530

4. Hrebenyuk A.M., & Rybalchenko L.V. (2020). Fundamentals of information security management: training. manual. [Osnovy upravlinnya informatsiynoyu bezpekoyu: navch. posibnyk]. Dnipro: DDUVS, – 144 c. https://scholar.google.com.ua/citations?user=WCRn9eAAAAAJ&hl=ru&oi=sra. [in Ukrainian]

5. Rybalchenko L.V., Kosychenko O.O., Klinitskyi I.I. (2022). Ensuring economic security of enterprises taking into account the peculiarities of information security. Philosophy, Economics and Law Review. Volume 2, no. 1, p. 96-107. https://doi.org/10.31733/2786-491X-2022-1-96-107

6. Haborets O. (2023). Ensuring cybersecurity of Ukraine against cyberterrorism threats: a systematic approach. Scientific innovations and advanced technologies. Issue № 11(25). p. 197–205. https:// doi.org/10.52058/2786-5274-2023-11(25)-197-205