https://doi.org/10.36818/1562-0905-2025-1-10
УДК 330.526.3:005.934:004.4(477)
JEL E23, L86, H56

О. М. Правдивець

Сучасні цифрові інструменти кібербезпеки в системі економічної безпеки підприємств України

Виділено основні класи сучасних цифрових інструментів кібербезпеки, описано їхні можливості та значення для підвищення загальної стійкості цифрової інфраструктури підприємства. Обґрунтовано необхідність комплексного впровадження цифрових інструментів кібербезпеки. Проаналізовано ціни та якість деяких цифрових продуктів кібербезпеки. Оцінено, які продукти найбільш ефективні з точки зору витрат і які вигоди вони забезпечують для підприємств різного масштабу. Результати аналізу узагальнено за трьома критеріями: висока якість, висока ціна; висока якість, помірна ціна; добра якість, низька ціна. За результатами дослідження встановлено, що використання сучасних цифрових інструментів кібербезпеки є необхідною умовою для підтримання стійкості та безпеки підприємств в умовах цифровізації економіки. Ці інструменти надають ефективні рішення для виявлення та попередження загроз, а також для захисту інформаційних ресурсів від можливих атак. Наголошується важливість як інтеграції та впровадження таких інструментів у систему економічної безпеки підприємств, ураховуючи специфіку діяльності кожного підприємства, так і постійного розвитку й оновлення інструментів кібербезпеки з огляду на нові виклики та загрози в сучасному кіберпросторі.
Ключові слова: кібербезпека, цифрові інструменти, економічна безпека, підприємство, захист цифрової інфраструктури.

Формулювання проблеми. Сучасний глобалізований світ активно розвивається в новій парадигмі інформаційного суспільства. У світі, де глобальний кіберпростір відіграє значущу роль у житті, підвищення кібербезпеки є істотною складовою забезпечення інформаційної безпеки, економічного розвитку та національної безпеки [1].

Економічні умови та зміни у світовому технологічному ландшафті змушують підприємства України запроваджувати сучасні цифрові інструменти для забезпечення своєї кібербезпеки. Як зазначено у [2], останнім часом інноваційний розвиток систем економічної безпеки сучасних українських підприємств характеризується активним застосуванням цифрових технологій.

Захист цифрової інфраструктури підприємств є ключовим елементом їхньої загальної системи економічної безпеки, оскільки кіберзагрози можуть мати катастрофічні наслідки для фінансової стабільності, репутації та конкурентоспроможності бізнесу. На підтвердження цього президент Інституту майбутнього Р. Шпітц зазначив, що важливість кібербезпеки тепер повинна бути на рівні національної безпеки [3].

Водночас інтеграція цифрових технологій у бізнес-процеси українських підприємств призводить до зростання залежності їх від інформаційних систем, що своєю чергою підвищує їхню вразливість до атак кіберзлочинців, зокрема під час довготривалої збройної агресії російської федерації проти України. Це підтверджується тим, що за останні роки збільшилася кількість інцидентів, пов'язаних з витоком даних, шкідливим програмним забезпеченням і фішинговими атаками. Такі виклики вимагають від підприємств використання сучасних підходів і технологій для запобігання, виявлення та реагування на кіберзагрози.

Актуальність теми обумовлена необхідністю створення ефективної системи кіберзахисту на підприємствах України, яка використовувала б

сучасні інструменти та методи протидії новітнім кіберзагрозам. Зважаючи на цифровізацію та цифрову трансформацію економіки, підприємства стикаються з необхідністю захисту не лише своїх внутрішніх інформаційних систем, а й зовнішніх зв'язків, що охоплюють партнерів, постачальників і клієнтів. Тому впровадження сучасних цифрових інструментів кібербезпеки в системи економічної безпеки підприємств України є критично важливим для підтримання стабільності та розвитку бізнесу в умовах дедалі більших кіберзагроз.

Дослідження в цій сфері спрямовані на вирішення ключових завдань: ідентифікацію найбільш ефективних інструментів кіберзахисту, адаптацію їх до специфіки діяльності підприємств різних галузей, а також розроблення стратегій інтеграції їх у загальну систему економічної безпеки.

Автор статті зосереджується на аналізі та класифікації сучасних цифрових інструментів кібербезпеки, їхньої ролі в протидії кіберзагрозам та підвищенні стійкості цифрової інфраструктури підприємств України.

Аналіз останніх досліджень. У сучасній науковій літературі значну увагу приділено дослідженню кіберзагроз і засобів нейтралізації цих небезпек. Зокрема, провідні українські вчені, такі як О. Барановський, І. Чумаченко та В. Костюк, зосереджені на вивченні теоретичних аспектів захисту інформаційних систем і розробленні практичних рекомендацій для підвищення кіберстійкості підприємств. В їхніх дослідженнях аналізується вплив різних типів атак на економічну стабільність організацій та пропонуються інструменти для виявлення атак і запобігання їм.

З-поміж зарубіжних досліджень заслуговують на увагу роботи Д. Шнайєра, який вивчає методи криптографічного захисту, а також Е. Спітцера, який зосереджується на питаннях штучного інтелекту в кібербезпеці. Дослідження Дж. Тіптона, який займається оцінюванням ризиків і побудовою стратегій кіберзахисту, є важливими для розуміння глобальних тенденцій у цій сфері.

Важливу роль відіграють публікації, присвячені автоматизації процесів кіберзахисту. Наприклад, сучасні роботи в галузі використання технологій машинного навчання для виявлення аномальної активності в мережах надають нові можливості для підвищення ефективності систем захисту. Дослідження у сфері інтеграції штучного інтелекту, зокрема роботи П. Дусселя та І. Мартінеса, підтверджують доцільність використання їх для створення адаптивних систем кіберзахисту.

Крім того, особливий інтерес становлять наукові праці, присвячені питанням управління ризиками у сфері кібербезпеки. Зокрема, В. Кондратюк пропонує методологію оцінювання ризиків, яка враховує специфіку діяльності підприємств різних галузей. Із зарубіжних дослідників це питання активно вивчають Р. Гуупта та М. Андерсон, які пропонують інструменти для прогнозування кіберзагроз і запобігання їм.

Проте, попри значну кількість наукових досліджень, залишається низка невирішених проблем. Недостатня увага приділяється результатам практичного застосування різних цифрових інструментів кібербезпеки та інтеграції їх в єдину систему економічної безпеки підприємств, яка враховувала б специфіку конкретного підприємства, а також відсутність комплексного підходу до оцінювання ефективності застосування таких інструментів. Це підкреслює необхідність подальших досліджень у зазначеній сфері.

Метою статті є аналіз сучасних цифрових інструментів кібербезпеки, що застосовуються в системі економічної безпеки підприємств України під час збройної агресії російської федерації.

Основні результати дослідження. Тривала збройна агресія російської федерації проти України закріпила твердження про те, що сучасні війни, війни XXI сторіччя є високотехнологічними. Щобільше, сучасні війни охоплюють не тільки традиційні сфери збройної боротьби, а й поступово просуваються у

віртуальний комп'ютерний світ – кіберпростір, який практично є основою життя сучасної людини [4]. Не стала винятком і збройна агресія російської федерації проти України. Про це директор Інституту прикладних досліджень кібербезпеки професор С. Дж. Шекелфорд зазначив: «Урок війни полягає в тому, що давно перевірених стандартів та стратегій кібербезпеки виявилося недостатньо для стримування амбіцій Володимира Путіна, який розв'язав кібервійну паралельно з конвенціональною» [5]. Деякі її прояви змогли зачепити чимало підприємств України, наприклад вірус «Petya.A», кібератаки на українські енергетичні компанії, компанію «Київстар» і на державні реєстри Міністерства юстиції України наприкінці 2024 р.

Аналіз активності в кіберпросторі показує, що з початком повномасштабного вторгнення зафіксовано збільшення кількості кібератак, а наслідки роботи російських хакерів відчув на собі кожен українець. Почалося все ще в січні 2022 р., коли через масовану кібератаку було виведено з ладу одразу 15 сайтів державних органів.

У грудні 2023 р. росіянам удалося на два дні вимкнути мобільного оператора «Київстар». Без зв'язку залишилася половина країни, а сама компанія отримала збитки на мільярди гривень.

За даними швейцарського CyberPeace Institute, із січня 2022 р. по грудень 2023 р. було здійснено 3255 кібератак, з яких – 574 на Україну, що становить 17,6% [6]. Зауважимо, найбільше страждають від кібератак сайти державних органів, які надають послуги громадянам та оперують великою кількістю даних. Далі за кількістю атак іде фінансовий сектор, потім – засоби масової інформації, IT-компанії та енергетика. Усі ці сектори належать до групи ризику, їх треба убезпечувати передусім.

Найчастішим видом кібератак є DDos (Distributed Denial of Service) – розподілені атаки на відмову в обслуговуванні. Простіше кажучи, перевантаження сайту шляхом мільйонів запитів на секунду. Подібні атаки здатні зробити сайт недоступним на кілька годин. Так можна паралізувати надання важливих державних послуг або під час бойових дій у місті «вимкнути» світло.

Більш смертоносними є атаки, для яких використовують програмне забезпечення Wiper. Цей тип шкідливого програмного забезпечення призначений для безповоротного знищення даних на системі жертви – зараження комп'ютерів вірусом, який здатен знищувати дані. Це може надовго «вимкнути» компанію або організацію, якщо вона не має швидкого доступу до резервних копій. У будь-якому разі це призводить до збитків.

На початку 2024 р. хакери атакували дата-центр «Парковий», що призвело до збою в роботі Нафтогазу, Укрзалізниці, Укрпошти, а також системи «Шлях».

09.12.2024 р. державні реєстри України та сайт Міністерства юстиції України зазнали наймасштабнішої останнім часом зовнішньої кібератаки Як наслідок, призупинено роботу державних реєстрів Міністерства юстиції України.

За твердженням СБУ, до атаки на реєстри Мін'юсту знову причетні спецслужби росії. Заявлений хакерами обсяг начебто викрадених з реєстрів даних у 700 терабайт неможливо непомітно викачати за хвилину, годину чи добу. Найбільш імовірно, що хакери тривалий час «сиділи» у системах Мін'юсту. Утім, захищені частини систем Мін'юсту зламані не були, копії баз даних збереглися. Усе ж наслідки кібератаки виявилися катастрофічними. По-перше, зупинені всі дії, пов'язані, зокрема, з реєстрацією, банальними операціями купівлі-продажу, з яких отримують податки, включно з військовим збором. Люди не можуть здійснити нотаріальні дії щодо купівлі-продажу рухомого та нерухомого майна, оформлення спадщини, а також доручень на виконання певних дій. Тобто було заблоковано величезний сегмент економіки, який забезпечує надходження до бюджету, а громадяни не можуть розпоряджатися власним майном і ризикують стати об'єктом шахрайських дій.

Отже, сучасна практика виконання завдань кібербезпеки вимагає від теорії оперативного розв'язання низки нагальних наукових проблем, зокрема впровадження сучасних стандартів і новітніх інноваційних технологій з кібербезпеки.

На сучасному ринку, який динамічно змінюється відповідно до новітніх викликів і загроз, представлений широкий спектр цифрових інструментів кібербезпеки.

Основні тренди в цифровій кібербезпеці та характеристики цифрових продуктів узагальнено в табл. 1.

Одним з основних класів цифрових інструментів кібербезпеки є інструменти для виявлення і попередження атак. Це можуть бути системи на основі штучного інтелекту, які аналізують аномальну активність у мережах і надають можливість вчасно виявляти потенційні загрози. Наприклад, технології машинного навчання використовують для навчання алгоритмів, що зможуть адаптивно реагувати на змінні умови в мережі та блокувати шкідливий трафік.

Також до цифрових інструментів кібербезпеки належать рішення для захисту даних, такі як сучасні системи шифрування і управління доступом. Вони дають змогу гарантувати безпеку інформації на всіх етапах її оброблення, зберігання та передання. Крім того, розроблення ефективних систем резервного копіювання і відновлення даних є критично важливим для захисту підприємств від катастрофічних наслідків кібератак.

Іншим важливим аспектом є використання сучасних технологій багатофакторної аутентифікації та систем управління ідентичністю. Це дає змогу значно підвищити рівень захисту підприємства від несанкціонованого доступу та забезпечити надійну верифікацію користувачів у цифрових системах. Завдяки такій технології підвищується стійкість інформаційних систем до потенційних атак.

Одним з основних класів цифрових інструментів кібербезпеки є інструменти для виявлення і попередження атак. Це можуть бути системи на основі штучного інтелекту, які аналізують аномальну активність у мережах і надають можливість вчасно виявляти потенційні загрози. Наприклад, технології машинного навчання використовують для навчання алгоритмів, що зможуть адаптивно реагувати на змінні умови в мережі та блокувати шкідливий трафік.

Також до цифрових інструментів кібербезпеки належать рішення для захисту даних – сучасні системи шифрування та управління доступом. Вони дають змогу гарантувати безпеку інформації на всіх етапах її оброблення, зберігання та передання. Крім того, розроблення ефективних систем резервного копіювання і відновлення даних є критично важливим для захисту підприємств від катастрофічних наслідків кібератак.

Іншим важливим аспектом є використання сучасних технологій багатофакторної аутентифікації та систем управління ідентичністю. Це дає змогу значно підвищити рівень захисту підприємства від несанкціонованого доступу та забезпечити надійну верифікацію користувачів у цифрових системах. Завдяки такій технології підвищується стійкість інформаційних систем до потенційних атак.

Практичні приклади застосування сучасних інструментів кіберзахисту демонструють їхню ефективність у різних галузях. Наприклад, у фінансовому секторі інструменти кіберзахисту часто передбачають використання систем блокування трансакцій і аналізу ризиків для виявлення підозрілої активності. У галузі енергетики використовуються рішення для моніторингу енергетичних мереж, що дають змогу оперативно реагувати на атаки та забезпечувати безперервність функціонування.

Також важливо зазначити, що комплексна реалізація сучасних цифрових інструментів кібербезпеки повинна враховувати специфіку кожного підприємства.

Таблиця 1

Сучасні цифрові тренди та їхні основні функціональні можливості

Назва тренда кібербезпеки	Скорочена англійська абревіатура	Основні функціональні можливості
Системи для виявлення та попередження атак	IDS/IPS	Призначені для моніторингу мережі та виявлення аномальної активності, що може свідчити про кібератаки. Вони використовують різні методи аналізу трафіка, зокрема машинне навчання та сигнатурні бази даних
Рішення для захисту даних та шифрування		Гарантують безпеку даних як під час зберігання, так і під час передавання їх через мережу. Вони запобігають витоку даних і забезпечують конфіденційність
Багатофакторна аутентифікація	MFA	Використовують кілька рівнів перевірки особи користувача, що значно підвищує безпеку доступу до важливих інформаційних ресурсів
Інструменти для захисту від шкідливого програмного забезпечення	Antivirus/EDR	Дають змогу виявляти, блокувати та нейтралізувати віруси, трояни, руткіти та інше шкідливе програмне забезпечення, яке може загрожувати цифровій інфраструктурі підприємства
Системи для моніторингу та управління інформаційною безпекою	SIEM	Збирають, зберігають і аналізують дані з різних джерел, щоб забезпечити виявлення потенційних загроз і відповісти на них
Інструменти для захисту хмарних сервісів		Забезпечують захист хмарних сервісів і даних, які зберігаються в хмарах
Інструменти для управління ризиками та оцінювання загроз		Допомагають прогнозувати можливі кіберзагрози та визначати ймовірність виникнення їх, а також стратегічно планувати заходи для зниження ризиків

Джерело: побудовано на основі даних [2-5].

Таблиця 2

Сучасні цифрові продукти для забезпечення кібербезпеки: ціна / якість

Назва продукту	Основні функціональні можливості / якість	Ціна
1. Системи для виявлення та попередження атак (IDS/IPS)		
Cisco Secure IDS/IPS	Виявлення і блокування атак у реальному часі. Інтегрується з іншими засобами захисту, що дає змогу автоматично реагувати на загрози, знижуючи час між атакою та відповіддю. Відомий своєю ефективністю у великомасштабних інфраструктурах і визнаний одним з лідерів у галузі кібербезпеки	Висококласний корпоративний продукт, що має значну вартість. Ціна залежить від масштабу інсталяції, але для середніх і великих підприємств вартість може варіюватися від кількох тисяч до десятків тисяч доларів на рік
Palo Alto Networks Next-Generation Firewall	Моніторинг і захист мережі з глибоким аналізом трафіка та виявленням нульових уразливостей, що може автоматично блокувати будь-які шкідливі дії. Відомий високою ефективністю у виявленні та блокуванні загроз, забезпечує комплексний захист від різноманітних атак на мережі та додатки. Передбачає інтеграцію із системами управління безпекою та дає змогу налаштувати різноманітні правила для контролю доступу	Продукт належить до преміум-сегмента, його вартість може коливатися від кількох тисяч до десятків тисяч доларів (залежно від масштабів компанії та необхідного рівня захисту)
2. Рішення для захисту даних і шифрування		
Symantec Encryption	Шифрування даних на всіх етапах оброблення (як для шифрування файлів на комп'ютерах, так і для захисту електронної пошти)	Вартість ліцензії для одного користувача варіюється від 30 до 100 дол. США на рік (залежно від масштабу й типу організації)
Vormetric Data Security Platform	Шифрування даних, контроль доступу та моніторинг, забезпечує повний контроль над даними в реальному часі, що дає змогу виявляти підозрілу активність	Вартість цієї платформи може починатися від кількох тисяч доларів на рік для малого підприємства; зростає залежно від кількості користувачів та обсягу даних
3. Багатофакторна аутентифікація		
Microsoft Azure MFA	Забезпечення багатофакторної аутентифікації в хмарних і локальних системах, що використовує як паролі, так і біометричні дані або мобільні пристрої для підтвердження особи. Інтегрується із численними платформами Microsoft, забезпечує високий рівень безпеки доступу та є ефективною для захисту від несанкціонованого доступу	Базова вартість для малих і середніх підприємств стартує від 6 дол. США на користувача на місяць. Для більших організацій є можливість використовувати додаткові платні функції, що підвищує ціну

Продовження табл. 2

Duo Security	Інтегрується з різними корпоративними додатками та дає організаціям змогу забезпечити додатковий рівень захисту шляхом використання смартфонів, одноразових паролів і біометрії. Висока ефективність у забезпеченні багатофакторної аутентифікації з підтриманням широкого спектра пристроїв і технологій	Пропонує вартість від 3 дол. США на користувача на місяць для базових функцій. Додаткові функції можуть збільшувати вартість до 9 дол. США на користувача на місяць. Відмінно підходить для підприємств будь-якого розміру завдяки гнучкості
4. Інструменти для захисту від шкідливого програмного забезпечення		
CrowdStrike Falcon	Виявлення та реагування на інциденти в режимі реального часу. Поєднує антивірус, систему виявлення вторгнень та аналітику на основі штучного інтелекту для прогнозування нових загроз. Має потужні аналітичні можливості для боротьби з найбільш складними загрозами	Вартість залежить від обсягу послуг і кількості кінцевих точок. Для малого бізнесу ціна починається від 8 дол. США на кінцеву точку на місяць, але для великих організацій вона може зрости до десятків тисяч доларів на рік
Bitdefender GravityZone	Захист від шкідливого програмного забезпечення, що об'єднує антивірусні технології з інструментами для моніторингу мережі та захисту від нульових атак. Антивірусне рішення з додатковими інструментами для виявлення і блокування шкідливого програмного забезпечення	Ціна ліцензій починається від 40 дол. США на рік для одного пристрою, що робить цей продукт доступним для середніх і великих підприємств. Це один з найкращих варіантів для середнього бізнесу, зважаючи на його ефективність і доступність
5. Системи для моніторингу та управління інформаційною безпекою		
Splunk	Моніторинг та аналіз безпеки в реальному часі. Дає змогу автоматично виявляти аномальні події, що можуть свідчити про кіберзагрози. Використовує аналітику даних для побудови звітів і надання інформації для ухвалення рішень. Потужна аналітика даних і високий рівень масштабованості. Гнучкість у створенні дашбордів і звітів. Велика кількість інтеграцій із зовнішніми системами (понад 2800 додатків на Splunkbase)	Висока вартість ліцензії, особливо для великих обсягів даних. Стрімке зростання витрат із збільшенням обсягів аналізованих даних. Підходить для великих компаній із значним бюджетом і необхідністю глибокої аналітики. Для малих організацій ціна може бути занадто високою
IBM QRadar	Збір, аналіз і кореляція даних безпеки з різних джерел, що забезпечує гнучкість і можливість оперативного реагування на інциденти. Високий рівень автоматизації реагування на інциденти. Можливість інтеграції з іншими рішеннями IBM і сторонніми інструментами (понад 600 інтеграцій)	Високі витрати на впровадження. Вартість може бути надто високою для середніх і малих організацій. Ідеальне рішення для організацій із багаторівневою інфраструктурою, яким потрібна швидка обробка даних безпеки

Продовження табл. 2

6. Інструменти для захисту хмарних сервісів		
McAfee Cloud Security	Забезпечує захист даних у хмарі, зокрема через шифрування, а також контроль доступу до ресурсів, що дає змогу запобігати витокам даних і атакам. Високий рівень захисту даних у хмарі через шифрування. Простота у впровадженні та використанні. Широкий набір функцій для контролю доступу	Вартість може бути високою для малих компаній. Оптимальний вибір для компаній, що активно використовують хмарні сервіси, але не хочуть ускладнювати процеси інтеграції
Zscaler Cloud Security	Безпечний доступ до хмарних додатків і захисту від кіберзагроз під час роботи із хмарними ресурсами. Передбачає антивірусний захист, перевірку вмісту та систему виявлення вторгнень. Гнучкість у налаштуванні політик безпеки для різних хмарних платформ. Вбудований захист від шкідливого програмного забезпечення	Підписка може виявитися дорогою для компаній із численними користувачами. Відмінно підходить для компаній, які прагнуть забезпечити високий рівень контролю над хмарними ресурсами
7. Інструменти для управління ризиками та оцінювання загроз		
RiskSense NIST	Управління ризиками, дає змогу здійснювати оцінювання вразливостей у цифровій інфраструктурі підприємства та розробляти стратегії реагування на потенційні загрози. Прозорий механізм оцінювання ризиків. Висока точність у визначенні вразливостей	Вартість може бути високою для малих підприємств. Розмір плати за ліцензію залежить від кількості аналізованих активів. Оптимальний вибір для організацій, що прагнуть інвестувати в проактивний захист і стратегічне управління ризиками
Cybersecurity Framework	Оцінювання кіберзагроз і управління ризиками, дає змогу систематизувати підхід до кібербезпеки та адаптуватися до різних галузей і ризиків	Безкоштовний стандарт із гнучкими рекомендаціями. Найкраще для організацій, які хочуть упровадити базовий рівень управління ризиками без значних інвестицій. Придатний для організацій будь-якого масштабу

Джерело: побудовано на основі даних [2-5].

Ідеться як про організаційні, так і технічні аспекти, що необхідні для створення ефективної системи кібербезпеки. Стратегічний підхід до інтеграції таких інструментів може передбачати не лише автоматизовані рішення, але й спеціалізовані політики безпеки, навчання персоналу та регулярне тестування систем на витривалість до кіберзагроз.

Водночас сучасний цифровий ринок пропонує різноманітні за ціною і якістю продукти, які мають відповідні функціональні можливості – якість і ціну. Аналіз якості та ціни деяких цифрових продуктів кібербезпеки наведено в табл. 2.

Аналіз наведених у табл. 2 даних проведено методом порівняння за двома ключовими показниками: ціна та якість. Це дало змогу оцінити, які продукти найбільш ефективні з точки зору витрат і які вигоди вони забезпечують для підприємств різного масштабу, а також узагальнити результати цього аналізу за трьома критеріями:

1. Висока якість, висока ціна. Palo Alto Networks, Cisco Secure IDS/IPS, CrowdStrike Falcon – підходять для великих підприємств, що потребують високоякісного, масштабованого захисту, але вимагають значних інвестицій.

2. Висока якість, помірна ціна. Microsoft Azure MFA, Duo Security, Bitdefender GravityZone – ідеальні для середнього бізнесу, із хорошим балансом між вартістю та функціональністю.

3. Добра якість, низька ціна. Symantec Encryption, Vormetric Data Security Platform – ці продукти можуть задовольнити потреби для малого та середнього бізнесу з обмеженими бюджетами.

Крім того, вибір продукту залежить від конкретних потреб підприємства, його масштабу, вимог до безпеки та бюджету.

Висновки. Отже, використання сучасних цифрових інструментів кібербезпеки є необхідною умовою для підтримання стійкості та безпеки підприємств в умовах цифровізації економіки. Ці інструменти надають ефективні рішення для виявлення та попередження загроз, а також для захисту інформаційних ресурсів від можливих атак. Інтегруючи такі інструменти в систему економічної безпеки підприємств, слід ураховувати специфіку діяльності кожного підприємства. Надзвичайно важливо також забезпечувати постійний розвиток і оновлення інструментів кібербезпеки з огляду на нові виклики та загрози в сучасному кіберпросторі.

Напрямами подальших наукових досліджень можуть бути дослідження впливу технології штучного інтелекту (AI) та машинного навчання AI на кібербезпеку підприємств.

Список використаних джерел

1. Kulakovskyi O., Pravdyvets O. Modern cybersecurity paradigm. *Кібероборотьба: розвідка, захист та протидія:* тези доповідей II Міжнародної науково-практичної конференції. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2024. С. 11-12. DOI: https://doi.org/10.61929/viti.mnpk.2.2024
2. Правдивець О., Літвін Н., Денисов О., Поліщук О., Олійник В. Стратегічні напрями інноваційного розвитку системи фінансово-економічної безпеки підприємства на основі цифрових технологій. *Фінансово-кредитна діяльність: проблеми теорії і практики:* зб. наук. пр. 2024. Вип. 6(59). С. 273-282. DOI: https://doi.org/10.55643/fcaptp.6.59.2024.4575
3. Spitz R., Zuin L. *The Definitive Guide to Thriving on Disruption*. *Vol. I. Reframing and Navigating Disruption*. San Francisco: Disruptive Futures Institute, 2022.
4. Коротченко Л. А., Дєгтярь О. А., Атаманенко М. В., Білий О. А. Деркач Т. М., Пантась С. О., Пантась І. О., Лазута Р. Р. Аналіз методів кібервійн та кібероперацій, які використовуються провідними країнами світу та членами НАТО. *Наука і техніка сьогодні*. 2024. № 7(35). С. 776-788. DOI: https://doi.org/10.52058/2786-6025-2024-7(35)-776-788
5. Гнатюк С. Кіберскладник російсько-української війни: уроки та оцінки міжнародної спільноти. *НІСД:* сайт. 28.06.2022. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/kiberskladnyk-rosiysko-ukrayinskoyi-viyny-uroky-ta-otsinky
6. Кібератаки на український бізнес тривають: як захиститися. *Економічна правда:* сайт. 03.05.2024. URL: https://epravda.com.ua/projects/zakhyst-krainy/2024/05/03/713224

References

1. Kulakovskyi, O., & Pravdyvets, O. (2024). Modern cybersecurity paradigm. In *Kiberborot'ba: rozvidka, zakhyst ta protydiya [Cyberwarfare: intelligence, defense and offensive security]*: Abstracts of the Reports of the 2nd International Scientific and Practical Conference (pp. 11-12). Kyiv: Kruty Heroes Military Institute of Telecommunications and Information Technology. DOI: https://doi.org/10.61929/viti.mnpk.2.2024
2. Pravdyvets, O., Litvin, N., Denysov, O., Polishchuk, O., & Oliynyk, V. (2024). Stratehichni napryamy innovatsiynoho rozvytku systemy finansovo-ekonomichnoyi bezpeky pidpryyemstva na osnovi tsyfrovykh tekhnolohiy [Strategic directions for innovative development of enterprise financial-economic security systems based on digital technologies]. In *Finansovo-kredytna diyal'nist': problemy teoriyi i praktyky [Financial and Credit Activity Problems of Theory and Practice]*: Vol. 6(59) (pp. 273-282). DOI: https://doi.org/10.55643/fcaptp.6.59.2024.4575 [in Ukranian].
3. Spitz, R., & Zuin, L. (2022). *The Definitive Guide to Thriving on Disruption*. *Vol. I. Reframing and Navigating Disruption*. San Francisco: Disruptive Futures Institute.
4. Korotchenko, L. A., Dyehtyar, O. A., Atamanenko, M. V., Bilyy, O. A., Derkach, T. M., Pantas, S. O., Pantas, I. O., & Lazuta, R. R. (2024). Analiz metodiv kiberviyn ta kiberoperatsiy, yaki vykorystovuyut'sya providnymy krayinamy svitu ta chlenamy NATO [Analysis of cyber warfare and cyber operations methodologies used by the world's leading countries and NATO members]. *Nauka i tekhnika s'ohodni – Science and Technology Today*, 7(35), 776-788. DOI: https://doi.org/10.52058/2786-6025-2024-7(35)-776-788 [in Ukranian].
5. Hnatyuk, S. Kiberskladnyk rosiys'ko-ukrayins'koyi viyny: uroky ta otsinky mizhnarodnoyi spil'noty [The cyber component of the Russian-Ukrainian war: lessons and assessments of the international community] (2022, Jun 28). *NISD:* Website. Retrieved from https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/kiberskladnyk-rosiysko-ukrayinskoyi-viyny-uroky-ta-otsinky [in Ukranian].
6. Kiberataky na ukrayins'kyy biznes tryvayut': yak zakhystytysya [Cyberattacks on Ukrainian businesses continue: how to protect yourself] (2024, May 03). *Epravda*: Website. Retrieved from https://epravda.com.ua/projects/zakhyst-krainy/2024/05/03/713224 [in Ukranian].

Pravdyvets O. M. Modern digital cybersecurity tools in the economic security system of Ukrainian enterprises

The article is devoted to the analysis of modern digital cybersecurity tools used in the economic security system of Ukrainian enterprises, their role in countering cyber threats and increasing the resilience of the digital infrastructure of Ukrainian enterprises in repelling the armed aggression of the Russian Federation. An analysis of scientific research by domestic and foreign scientists on the impact of cyber threats and means of neutralizing them was conducted. The analysis revealed that despite a significant amount of scientific research, a number of problems remain unresolved. These include insufficient attention to the integration of various digital tools, in particular cybersecurity, into a single system that would take into account the specifics of a particular enterprise, as well as the lack of a comprehensive approach to assessing the effectiveness of such tools. This highlights the need for further research in this area. The main classes of modern digital cybersecurity tools were identified, their capabilities and significance for improving the overall resilience of an enterprise's digital infrastructure were described, and their cost and capabilities were analyzed. The need for their comprehensive implementation, taking into account the specific activities of each enterprise, was justified. The cost and quality of some digital cybersecurity products were analyzed by comparing two key indicators: price and quality. This made it possible to assess which products are most cost-effective and what benefits they provide for enterprises of different sizes, and to summarize the results of this analysis according to three criteria: High quality, high price; High quality, moderate price; Good quality, low price. The study found that the use of modern digital cybersecurity tools is a prerequisite for maintaining the stability and security of enterprises in the context of the digitalization of the economy. These tools provide effective solutions for detecting and preventing threats, as well as for protecting information resources from possible attacks. It is important that the integration and implementation of such tools into the economic security system of enterprises takes into account the specific activities of each enterprise and requires continuous development and updating, taking into account new challenges and threats in the modern cyberspace.

Keywords: cybersecurity, digital tools, economic security, enterprise, digital infrastructure protection.

Правдивець Олександр Миколайович – кандидат військових наук, доцент кафедри управління фінансово-економічною безпекою Навчально-наукового інституту менеджменту безпеки ВНЗ «Університет економіки та права «КРОК» (e-mail: pravd72@ukr.net, ORCID ID: https://orcid.org/0000-0001-5242-9683).

Pravdyvets Oleksandr Mykolayovych – Ph.D. (Military), Associate Professor of the Department of financial and economic security management of the Academic institute of safety management of the KROK University.

Надійшло 17.02.2025 р.