УДК 004.056.5:658.5
JEL Classification: G 32, O 10, H 56, D 81, L 86
DOI: *http://doi.org/10.34025/2310-8185-2024-2.94.02*

Анна Кримська, к.т.н., ст. викладач,
https://orcid.org/0000-0001-6410-9476
Чернівецький торговельно-економічний інститут ДТЕУ,
м. Чернівці

АНАЛІЗ ЕФЕКТИВНОСТІ ЗАХОДІВ З БЕЗПЕКИ ІНФОРМАЦІЙНИХ МЕРЕЖ В ЕКОНОМІЧНОМУ КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

Анотація

Актуальність. Постановка проблеми. У сучасних умовах цифрового середовища захист конфіденційної інформації в економічних організаціях має надзвичайно важливе значення. У статті розглянуто критично важливу сферу безпеки інформаційних мереж, досліджено її ефективність в економічному корпоративному середовищі. Актуальність дослідження зумовлена зростанням частоти та складності кіберзагроз, спрямованих на підприємства у всьому світі, що вимагає всебічного вивчення ефективності заходів безпеки.

Мета дослідження – оцінити ефективність наявних заходів безпеки інформаційних мереж, що застосовуються в економічному корпоративному середовищі. За допомогою детального аналізу різних протоколів безпеки, методів шифрування, контролю доступу та систем моніторингу в дослідженні визначено їх реальну ефективність у зменшенні кіберзагроз та захисті корпоративних активів.

Результати дослідження виявили як сильні, так і слабкі сторони сучасних практик безпеки інформаційних мереж. Незважаючи на те, що деякі заходи показують високу стійкість до типових кіберзагроз, вразливості залишаються, що наражає корпорації на потенційні загрози зламу та компрометації даних. Такі фактори, як недостатня підготовка працівників, застаріле програмне забезпечення та нові кіберзагрози, посилюють ці вразливості.

На основі отриманих даних можна зробити кілька важливих висновків. По-перше, необхідний цілісний підхід до безпеки інформаційних мереж, що охоплює технологічні, організаційні та людські чинники. По-друге, постійний моніторинг, оцінювання та адаптація заходів безпеки є обов'язковими для ефективної протидії новим кіберзагрозам. До того ж розвиток культури кібербезпеки серед працівників має вирішальне значення для зміцнення корпоративного захисту.

Практичне значення. У статті підкреслено критичну важливість надійних заходів безпеки інформаційних мереж в економічному корпоративному середовищі. Завдяки всебічному оцінюванню ефективності наявних протоколів безпеки, виявленню вразливостей та окресленню стратегій їх вдосконалення результати цього дослідження сприяють зміцненню корпоративного захисту від

кіберзагроз. Постійний розвиток технологій та кіберзагроз вимагає постійної уваги та адаптації для захисту корпоративних активів та збереження довіри до цифрової екосистеми.

Перспективи подальших досліджень. Майбутні дослідження можуть стосуватися нових технологій, як-от штучний інтелект і блокчейн, у підвищенні безпеки інформаційних мереж. Цінною інформацією можуть стати дослідження впливу нормативно-правової бази та галузевих стандартів на корпоративні практики кібербезпеки.

Ключові слова: захист даних, кіберзагрози, шифрування інформації, комплаєнс у кібербезпеці, криптографічні протоколи.

Кількість джерел: 17; кількість таблиць: 2.

Anna Krymska, Candidate of Technical Sciences,
Senior Lecturer,
https://orcid.org/0000-0001-6410-9476
Chernivtsi Institute of Trade and Economic of SUTE, Chernivtsi

ANALYSIS OF THE EFFECTIVENESS OF INFORMATION NETWORK SECURITY MEASURES IN AN ECONOMIC CORPORATE ENVIRONMENT

Summary

In modern conditions of the digital environment, the protection of confidential information in economic organizations is of paramount importance. This article examines the critically important sphere of information network security and investigates its effectiveness in the economic corporate environment. The relevance of this research is driven by the increasing frequency and complexity of cyber threats targeting enterprises worldwide, necessitating a comprehensive study of the effectiveness of security measures.

The research aims to assess the effectiveness of existing information network security measures applied in the economic corporate environment. This study identifies their real effectiveness in reducing cyber threats and protecting corporate assets through detailed analysis of various security protocols, encryption methods, access control, and monitoring systems.

The research results reveal both strengths and weaknesses of modern information network security practices. Despite some measures demonstrating high resilience to typical cyber threats, vulnerabilities persist, exposing corporations to potential data breaches and compromises. Factors such as inadequate employee training, outdated software and emerging cyber threats exacerbate these vulnerabilities.

Based on the data obtained, several important conclusions can be drawn. Firstly, a comprehensive approach to information network security is necessary, which encompasses technological, organizational, and human factors. Secondly, continuous

monitoring, assessment, and adaptation of security measures are mandatory for effectively combating new cyber threats. Moreover, fostering a culture of cybersecurity among employees is crucial for strengthening corporate defense.

In conclusion, this article underscores the critical importance of reliable information network security measures in the economic corporate environment. Through comprehensive evaluation of the effectiveness of existing security protocols, vulnerability identification and outlining strategies for improvement, the results of this research contribute to enhancing corporate protection against cyber threats.

Keywords: Data protection, cyber threats, information encryption, cyber security compliance, cryptographic protocols.

Number of sources – 17, number of tables – 2.

Постановка проблеми. У сучасну цифрову епоху безпека інформаційних мереж стала одним із найважливіших питань для організацій, особливо в економічному корпоративному середовищі. В умовах, коли бізнес щораз більше покладається на складні інформаційні системи для управління операціями, захисту конфіденційних даних та збереження конкурентних переваг, потреба в надійних заходах безпеки є як ніколи актуальною. Проблема забезпечення мережевої безпеки охоплює різні виклики, зокрема захист від кіберзагроз, захист інтелектуальної власності, збереження цілісності та доступності даних.

Важливість цього дослідження зумовлена зростанням частоти та складності кібератак, спрямованих на корпоративні мережі. Фінансові, репутаційні та операційні наслідки порушень безпеки можуть бути катастрофічними, призводячи до значних збитків і довгострокових наслідків для бізнесу. Шляхом систематичного аналізу та оцінювання різних заходів безпеки в дослідженні сформульовано пропозиції, які можуть допомогти організаціям удосконалити свої системи безпеки та краще захистити свої інформаційні активи.

Аналіз останніх досліджень і публікацій. Аналіз ефективності заходів безпеки інформаційних мереж в економічному корпоративному середовищі є важливою сферою дослідження з огляду на частоту та складність кіберзагроз, що зростають. Сучасні дослідження [1, с. 179] зосереджені як на технологічних, так і на організаційних аспектах мережевої безпеки, висвітлюють досягнення та виявляють недоліки, які все ще потребують вирішення.

Одним із важливих напрямів розвитку є впровадження передових алгоритмів машинного навчання для систем виявлення проникнень (IDS). Такі дослідники, як М. В. Копійка [2, с. 93], показали, що моделі глибинного навчання, особливо ті, що базуються на нейронних мережах, можуть значно підвищити точність і ефективність виявлення аномальної активності в корпоративних мережах. Такі моделі навчаються на великих масивах даних, щоб розпізнавати патерни, які можуть сигналізувати про потенційні порушення безпеки, що дозволить запобігти загрозам та швидко реагувати на них.

На доповнення до технологічних досягнень зростає увага й до людського фактора в безпеці інформаційних мереж. Такі науковці, як І. М. Доронін [3, с. 34] та А. В. Турчак [4, с. 125], дослідили, як поведінка та обізнаність працівників впливають на загальний стан безпеки організації. Їхні дослідження показали, що регулярне навчання та спеціальні програми можуть сприяти зниженню ризику інцидентів безпеки, спричинених людськими помилками. Водночас вони також наголошують, що підтримання високого рівня обізнаності серед працівників залишається постійним викликом.

Ефективність заходів мережевої безпеки також дуже тісно пов’язана з інтеграцією надійних протоколів шифрування [5]. Розвідки таких провідних дослідників, як І. О. Ревак, Р. Т. Грень [6, с. 167], наголошують на важливості використання передових стандартів шифрування (AES) та інфраструктури відкритих ключів (PKI) для захисту конфіденційних корпоративних даних. Ці методи забезпечують надійний захист від несанкціонованого доступу, але швидкий розвиток квантових обчислень створює загрозу для наявних криптографічних методів. Науковці активно досліджують квантово-стійкі алгоритми, але їх практична реалізація все ще перебуває на початковій стадії.

Поява пристроїв Інтернету речей (IoT) у корпоративному середовищі створює нові вразливості. Дослідження А. О. Остапець [7, с. 42] підкреслює складність захисту великого і неоднорідного масиву приєднаних пристроїв. Цим пристроям часто бракує надійних захисних засобів, що робить їх

головними цілями для атак. Докладаються зусилля для розроблення комплексних систем безпеки, здатних урахувати різноманітну природу екосистем Інтернету речей, але стандартизація в цій галузі все ще відсутня.

Технологія блокчейн є ще одним перспективним напрямом для підвищення безпеки мережі. Деякі дослідники, як-от А. О. Шульга [8, с. 87], вивчали використання блокчейну для безпечних транзакцій даних та управління ідентифікацією. Децентралізована природа блокчейну забезпечує невід'ємні переваги безпеки, такі як захист записів від несанкціонованого доступу та прозорі аудиторські записи. Втім, для того щоб блокчейн став прийнятним варіантом для широкого корпоративного впровадження, необхідно вирішити питання масштабованості та енергоефективності.

Незважаючи на певні досягнення у сфері кібербезпеки, залишається кілька невирішених питань. Однією з головних проблем є узгодження заходів безпеки з організаційними цілями та економічними міркуваннями. Як зазначає М. С. Курков [9, с. 144], часто існує розрив між уявною вартістю інвестицій у безпеку та їх фактичним впливом на ефективність бізнесу. Ця невідповідність може призвести до недостатнього інвестування в критично важливу інфраструктуру безпеки або, навпаки, до надмірного інвестування в менш ефективні заходи.

Іншим важливим викликом є мінливий характер кіберзагроз. Зловмисники постійно адаптують свою тактику, що ускладнює збереження ефективності статичних заходів безпеки.

Формулювання цілей статті й аргументування актуальності поставленого завдання. Мета дослідження – оцінити ефективність наявних заходів безпеки інформаційних мереж, що застосовуються в економічному корпоративному середовищі.Відповідно до мети було поставлено та вирішено такі завдання: визначити та систематизувати різні типи заходів безпеки, які наразі впроваджуються в інформаційних мережах економічних корпоративних середовищ; оцінити потенційні загрози та вразливості, які ці заходи безпеки повинні усунути, включно з аналізом останніх тенденцій кібератак; провести

аналіз конкретних прикладів окремих корпорацій для вивчення практичних даних про впровадження та ефективність їхніх заходів безпеки.

Актуальність дослідження зумовлена зростанням частоти та складності кіберзагроз, спрямованих на підприємства у світі, що вимагає всебічного вивчення ефективності заходів безпеки.

Виклад основного матеріалу. Забезпечення інформаційної безпеки є багатоаспектним завданням, яке вимагає комплексного підходу, що поєднує технологічні заходи, організаційну політику та постійне навчання персоналу. В умовах зростання складності та досконалості кіберзагроз організації мають застосовувати надійний набір методів і засобів для захисту своїх інформаційних активів. Це стосується як технологічних заходів, як-от шифрування даних, мережеві екрани та системи виявлення вторгнень, так і організаційних заходів, таких як політика безпеки та безперервне навчання і підвищення кваліфікації персоналу (табл. 1).

Технологічні заходи становлять основу стратегій інформаційної безпеки. Одним із найважливіших технологічних заходів є шифрування даних. Шифрування перетворює читабельний формат даних у нечитабельний за допомогою алгоритмів і ключів, а це гарантує, що в разі перехоплення інформації її неможливо буде розшифрувати без відповідного ключа. Така технологія є дуже важливою для захисту конфіденційної інформації, яка зберігається на серверах, передається мережею або використовується в комунікації. Стандарти шифрування, як-от Advanced Encryption Standard (AES) і RSA, набули широкого поширення для захисту цілісності та конфіденційності даних [10, с. 211].

Мережеві екрани, які зазвичай називають брандмауерами, є ще одним важливим компонентом технологічних заходів. Вони виступають бар’єрами між довіреними внутрішніми мережами та зовнішніми мережами, такими як Інтернет, які визнаються як ненадійні. Вони здатні відстежувати та здійснювати контроль мережевого трафіку, спираючись на визначені правила безпеки.

Таблиця 1

Технологічні та організаційні засоби забезпечення інформаційної безпеки*

Технологічні за сади	*Організаційні засади*
Шифрування даних, яке захищає конфіденційну інформацію, перетворюючи її в нечитабельний формат за допомогою алгоритмів і ключів. Приклади включають AES і RSA.	Політики безпеки, які встановлюють рамки для управління та захисту інформаційних активів, включно з політикою прийнятного використання, класифікацією даних, контролем доступу та процедурами реагування на інциденти.
Брандмауери – мережеві екрани, які відстежують і контролюють вхідний і вихідний трафік на основі правил безпеки для запобігання несанкціонованому доступу та блокування шкідливого трафіку.	Освітні програми, які навчають працівників найкращим практикам інформаційної безпеки, таким як розпізнавання спроб фішингу, створення надійних паролів та захист конфіденційної інформації.
Системи виявлення вторгнень (IDS), які здійснюють моніторинг мережевого трафіку на наявність ознак зловмисної діяльності або порушень політик, попередження про потенційні інциденти безпеки.	Професійний розвиток, який надає можливості для безперервної освіти та сертифікації для IT-спеціалістів і спеціалістів з безпеки для покращення навичок виявлення загроз, реагування на інциденти та дотримання нормативних вимог.
Системи запобігання вторгненням (IPS), які автоматично вживають заходів для блокування або карантину загроз, виявлених IDS, посилюючи проактивні заходи безпеки.	Плани реагування на інциденти – детальні процедури реагування на інциденти безпеки, включаючи ролі, обов'язки і кроки для пом'якшення наслідків атак та відновлення після них.
Антивірусне програмне забезпечення – виявляє та видаляє зловмисні програми, захищаючи систему від шкідливого програмного забезпечення.	Управління контролем доступу – політика та процедури управління доступом до інформації та систем, які гарантують, що лише уповноважені особи мають знати та отримувати конфіденційні дані.
Безпечні мережеві протоколи – передбачають використання таких протоколів, як SSL/TLS, для захисту передачі даних мережею, забезпечення конфіденційності та цілісності комунікацій.	Регулярний аудит безпеки – постійне оцінювання політик, процедур і засобів контролю безпеки для виявлення та усунення вразливостей і забезпечення відповідності стандартам.
Управління оновленнями – регулярне оновлення програмного забезпечення та систем для усунення вразливостей безпеки та захисту від експлойтів.	Стратегії регулярного резервного копіювання даних та забезпечення їх швидкого відновлення у випадку втрати даних.
Багатофакторна автентифікація (MFA) є додатковим рівнем безпеки, що вимагає декількох різних форм перевірки перед наданням доступу до систем або даних.	Кампанії з підвищення обізнаності про безпеку – це ініціативи, спрямовані на просування культури безпеки в організації та заохочення працівників надавати пріоритет інформаційній безпеці у своїй повсякденній діяльності.

*Джерело: [9; 10].

Брандмауери можуть бути апаратними, програмними або комбінованими, вони відіграють важливу роль у запобіганні несанкціонованому доступу, блокують зловмисний трафік та пом'якшують наслідки різних видів кібератак.

Системи виявлення вторгнень (IDS) доповнюють брандмауери, забезпечуючи моніторинг і аналіз мережевого трафіку в режимі реального часу на предмет виявлення ознак зловмисної діяльності або порушень політик. IDS можуть бути мережевими (NIDS) або хостовими (HIDS). Мережеві системи контролюють трафік у сегменті мережі, тоді як хост-системи аналізують дії на окремих комп'ютерах або пристроях. IDS може попереджати адміністраторів про потенційні інциденти безпеки, що дозволяє швидко реагувати на них і пом'якшувати їх наслідки. Деякі системи також містять системи запобігання вторгненням (IPS), які можуть автоматично блокувати або відправляти загрози на карантин [11, с. 36].

Незважаючи на те, що технологічні заходи мають визначальне значення для забезпечення інформаційної безпеки, організаційні заходи є не менш важливими. Одним з основоположних організаційних заходів є створення комплексної політики безпеки. Така політика встановлює рамки для управління інформаційними активами організації та їх захисту. Вони окреслюють політики прийнятного використання, схеми класифікації даних, політики контролю доступу та процедури реагування на інциденти. Ефективні політики безпеки регулярно переглядаються та оновлюються, щоб адаптуватися до нових загроз та бізнес-вимог [12, с. 137].

Навчання та професійний розвиток персоналу є ключовими компонентами надійної стратегії інформаційної безпеки. Працівники нерідко є ланкою першої лінії захисту від кіберзагроз, а їх поінформованість і професіональна поведінка суттєво впливають на загальний стан безпеки організації. Регулярні освітні програми мають навчати працівників найкращим практикам інформаційної безпеки, як-от розпізнавання спроб фішингу, створення надійних паролів і захист конфіденційної інформації. Спеціалізовані тренінги для

IT-спеціалістів та фахівців з безпеки мають охоплювати такі складні теми, як виявлення загроз, реагування на інциденти та дотримання стандартів і правил безпеки [13, с. 106]. До того ж розвиток культури безпеки в організації заохочує співробітників надавати пріоритет інформаційній безпеці у своїй повсякденній діяльності. Цього можна досягти завдяки можливостям безперервного професійного розвитку, сертифікації та участі в безпекових спільнотах і форумах. Завдяки інвестиціям у навички та знання персоналу компанії можуть краще підготуватися до загроз та реагувати на них.

Аналіз реальних випадків щодо кібербезпеки корпоративного середовища наголошує на важливості багаторівневого підходу до цієї проблеми. У 2017 році злам Equifax був яскравим прикладом того, як численні збої в системі безпеки поглибили наслідки. Відому вразливість у вебдодатку не було виправлено, а недостатня сегментація мережі дозволила зловмисникам отримати доступ до конфіденційних даних. Цей інцидент свідчить про важливість своєчасного управління оновленнями та необхідність надійного захисту зовнішнього периметру в поєднанні з внутрішнім контролем [14, с. 28].

У випадку атаки SolarWinds 2020 року зловмисники вставили шкідливий код в оновлення програмного забезпечення Orion, який потім було розповсюджено серед численних організацій. Ця складна атака на ланцюжок поставок показала вразливість процесів розроблення та розповсюдження програмного забезпечення. Інцидент наголосив на необхідності комплексних заходів безпеки ланцюга постачання та постійного моніторингу цілісності програмного забезпечення. Зазначимо, що в наявних натепер методах та підходах інформаційної безпеки на корпоративних підприємствах є ціла низка слабких місць, які роблять їх вразливими до атак (табл. 2).

Виявлення загальних слабких місць і недоліків у наявних методах забезпечення безпеки інформаційних мереж дозволяє виявити кілька ключових напрямів для їх вдосконалення.

Таблиця 2

Слабкі місця наявних підходів до забезпечення безпеки інформаційних мереж у корпоративному середовищі*

Метод (підхід)	*Його «слабке» місце*
Брандмауери та IDS/IPS	Покладання на заздалегідь визначені правила та ознаки може пропустити нові або складні атаки; IDS може генерувати велику кількість помилкових спрацьовувань, що призводить до виснаження системи оповіщення.
Безпека кінцевих точок	Боротьба з експлоітами нульового рівня; управління та оновлення програмного забезпечення для захисту на численних пристроях може вимагати значних ресурсів.
Шифрування	Складність управління ключами; підвищення продуктивності; не захищає від усіх типів атак, як-от несанкціонований доступ за допомогою викрадених облікових даних.
Механізми контролю доступу (MFA, RBAC)	Впровадження та обслуговування може бути складним; MFA може сприйматися користувачами як незручний, що призводить до потенційного опору з їх боку.
Сегментація мережі	Може бути складним і дорогим у впровадженні та управлінні; неправильна сегментація все ще може дозволити зловмисникам рухатися в обхід мережі.
SIEM-системи	Висока вартість і значний експертний потенціал, необхідний для ефективного управління; може призвести до виснаження через великий обсяг даних і хибних спрацьовувань.
Управління виправленнями	Забезпечення своєчасного оновлення всіх систем може бути складним завданням; невиправлені вразливості залишаються значним ризиком.
Людський фактор (навчання та обізнаність)	Співробітники можуть стати жертвами спланованих соціальних атак; підтримка постійних ефективних навчальних програм є складним завданням.
Проактивні та адаптивні стратегії безпеки	Можуть бути ресурсомісткими та вимагати спеціалізованої експертизи; використання штучного інтелекту та аналітики загроз може призвести до ускладнення та появи нових типів уразливостей.
Обмеженість ресурсів у МСП	Обмежені фінансові та людські ресурси ускладнюють запровадження комплексних заходів безпеки; необхідні масштабовані рішення для забезпечення безпеки, але їх все ще може бути недостатньо.

*Джерело: [14; 15].

Однією з головних проблем є людський фактор. Незважаючи на передові технологічні заходи, людські помилки залишаються досить актуальними. Атаки соціальної інженерії, такі як фішинг, використовують цю вразливість, що підкреслює необхідність регулярних тренінгів та програм підвищення обізнаності для працівників [16, с. 78].

Ще одним критичним недоліком є реактивність багатьох заходів безпеки. Традиційні рішення безпеки часто спираються на відомі загрози та шаблони, що робить їх менш ефективними проти нових загроз. Це наголошує на важливості прийняття проактивних та адаптивних стратегій безпеки, як-от пошук загроз та використання штучного інтелекту (ШІ), для прогнозування та пом'якшення потенційних атак.

Обмеженість ресурсів також є значною проблемою. Малим та середнім підприємствам (МСП) часто не вистачає фінансових та людських ресурсів для впровадження комплексних заходів безпеки. Ця проблема свідчить про потребу в масштабованих рішеннях безпеки та про потенційні переваги керованих послуг безпеки, які можуть надати МСП доступ до передових технологій і досвіду в галузі безпеки [17, с. 46].

Висновки і перспективи подальших досліджень. Таким чином, забезпечення інформаційної безпеки вимагає цілісного підходу, який поєднує технологічні заходи з організаційною політикою і безперервним навчанням персоналу. Шифрування даних, мережеві екрани та системи виявлення вторгнень є важливими технологічними інструментами, які захищають від несанкціонованого доступу та кіберзагроз. Водночас надійна політика безпеки та регулярні навчальні програми гарантують, що працівники отримають усе необхідне для того, щоб зробити свій внесок у забезпечення безпеки своєї організації. Поєднуючи ці методи та засоби, корпорації здатні ефективно захищати свої інформаційні активи в умовах складного та небезпечного кіберсередовища, що постійно ускладнюється.

Реальні кейси показують важливість поєднання технологічних рішень із сильною організаційною політикою та

безперервним навчанням співробітників. Вирішуючи загальні недоліки і займаючи проактивну, адаптивну позицію безпеки, організації можуть краще захистити свої інформаційні мережі від кіберзагроз, що постійно зростають.

Майбутні наукові дослідження можуть стосуватися нових технологій, як-от штучний інтелект і блокчейн, у підвищенні безпеки інформаційних мереж. Цінною інформацією можуть стати дослідження впливу нормативно-правової бази та галузевих стандартів на корпоративні практики кібербезпеки.

Список використаних джерел:

1. Столбовий В. М., Кисленко Д. П. Заходи з підвищення кібербезпеки на державному та корпоративному рівнях в умовах діджиталізації суспільства. *Scientific notes of Lviv University of Business and Law*. 2023. № 37. С. 175-183. DOI: 10.5281/zenodo.8019971

2. Копійка М. В. Стратегічні ризики інформаційної безпеки європейських країн. *Міжнародні та політичні дослідження*. 2019. № 32. С. 85-102. DOI: 10.18524/2304-1439.2019.32.173847

3. Доронін І. М. Цифровий розвиток та національна безпека у контексті правових проблем. *Інформація і право*. 2019. № 1. С. 29-36.

4. Турчак А. В. Основні засади державної політики забезпечення інформаційної безпеки в Україні. *Інвестиції: практика та досвід*. 2019. № 11. С. 123-127. DOI: 10.32702/2306-6814.2019.11.123

5. Мельниченко С. Г. Аналіз стратегічного менеджменту та його вплив на успішність організацій. *Здобутки економіки: перспективи та інновації.* 2024. № 3. URL: https://econp.com.ua/index.php/journal/article/view/19/16 (дата звернення: 31.05.2024).

6. Ревак І. О., Грень Р. Т. Особливості формування безпечного кіберпростору в умовах розвитку цифрової економіки. *Інформаційні технології та економічна безпека.* 2021. № 87 (3 – 4). С. 164 – 169. DOI: 10.37332/2309-1533.2021.3-4.23

7. Остапець А. О., Парасій-Вергуненко І. М. Вплив ризику кіберзлочинності на діяльність технологічних підприємств. *Scientific Notes of Ostroh Academy National University," Economics" Series*. 2024. № 32 (60). С. 37-46. DOI: 10.25264/2311-5149-2024-32(60)-37-46

8. Шульга О. А. Конфіденційність та шахрайство в інтернет-сфері. *Економічний вісник університету*. 2021. № 48. С. 76-91. DOI: 10.31470/2306-546X-2021-48-76-91

9. Курков М. С. Концептуальна модель системи управління фінансами підприємств із застосуванням сучасних інформаційних технологій. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Економіка і управління*. 2019. № 30 (69). С. 142-148. DOI: 10.32838/2523-4803/69-5-25

10. Дименко Р. А. Формування структурно-логічної моделі реалізації комплаєнс-політики у телекомунікаційній галузі. *Ринкова економіка: сучасна теорія і практика управління*. 2019. № 18 (43)). С. 200-216. DOI: 10.18524/2413-9998.2019.3(43).183683

11. Савченко В. А., Степанченко Б. С. Розробка концепції прогнозування початку Ddos атаки на основі дослідження динаміки поведінки еволюційних рівнянь.

Телекомунікаційні та інформаційні технології. 2024. № 1. С. 26-44. DOI: 10.31673/2412-4338.2024.012644

12. Вдовічен А.А., Вдовічена О.Г., Кримська А.О. Цифрова економіка та кібербезпека: аналіз загроз та стратегій захисту в контексті інституціоналізації. *Економіка. Фінанси. Право.* 2024. № 4. С. 135–140. DOI: 10.37634/efp.2024.4.28

13. Ляхович О. О., Оплачко І. О. Економічна безпека та транспарентність підприємств в умовах цифровізації. *Bulletin National University of Water and Environmental Engineering*. 2021. № 2 (94). С. 100-111. DOI: 10.31713/ve2202110

14. Узбек Д. А. Аналіз трансформацій національних економічних інтересів в умовах розвитку інформаційної економіки. *Економічний простір*. 2022. № 182. С. 23-32. DOI: 10.32782/2224-6282/182-3

15. Баглей Р. Р. Особливості корпоративного управління інноваційним розвитком у міжнародних компаніях. *Інноваційна економіка.* 2023. № 3. С. 122-126. DOI: 10.37332/2309-1533.2023.3.16

16. Климчук О. В. Сучасні тренди та глобалізаційні виміри управління інформаційними технологіями і системами в Україні. *Економіка і організація управління*. 2021. № 1 (41). С. 72-85. DOI: 10.31558/2307-2318.2021.1.7

17. Королюк Ю. Г., Чичун В. А. Менеджмент кібербезпеки в системі лояльності покупців. *Вісник Чернівецького тоговельно-економічного інституту.* 2023. Вип. 4 (92). С. 39-53. DOI: 10.34025/2310-8185-2023-4.92.03

References:

1. Stolbovyi, V.M., & Kyslenko, D.P. (2023). Measures to increase cyber security at the state and corporate levels in conditions of digitalization of society. *Scientific Notes of Lviv University of Business and Law,* no. 37, pp. 175-183. DOI: 10.5281/zenodo.8019971 (in Ukr.).

2. Kopyika, M. V. (2019). Strategic risks of information security of European countries. *Mizhnarodni ta politychni doslidzhennia [International and Political Studies],* no. 32, pp. 85-102. DOI: 10.18524/2304-1439.2019.32.173847 (in Ukr.).

3. Doronin, I.M. (2019). Digital development and national security in the context of legal problems. *Informatsiia i pravo [Information and Law],* no. 1, pp. 29-36 (in Ukr.).

4. Turchak, A.V. (2019). Basic principles of the state policy of ensuring information security in Ukraine. *Investytsii: praktyka ta dosvid [Investments: Practice and Experience],* no. 11, pp. 123-127. DOI: 10.32702/2306-6814.2019.11.123 (in Ukr.).

5. Melnychenko, S.H. (2024). Analysis of strategic management and its influence on the success of organizations. *Zdobutky ekonomiky: perspektyvy ta innovatsii [Economic Achievements: Perspectives and Innovations],* no. 3. URL: https://econp.com.ua/index.php/journal/article/view/19/16 (Accessed May 31, 2024) (in Ukr.).

6. Revak, I.O., & Hren, R.T. (2021). Peculiarities of the formation of a safe cyberspace in the conditions of the development of the digital economy. *Informatsiini tekhnolohii ta ekonomichna bezpeka [Information Technologies and Economic Security],* no. 87 (3-4), pp. 164-169. DOI: 10.37332/2309-1533.2021.3-4.23 (in Ukr.).

7. Ostapets, AO., & Parasiy-Vergunenko, I.M. (2024). The influence of the risk of cybercrime on the activity of technological enterprises. *Scientific Notes of Ostroh Academy National University, "Economics" Series,* no. 32 (60), pp. 37-46. DOI: 10.25264/2311-5149-2024-32(60)-37-46 (in Ukr.).

8. Shulha, O.A. (2021). Confidentiality and fraud in the Internet sphere. *Ekonomichnyi Visnyk Universytetu [University Economic Bulletin],* no. 48, pp. 76-91. DOI: 10.31470/2306-546X-2021-48-76-91 (in Ukr.).

9. Kurkov, M.S. (2019). Conceptual model of the financial management system of enterprises with the use of modern information technologies. *Vcheni zapiski Tavriiskoho Natsionalnoho Universytetu imeni VI Vernadskoho. Seriia: Ekonomika i Upravlinnia [Scientific Notes of V.I. Vernadsky Taurida National University. Series: Economics and Management],* no. 30 (69), pp. 142-148. DOI: 10.32838/2523-4803/69-5-25 (in Ukr.)

10. Dymenko, R.A. (2019). Formation of a structural and logical model of compliance policy implementation in the telecommunications industry. *Rynkova ekonomika: suchasna teoriia i praktyka upravlinnia [Market Economy: Contemporary Theory and Management Practice],* no. 18 (43), pp. 200-216. DOI: 10.18524/2413-9998.2019.3(43).183683 (in Ukr.).

11. Savchenko, V.A., & Stepanchenko, B.S. (2024). Development of the concept of predicting the beginning of a Ddos attack based on the study of the dynamics of the behavior of evolutionary equations. *Telekomunikatsiini ta Informatsiini Tekhnolohii [Telecommunications and Information Technologies],* no. 1, pp. 26-44. DOI: 10.31673/2412-4338.2024.012644 (in Ukr.).

12. Vdovichen, A.A., Vdovichena, O.G., Krymska, A.O. (2024). Digital economy and cybersecurity: analysis of threats and defense strategies in the context of institutionalization. *Ekonomika. Finansy. Pravo [Economics. Finances. Law],* no. 4, pp. 135–140. DOI: 10.37634/efp.2024.4.28 (in Ukr.).

13. Liakhovych, O.O., & Oplachko, I.O. (2021). Economic security and transparency of enterprises in conditions of digitalization. *Bulletin National University of Water and Environmental Engineering,* no. 2 (94), pp. 100-111. DOI: 10.31713/ve2202110 (in Ukr.).

14. Uzbek, D.A. (2022). Analysis of transformations of national economic interests in the context of information economy development. *Ekonomichnyi prostir [Economic Space],* no. 182, pp. 23-32.DOI: https:10.32782/2224-6282/182-3 (in Ukr.).

15. Bahlei, R.R. (2023). Peculiarities of corporate management of innovative development in international companies. *Innovatsiina ekonomika [Innovative Economy],* no. 3, pp. 122-126. DOI: https://doi.org/10.37332/2309-1533.2023.3.16 (in Ukr.).

16. Klymchuk, O.V. (2021). Modern trends and globalization dimensions of management of information technologies and systems in Ukraine. *Ekonomika i orhanizatsiia upravlinnia [Economics and Management Organization],* no. 1 (41), pp. 72-85. DOI: 10.31558/2307-2318.2021.1.7 (in Ukr.).

17. Koroliuk, Y.G., Chychun, V.A. (2023). Cyber security management in the buyer loyalty system. *Visnyk Chernivetskoho torhovelno-ekonomichnoho instytutu [Bulletin of the Chernivtsi Trade and Economic Institute],* issue 4 (92), pp. 39-53. DOI: 10.34025/2310-8185-2023-4.92.03 (in Ukr.).