КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1073
УДК 004.056.5:004.056.55

Задворний Дмитро Сергійович
магістрант кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0009-0005-5163-1472
dszadvornyi.fitm24m@kubg.edu.ua

Козачок Валерій Анатолійович
кандидат технічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0003-0072-2567
v.kozachok@kubg.edu.ua

Черевик В'ячеслав Михайлович
кандидат технічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-2735-5341
v.cherevyk@kubg.edu.ua

Бодненко Дмитро Миколайович
кандидат педагогіних наук, доцент,
доцент кафедри математики і фізики
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0001-9303-6587
d.bodnenko@kubg.edu.ua

Добришин Юрій Євгенович
кандидат технічних наук, доцент,
Національна академія Служби безпеки України, Київ, Україна
ORCID: 0000-0003-2473-9507
ydobryshyn@gmail.com

МЕТОДИ ТА ЗАСОБИ ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТИПОВОГО ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Анотація. Ця робота висвітлює проблему розробки комплексної системи захисту інформації (КСЗІ) для типового об'єкта інформаційної діяльності в умовах зростання рівня кіберзагроз та посилення вимог до інформаційної безпеки. В ній представлено аналіз сучасних тенденцій кіберінцидентів в Україні та світі, досліджено нормативно-правову базу, що регламентує створення КСЗІ, а також розглянуто міжнародні стандарти ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 і рекомендації NIST. Розкрито методологію побудови КСЗІ, зокрема класифікацію об'єктів інформаційної діяльності, етапи аналізу загроз, моделювання порушника та формування політики безпеки. Представлено результати розробки моделі КСЗІ для типового об'єкта інформаційної діяльності: аналіз інформаційних потоків, моделі загроз і порушників, оцінка рівня захищеності, формування профілю безпеки та вибір технічних, криптографічних і організаційних заходів. Оцінено ефективність впровадження, визначено очікувані вигоди, включно зі зниженням ризиків витоку, підвищенням стійкості бізнес-процесів та відповідністю міжнародним стандартам. Висновки містять рекомендації щодо підвищення рівня кіберстійкості та перспективи подальших досліджень.

Ключові слова: інформаційна безпека; кіберзагроза; об'єкт інформаційної діяльності; комплексна система захисту інформації; модель загроз; модель порушника; криптографічний захист; технічні засоби захисту.

ВСТУП

Стрімка цифровізація, розвиток IT-інфраструктури та глобалізація інформаційного простору зумовлюють зростання вразливості організацій до кіберзагроз. Дані стали одним із ключових активів підприємств, а від їхнього захисту залежить стабільність функціонування, економічна ефективність та конкурентоспроможність. Паралельно з розвитком технологій зростає кількість та складність атак – від фішингу й соціальної інженерії до APT-кампаній та шкідливого програмного забезпечення нового покоління [1; 2].

В Україні ця проблема має особливу актуальність через системні кібератаки на державні реєстри, органи влади та критичну інфраструктуру, що підтверджується статистикою Державної служби спеціального зв'язку та захисту інформації (звіти CERT-UA) та міжнародних аналітичних центрів [3].

У таких умовах забезпечення інформаційної безпеки вимагає впровадження комплексних систем захисту інформації (КСЗІ), які враховують вимоги національного законодавства щодо захисту інформації, кібербезпеки та міжнародних стандартів ISO/IEC 27001, що поєднують правові, організаційні, технічні та криптографічні заходи [4; 5; 6].

Постановка проблеми. Сучасні кібератаки характеризуються високою складністю, використанням прихованих методів проникнення, що описані у дослідженнях APT-кампаній [2].

Особливий ризик становлять:

1. APT-атаки, що орієнтовані на довготривале проникнення.
2. Шкідливі програми-вимагачі (ransomware).
3. Атаки на ланцюги постачання.
4. Засоби соціальної інженерії.
5. Атаки на промислові системи (SCADA/OT).

Проблемою є недостатнє впровадження технічних та організаційних заходів на підприємствах, а також низький рівень кіберкультури персоналу, на що звертають увагу міжнародні аналітики, зокрема рекомендації NIST CSF 2.0 [7]. Відсутність системного підходу до захисту призводить до катастрофічних наслідків у разі інциденту.

Аналіз останніх досліджень і публікацій. Проблему інформаційної безпеки та побудови КСЗІ досліджували численні українські й міжнародні автори. У світовій літературі питання інформаційної безпеки детально розглянуті в роботах Bishop [1], Whitman & Mattord [8], Stallings [9]. Криптографічні засоби та принципи побудови захищених систем ґрунтовно описані в «Handbook of Applied Cryptography» [10]. Проблеми виявлення вторгнень, IDS/IPS та аналізу атак описані в NIST SP 800-94 [11]. Ризик-орієнтований підхід, який є основою міжнародних стандартів ISO/IEC 27005 [12], активно використовується у дослідженнях Rid & Buchanan [13], що розглядають проблеми атрибуції атак.

Українські дослідники зосереджуються на адаптації міжнародних норм до національного законодавства, зокрема через нормативно правові документита результати наукових досліджень [4, 5, 14, 15, 16, 17 , 18, 19]. Разом з тим, недостатньо висвітленими залишаються питання адаптації КСЗІ для типових підприємств малого та середнього бізнесу, інтеграції сучасних систем SOC/SIEM/SOAR, також DevSecOps-підходів, а офіційні звіти CERT-UA [3] надають актуальну статистику кібератак.

Мета статті. Метою статті є розробка моделі КСЗІ для типового об'єкта інформаційної діяльності, що відповідає вимогам міжнародних стандартів ISO/IEC

27001 [6], ISO/IEC 27005 [12] та національних нормативно-правових актів України [4, 5, 14, 15].

Для досягнення мети визначено завдання:

1. Проаналізувати сучасні кіберзагрози та нормативно-правові вимоги;
2. Вивчити класифікацію об'єктів інформаційної діяльності;
3. Дослідити методологію створення КСЗІ;
4. Розробити модель КСЗІ для типового об'єкта інформаційної діяльності;
5. Оцінити ефективність запропонованих заходів.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Теоретична база ґрунтується на міжнародних стандартах ISO/IEC 27000 [6; 12], рекомендаціях NIST [7], ризик-орієнтованому підході, концепції Zero Trust, принципах багаторівневого захисту (defense in depth) та сучасних моделях кіберзагроз [1; 8]. Ключовими поняттями є конфіденційність, цілісність, доступність, підзвітність, стійкість.

МЕТОДИКА ДОСЛІДЖЕННЯ

Методологія передбачає:

1. Аналіз активів і класифікацію інформаційних потоків;
2. Моделювання порушника (внутрішній/зовнішній);
3. Моделювання загроз (методики STRIDE/DREAD);
4. Оцінку ризиків (ISO/IEC 27005);
5. Формування політики безпеки;
6. Вибір технічних, криптографічних та організаційних заходів;
7. Оцінку ефективності (метрики MTTD, MTTR, SLA, CVSS).

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

1. Аналіз інформаційної системи підприємства:

Типовий об'єкт інформаційної діяльності має (таблиця 1):

1) Локальну мережу з сегментацією.
2) Серверні ресурси (AD, файлові, поштові сервери).
3) Робочі станції.
4) VPN-доступ.
5) Бази даних.
6) Зовнішні сервіси.

Таблиця 1

Аналіз інформаційної системи підприємства

Актив / компонент	Опис	Значимість	Потенційні ризики
Локальна мережа з сегментацією	VLAN, відокремлені зони, доступ через комутатори	Висока	Пересування зловмисника між сегментами

Сервери (AD, файловий, поштовий)	Централізовані служби підприємства	Дуже висока	Компрометація домену, втрата даних
Робочі станції	Користувацькі ПК, офісні програми	Середня	Вразливість до фішингу, malware
VPN-доступ	Підключення співробітників та підрядників	Висока	Brute-force, компрометація облікових записів
Бази даних	Персональні, фінансові та комерційні відомості	Дуже висока	SQLi, витік через внутрішні помилки
Зовнішні сервіси	Хмарні сервіси, сторонні API	Висока	Компрометація через сторонніх підрядників

Ідентифіковано основні активи: персональні дані працівників, фінансова інформація, конфіденційні документи, журнали подій.

2. Модель порушника:

Порушники діляться на два типа (таблиця 2):

1. Зовнішні порушники (аутсайдери): хакерські угруповання, конкурентні структури, фінансово мотивовані кіберзлочинці.
2. Внутрішні порушники (інсайдери): співробітники, підрядники, зловмисники з доступом.

Таблиця 2

Модель порушника

Тип порушника	Мотивація	Рівень ресурсів	Типові атаки	Потенційні наслідки
Зовнішні кіберзлочинці	Фінансова вигода, вимагання	Середній/високий	Фішинг, malware, SQL-injection	Компрометація даних, параліч сервісів
Внутрішні користувачі	Помилки, недбалість	Низький	Слабкі паролі, передача даних у незахищених каналах	Витік, порушення цілісності баз
Інсайдери з привілеями	Помста, зловживання	Високий	Маніпуляції з доступами, видалення або модифікація даних	Повний контроль над інфраструктурою
Підрядники / сторонні	Непрямий вплив, компрометація	Середній	Злам VPN, доступ через API	Вразливість ланцюга постачання
APT-групи / державні	Шпигунство, саботаж	Дуже високий	Нульові вразливості, тривале проникнення	Значні операційні втрати, зупинка бізнесу

3. Модель загроз:

Загрози класифіковано за групами (таблиця 3):

1) Несанкціонований доступ.
2) Втручання у мережеву інфраструктуру.
3) Підміна даних.
4) Перехоплення трафіку.
5) Людський фактор.
6) Атаки на сервіси (DoS, SQLi, XSS, MITM).

Таблиця 3

Модель загроз

Група загроз	Приклади атак / сценаріїв	Ймовірність	Потенційний вплив
Несанкціонований доступ	Фішинг, викрадення облікових записів, brute force, доступ через хмарні сервіси	Висока	Високий
Втручання у мережеву інфраструктуру	Компрометація маршрутизаторів, VLAN-атаки, використання відкритих портів	Середня	Високий
Підміна даних	SQL-injection, зміна параметрів транзакцій, модифікація API-запитів	Середня	Високий
Перехоплення трафіку	MITM, прослуховування незашифрованих каналів, атак на VPN	Середня	Значний
Людський фактор	Помилки персоналу, слабкі паролі, випадкове видалення чи розголошення даних	Висока	Середній
Атаки на сервіси	DoS/DDoS, XSS, експлуатація вразливих API, атаки на веб-сервіси	Середня	Високий

4. Оцінка рівня захищеності:

Виявлено критичні вразливості (табдиця 4):

1) Відсутність DLP.
2) Недостатні засоби багатофакторної автентифікації.
3) Відсутність SIEM.
4) Слабка сегментація мережі.
5) Відсутність плану реагування на інциденти.

Таблиця 4

Оцінка рівня захищеності

Вразливість	Опис	Рівень ризику	Потенційні наслідки
Відсутність DLP	Немає захисту від витоку даних	Високий	Витік персональних і комерційних даних
Відсутність MFA	Використання однофакторної автентифікації	Високий	Компрометація доступів, злам систем
Відсутність SIEM	Немає централізованого моніторингу	Високий	Запізніле виявлення атак
Слабка сегментація мережі	Нечітке розмежування зон	Середній	Латеральний рух зловмисника
Немає плану IRP	Не встановлені процедури реагування	Середній	Довготривалі простої при інцидентах

6. Програмно-технічні заходи захисту:

Для захисту типового обєкта інформаційної діяльності запропоновані наступні прграмно-технічні засоби захисту інформації (таблиця 5):

1) Міжмережеві екрани нового покоління (NGFW).
2) IDS/IPS.
3) SIEM із кореляцією подій.
4) DLP для контролю витоків.
5) PAM та MFA.
6) Сегментація мережі VLAN.
7) Резервне копіювання за схемою 3-2-1.

Таблиця 5

Програмно-технічні заходи захисту

Засіб / технологія	Призначення	Ключовий ефект
NGFW	Контроль трафіку, IDS/IPS, фільтрування	Зниження атак на периметр
IDS/IPS	Виявлення атак	Раннє виявлення вторгнень
SIEM	Кореляція подій	Скорочення часу реагування
DLP	Захист від витоків	Контроль каналів передачі даних
PAM	Контроль привілейованих доступів	Усунення інсайдерських загроз
MFA	Сильна автентифікація	Захист від компрометації акаунтів

VLAN-сегментація	Розмежування мереж	Зменшення впливу атаки
Резервне копіювання 3-2-1	Захист даних	Гарантоване відновлення після атаки

6. Криптографічні заходи захисту (таблиця 6)**:**

1) Шифрування дисків.
2) Шифрування каналів (TLS, IPsec).
3) КЕП/ЕЦП.
4) Хешування за стандартами SHA-3.
5) HSM для зберігання ключів.

Таблиця 6

Криптографічні заходи захисту

Засіб	**Призначення**	**Практичний ефект**
Шифрування дисків	Захист даних на ПК/ноутбуках	Унеможливлення доступу при викраденні
TLS / IPsec	Захист каналів	Конфіденційність трафіку
КЕП/ЕЦП	Підпис документів	Захист цілісності документів
SHA-3	Хешування	Стійкість до колізій
HSM	Захист ключів	Високий рівень безпеки криптографії

7. Організаційні заходи захисту (таблиця 7):

1) Положення про політику безпеки.
2) Навчання персоналу.
3) Обмеження доступу за ролями (RBAC).
4) Журналювання та аудит.
5) План реагування на інциденти (IRP).
6) Політика резервного копіювання.
7) Періодичний аудит безпеки.

Таблиця 7

Організаційні заходи захисту

Захід	**Призначення**	**Практичний ефект**
Політика інформаційної безпеки	Регламентація процесів	Зниження хаотичних дій персоналу
Навчання персоналу	Підвищення компетенції	Зменшення фішинг-інцидентів

RBAC	Контроль доступу	Мінімізація прав і ризиків
Аудит і журналювання	Контроль активності	Виявлення підозрілих дій
План IRP	Реагування на інциденти	Скорочення простоїв
Політика бекапів	Відновлення даних	Сталість бізнес-процесів
Періодичний аудит	Перевірка системи	Виявлення слабких місць

8. Оцінка ефективності захисту інформації (таблиця 8):
Використано показники:

1) Зниження ризику витоку даних на 60 %;
2) Зменшення часу виявлення інцидентів (MTTD) у 4 рази;
3) Скорочення MTTR до 2 годин;
4) Відповідність ISO/IEC 27001;
5) Готовність до проходження державної експертизи.

Таблиця 8

Оцінка ефективності КСЗІ

Показник	**Результат**	**Джерело ефекту**
Зниження ризику витоку	–60%	Впровадження DLP, RBAC
MTTD	Зменшено у 4 рази	SIEM, IDS/IPS
MTTR	Скорочено до 2 годин	IRP, автоматизація
Відповідність ISO 27001	Досягнуто	Політики, технічні заходи
Готовність до експертизи ДССЗЗІ	Досягнуто	Комплексність моделі КСЗІ

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті наведено модель побудови КСЗІ для типового об’єкта інформаційної діяльності. Проведено аналіз загроз, моделювання порушника, оцінку вразливостей та розроблено набір технічних, криптографічних і організаційних заходів. Запропонована модель КСЗІ відповідає вимогам ISO/IEC 27001, ISO/IEC 27005, NIST SP 800-94, NIST CSF 2.0 та нормативним актам України.

Перспективи подальших досліджень:

1. Інтеграція штучного інтелекту в системи кіберзахисту;
2. Впровадження постквантової криптографії;
3. Використання Zero Trust Architecture;
4. Автоматизація реагування через SOAR;
5. Підвищення кіберграмотності персоналу.

Впровадження запропонованої КСЗІ забезпечує значне підвищення стійкості до кіберзагроз та відповідність національним і міжнародним стандартам.

ПОДЯКА

Результати наукових досліджень були виконані в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№ 0122U200483, КСУБГ, м. Київ).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bishop, M. (2019). *Computer security: Art and science*. Addison-Wesley.
2. Chen, T. (2014). Advances in persistent threats. *IEEE Security & Privacy, 12*(3), 16–25. https://doi.org/10.1109/MSP.2014.51
3. CERT-UA. (2024). *Operational report on cyberattacks in the first half of 2024*. https://cert.gov.ua
4. Verkhovna Rada of Ukraine. (2010). *Law of Ukraine "On Personal Data Protection" No. 2297-VI*. https://zakon.rada.gov.ua
5. Verkhovna Rada of Ukraine. (2017). *Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" No. 2163-VIII*. https://zakon.rada.gov.ua
6. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.
7. National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0*. https://www.nist.gov/cyberframework
8. Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.
9. Stallings, W. (2022). *Network security essentials*. Pearson.
10. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2019). *Handbook of applied cryptography*. CRC Press.
11. Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (NIST Special Publication 800-94). National Institute of Standards and Technology.
12. International Organization for Standardization. (2022). *ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on information security risk management*. ISO.
13. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382
14. Derzhspetszviazok of Ukraine. (2022). *Methodological recommendations on building comprehensive information security systems*. DSSZZI.
15. ND TZI 3.7-003-2023. (2023). *The procedure for carrying out work on creating a comprehensive information protection system in information and telecommunications systems*.
16. Kozachok, V. A. (2014). Conceptual principles for creating comprehensive information protection systems in information and telecommunications systems. *Zviazok: Collection of Scientific Works*, 3(109), 8–13.
17. Kozachok, V. A., & Kovalenko, Y. B. (2015). Features of building complex information protection systems in distributed corporate networks. *Modern Information Protection*, 1, 41–47.
18. Kozachok, V. A., Kyrychok, R. V., Skladannyi, P. M., Buryachok, V. L., & Gulak, G. M. (2016). Problems of ensuring control of corporate network security and ways to solve them. *Scientific Notes of the Ukrainian Research Institute of Communications, 3*(43), 48–61.
19. Gulak, G. M., Kozachok, V. A., Skladannyi, P. M., Bondarenko, M. O., & Vovkotrub, B. V. (2017). Personal data protection systems in modern information and telecommunication systems. *Modern Information Security*, 2(30), 65–71.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Dmytro Zadvornyi
student of the Department of Information and Cybersecurity named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0009-0005-5163-1472
dszadvornyi.fitm24m@kubg.edu.ua

Valeriy Kozachok
PhD, Associate Professor,
Associate Professor of the Department of Information and
Cybersecurity named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0003-0072-2567
v.kozachok@kubg.edu.ua

Vyacheslav Cherevyk
PhD, Associate Professor,
Associate Professor of the Department of Information and
Cybersecurity named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-2735-5341
v.cherevyk@kubg.edu.ua

Dmytro Bodnenko
PhD, Associate Professor
Associate Professor at the Department of Mathematics and Physics
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0001-9303-6587
d.bodnenko@kubg.edu.ua

Yurii Dobryshyn
PhD, Associate Professor,
National Academy of the Security Service of Ukraine, Kyiv, Ukraine
ORCID: 0000-0003-2473-9507
ydobryshyn@gmail.com

METHODS AND MEANS OF BUILDUNG A COMPREHENSIVE INFORMATION SECURITY SYSTEM FOR A TYPICAL INFORMATION ACTIVITY OBJECT

Abstract. This work highlights the problem of developing a comprehensive information protection system (CIPS) for a typical information activity object in the context of increasing cyber threats and increasing requirements for information security. It presents an analysis of current trends in cyber incidents in Ukraine and the world, examines the regulatory framework governing the creation of CIPS, and also considers international standards ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and NIST recommendations. The methodology for building CIPS is disclosed, in particular, the classification of information activity objects, stages of threat analysis, modeling of the intruder and the formation of a security policy. The results of developing a CIPS model for a typical enterprise are presented: analysis of information flows, threat and intruder models, assessment of the level of security, formation of a security profile and selection of technical, cryptographic and organizational measures. The effectiveness of the implementation was assessed, and the expected benefits were identified, including reduced risk of leakage, increased business process resilience, and compliance with international standards. The conclusions include recommendations for improving cyber resilience and prospects for further research.

Keywords: information security; cyber threats; object of information activity; comprehensive information protection system; threat model; intruder model; cryptographic protection; technical means of protection.

1. Bishop, M. (2019). *Computer security: Art and science*. Addison-Wesley.
2. Chen, T. (2014). Advances in persistent threats. *IEEE Security & Privacy, 12*(3), 16–25. https://doi.org/10.1109/MSP.2014.51
3. CERT-UA. (2024). *Operational report on cyberattacks in the first half of 2024*. https://cert.gov.ua
4. Verkhovna Rada of Ukraine. (2010). *Law of Ukraine "On Personal Data Protection" No. 2297-VI*. https://zakon.rada.gov.ua
5. Verkhovna Rada of Ukraine. (2017). *Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" No. 2163-VIII*. https://zakon.rada.gov.ua
6. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.
7. National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0*. https://www.nist.gov/cyberframework
8. Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.
9. Stallings, W. (2022). *Network security essentials*. Pearson.
10. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2019). *Handbook of applied cryptography*. CRC Press.
11. Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (NIST Special Publication 800-94). National Institute of Standards and Technology.
12. International Organization for Standardization. (2022). *ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on information security risk management*. ISO.
13. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382
14. Derzhspetszviazok of Ukraine. (2022). *Methodological recommendations on building comprehensive information security systems*. DSSZZI.
15. ND TZI 3.7-003-2023. (2023). *The procedure for carrying out work on creating a comprehensive information protection system in information and telecommunications systems*.
16. Kozachok, V. A. (2014). Conceptual principles for creating comprehensive information protection systems in information and telecommunications systems. *Zviazok: Collection of Scientific Works*, 3(109), 8–13.
17. Kozachok, V. A., & Kovalenko, Y. B. (2015). Features of building complex information protection systems in distributed corporate networks. *Modern Information Protection*, 1, 41–47.
18. Kozachok, V. A., Kyrychok, R. V., Skladannyi, P. M., Buryachok, V. L., & Gulak, G. M. (2016). Problems of ensuring control of corporate network security and ways to solve them. *Scientific Notes of the Ukrainian Research Institute of Communications, 3*(43), 48–61.
19. Gulak, G. M., Kozachok, V. A., Skladannyi, P. M., Bondarenko, M. O., & Vovkotrub, B. V. (2017). Personal data protection systems in modern information and telecommunication systems. *Modern Information Security*, 2(30), 65–71.