DOI: https://doi.org/10.58253/2078-1628-2024-2(32)-030

УДК 004.056.5 (075.8)
JEL C80, C89, L86

Денис Анатолійович ТАРАСЕНКО
кандидат технічних наук,
доцент кафедри права та інформаційної справи,
Приватний заклад вищої освіти
«Східноєвропейський університет імені Рауфа Аблязова»,
м. Черкаси, Україна
https://orcid.org/0009-0006-0582-1619
denis.tarasenko@gmail.com

СУЧАСНІ ІНСТРУМЕНТИ ЗАХИСТУ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Анотація. *Цифровізація суспільства, розвиток сучасних технологій формують нові вимоги до отримання та збереження інформації. У статті досліджено дефініцію «інформаційні системи» та основні аспекти їхнього функціонування, визначено роль у збереженні й обробці даних. Значну увагу приділено питанням безпеки даних, які є ключовими елементами сучасних інформаційних систем. Проаналізовано загрози, що впливають на конфіденційність, цілісність та доступність даних, а також визначено причини та наслідки враження даних. У досліджені визначено основні методи та технології захисту даних, такі як: шифрування, автентифікація, копіювання тощо. Наведено види захисту даних та обґрунтовано доцільність розробки стратегії захисту даних із зазначенням її основних елементів та етапів реалізації. Автором запропоновано напрями вдосконалення процесів захисту баз даних, які передбачають: інтеграцію сучасних систем виявлення вторгнень, упровадження політик доступу, підвищення обізнаності персоналу та забезпечення кіберзахисту. Особливої актуальності, за визначенням автора, набирає комплексний підхід забезпечення безпеки даних у контексті швидкого розвитку інформаційних технологій і зростання обсягів цифрової інформації.*

Ключові слова: *дані, загрози, захист, інформаційні системи, інформація, кіберзагроза, конфіденційність, програмне забезпечення, стратегія, технології, шифрування.*

Постановка проблеми. Сучасні реалії вимагають побудови новітніх форм взаємодії бізнесу. Інтенсивний розвиток технологій, з одного боку – полегшує управління бізнесом та співпрацю з контрагентами, з іншого – призводить до зростання зовнішніх загроз щодо втрати даних. Наразі, усе більше підприємств використовують сучасні інформаційні системи та технології з метою оптимізації виробничих процесів та управління. Адже, сучасні інформаційні системи відіграють ключову роль у збиранні, зберіганні та обробці даних. Проте їхнє використання супроводжується значними викликами щодо захисту інформації від зовнішніх та внутрішніх загроз.

Захист даних поєднує стратегічні та процедурні механізми, які запроваджуються з метою захисту конфіденційності, доступності та цілісності прихованих даних. Відтак, в умовах швидкого зростання генерації та зберігання даних, надійність захисту даних є першочерговим завданням. Основна мета якого полягає, не лише в захисті конфіденційної інформації, а й у забезпеченні її доступності та надійності, таким чином зберігаючи довіру та відповідність операціям, орієнтованим на дані.

Основною проблемою сьогодення, у забезпечені безпеки даних, є вразливість до кібератак в умовах цифровізації, адже відбувається постійне зростання обсягів даних, а сучасні інформаційні системи стають дедалі складнішими, інтегруючи хмарні сервіси, Інтернет речей (IoT), штучний інтелект (AI) тощо. Дослідники, сучасного ринку інформаційних систем, серед основних причин збільшення загроз для збереження даних, виокремлюють: дефіцит експертів у сфері кібербезпеки; недостатню обізнаність користувачів; правові «провали» та використання застарілих систем, які не підтримують сучасні засоби захисту.

Відповідно, перелічені проблеми призводять до фінансових втрат, витоку персональних даних та втрати репутації, що призводить до юридичної відповідальності тощо. Відтак, захист даних та використання інформаційних систем є нагальною проблемою у системі управлінні.

Аналіз останніх досліджень і публікацій. Питання розвитку інформаційних систем та захисту даних постійно досліджуються та обговорюються вченими та фахівцями з усього світу. Так, Клод Шеннон, у

1948 році, запропонував основи теорії інформації, що є базою для побудови сучасних інформаційних систем [5]. Алан Тьюрінг, свого часу, сформував концепцію алгоритмів і автоматичних обчислювальних машин, що заклало основу для створення інформаційних систем [7].

Вітчизняні дослідники також зробили значний анесок у розвиток інформаційних систем. Так, Ю. Зарахович, дослідник у сфері математичного моделювання та захисту даних, присвятив свої дослідження питанням побудови захищених систем обробки інформації. М. Амосов займався моделюванням інформаційних процесів у біологічних системах, що вплинуло на розвиток інформаційних систем. Відомий український фахівець із криптографії та інформаційної безпеки, О.Кириченко розробив криптографічні алгоритми й систему захисту інформації.

Отже, інформаційна система – це сукупність програмного, апаратного забезпечення, персоналу, організаційних процедур та інформаційних ресурсів, яка забезпечує збір, зберігання, обробку, передачу та відображення інформації.

Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» інформаційну (автоматизовану) систему визначено, «як організаційно-технічну систему, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів» [13]. Положенням «Про технічний захист інформації» передбачено, що «Інформаційна система – автоматизована система, комп'ютерна мережа або система зв'язку» [14]. Інформаційна система, як організаційно-технічна система обробки інформації за допомогою технічних і програмних засобів, визначена Порядком взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах [12].

Таким чином, Н. Георгіаді вважав, що інформаційна система – це «сукупність різних видів інформації, суб’єктів інформаційної діяльності, інформаційних технологій та зв’язків між ними» [9]. На думку В. Пономаренка, метою інформаційної системи є нагромадження, передавання, збереження, оброблення, узагальнення та конкретизація інформації для використання управлінським апаратом [11].

У той час, Г. Пурій зазначає, що «в основі інформаційних систем лежать інформаційні моделі, які описують та регламентують інформаційні потоки в управлінні за допомогою певних алгоритмів і процедур фіксування й обробки інформації» [15].

Р. Яценко та І.Ніколаєв стверджують, що «компонентами інформаційної системи є база даних, концептуальна схема й інформаційний процесор, які утворюють разом систему зберігання і маніпулювання даними» [17].

Також автори зазначили, що «з технічної точки зору інформаційна система може бути визначена як набір взаємозалежних елементів, які збирають, обробляють, зберігають і розподіляють інформацію з метою підтримки процесу прийняття управлінських рішень та забезпечення механізму управління організацією в цілому» [17].

Використання інформаційних систем призводить до потреби захисту даних у системах. У 1976 році, Вітфілд Діффі та Мартін Геллман розробили метод асиметричного шифрування в захисті даних та криптографії [1]. Основи цифрових підписів стали доробком Ральфа Меркла, який відомий роботою над криптографічними хеш-функціями [16]. Шифруванню та кібербезпеці присвячено дослідження Брюса Шнайєра [4].

Питанням захисту даних присвячено дослідження Міхаеля Рабіна, співавтора алгоритму шифрування RSA. Шаї Халеві розробив сучасні методи гомоморфного шифрування, яке дозволяє працювати з зашифрованими даними. Сільвія Оссела досліджує питання кібербезпеки та впровадження штучного інтелекту для захисту інформаційних систем.

Разом тим існує низка правових актів, які забезпечують захист даних. Так, вимоги до системи управління інформаційною безпекою описані Міжнародним стандартом створення, впровадження, підтримки та вдосконалення системи управління інформаційною безпекою ISO/IEC 27001:2013 [2].

Захист персональних даних громадян ЄС і ЄЕЗ визначено Європейським регламентом про захист даних (GDPR), який встановлює вимоги для організацій у всьому світі щодо конфіденційності [3].

Вітчизняні дослідники досліджували захист інформації в мережевих базах даних, шифрування та контроль доступу, протидію кіберзагрозам у системі управління базами даних, вразливості SQL, розподілення бази даних, методи моніторингу та аудиту захисту даних, питання захист даних у Big Data та хмарних середовищах, застосування блокчейн-технологій тощо.

Науковці зробили вагомий внесок у розвиток захисту баз даних, досліджуючи сучасні загрози, інноваційні методи захисту та рекомендації щодо безпеки даних у різних галузях. Результати їхніх досліджень дали змогу розвинути сучасні підходи до розробки інформаційних систем і захисту даних, які використовуються у різних галузях. Проте, зростаючі темпи кіберзлочинів

вимагають розробки нових та удосконалення наявних інструментів захисту даних.

Формулювання мети статті. Метою статті є аналіз ключових аспектів використання інформаційних систем та забезпечення захисту даних.

Відповідно до поставленої мети, у статті досліджено дефініцію «інформаційні системи» та здійснено її класифікацію. Вивчено функції систем та розкрито зміст сучасних ризиків захисту даних. Проаналізовано найбільш поширені загрози та виявлено вразливість інформаційних систем. Досліджено сучасні технології та стандарти захисту, визначено ефективні стратегії інтеграції сучасних засобів захисту.

Методи і методологія здійснення дослідження. За допомогою системного аналізу, визначено сучасний інструментарій захисту даних у структурі інформаційних систем, ідентифіковано основні компоненти системи захисту, їхню взаємодію та вплив на ефективність систем. У процесі порівняння різних інструментів захисту даних, таких як антивірусні програми, міжмережеві екрани, криптографічні технології, системи багатофакторної аутентифікації було застосовано методи порівняльного аналізу. Оцінка ефективності наявних інструментів захисту та виявлення їхнього обмеження в реальних умовах роботи інформаційних систем виконана за допомогою критичного аналізу.

Виклад основного матеріалу й отриманих наукових результатів. В умовах сьогодення захист даних є критичним аспектом функціонування сучасних інформаційних систем. Основи цих понять охоплюють організаційні, технічні, правові та процедурні заходи, спрямовані на забезпечення безпеки інформації. Основними компонентами будь-якої інформаційної системи є апаратне та програмне забезпечення, користувачі та правила й процеси, які регулюють роботу всієї системи. Відтак, постає питання забезпечення захисту даних, який являє собою комплекс заходів спрямованих на забезпечення конфіденційності, цілісності й доступності інформації в межах інформаційної системи. Наразі, у світовій практиці, існує безліч методів захисту даних, основні з яких представлено на рис. 1.

Зокрема, основним методом захисту даних є шифрування – процес перетворення даних у код, який можуть прочитати лише авторизовані сторони [5]. Виокремлюють: симетричне (використання одного ключа для шифрування та дешифрування даних), наскрізне (дані залишаються захищеними з моменту їх надсилання до отримання одержувачем) та асиметричне (використовує два ключі: один для шифрування даних, а інший – для їхнього

дешифрування) шифрування. Використання антивірусного програмного забезпечення сприяє виявленню та видаленню шкідливого програмного забезпечення пристроїв. Брандмауери забезпечують контроль програм, дозволяючи обмежувати або дозволяти певним програмам доступ до даних. Значна кількість сучасних брандмауерів поєднують функції виявлення та запобігання вторгненням, які можуть ідентифікувати та блокувати потенційні загрози до того, як вони досягнуть системи [10].

Методи захисту даних		
Організаційні	***Технічні***	***Правові***
- шифрування інформації; - використання антивірусного програмного забезпечення; - брандмауери та системи виявлення вторгнень; - резервне копіювання.	- розробка політик інформаційної безпеки; - обмеження доступу до інформації; - навчання персоналу правилам безпеки.	- дотримання законодавства у сфері захисту персональних даних; - упровадження стандартів інформаційної безпеки.

Рис. 1. Класифікація методів захисту даних

Джерело: узагальнено та побудовано автором.

Резервне копіювання дозволяє підприємствам швидко відновлюватися після втрати даних, мінімізуючи час простою та знижуючи ризик остаточної втрати даних. Крім того, рішення для резервного копіювання та відновлення також можуть забезпечити додатковий рівень безпеки, оскільки їх можна використовувати для відновлення даних на більш ранній момент часу, ефективно скасовуючи будь-які неавторизовані зміни чи видалення [5].

Інформаційна безпека та контроль доступу сприяють обмеженню доступу до конфіденційної інформації неавторизованим користувачам. Цього можна досягти за допомогою паролів, багатофакторної автентифікації та рольового контролю доступу. Ці методи гарантують, що доступ до конфіденційних даних можуть мати лише ті, хто має належний дозвіл, зменшуючи ризик витоку даних і несанкціонованого доступу. Важливого значення набуває й постійне навчання персоналу та дотримання законодавства у сфері захисту даних. Адже, кіберзлочинці використовують усе складніші методи атак, включаючи атаки на основі штучного інтелекту.

Отже, захист даних є критично важливою складовою інформаційної безпеки, оскільки бази даних містять конфіденційну, комерційну чи іншу важливу інформацію. Разом з тим, інформаційні системи захисту даних

охоплюють широкий спектр технологій, які забезпечують конфіденційність, цілісність і доступність інформації (рис. 2).

Бізнес, щодня збільшує використання інформації у своїй роботі, що змушує шукати нові шляхи та інструменти захисту даних. Одним з таких механізмів є розробка стратегії захисту даних.

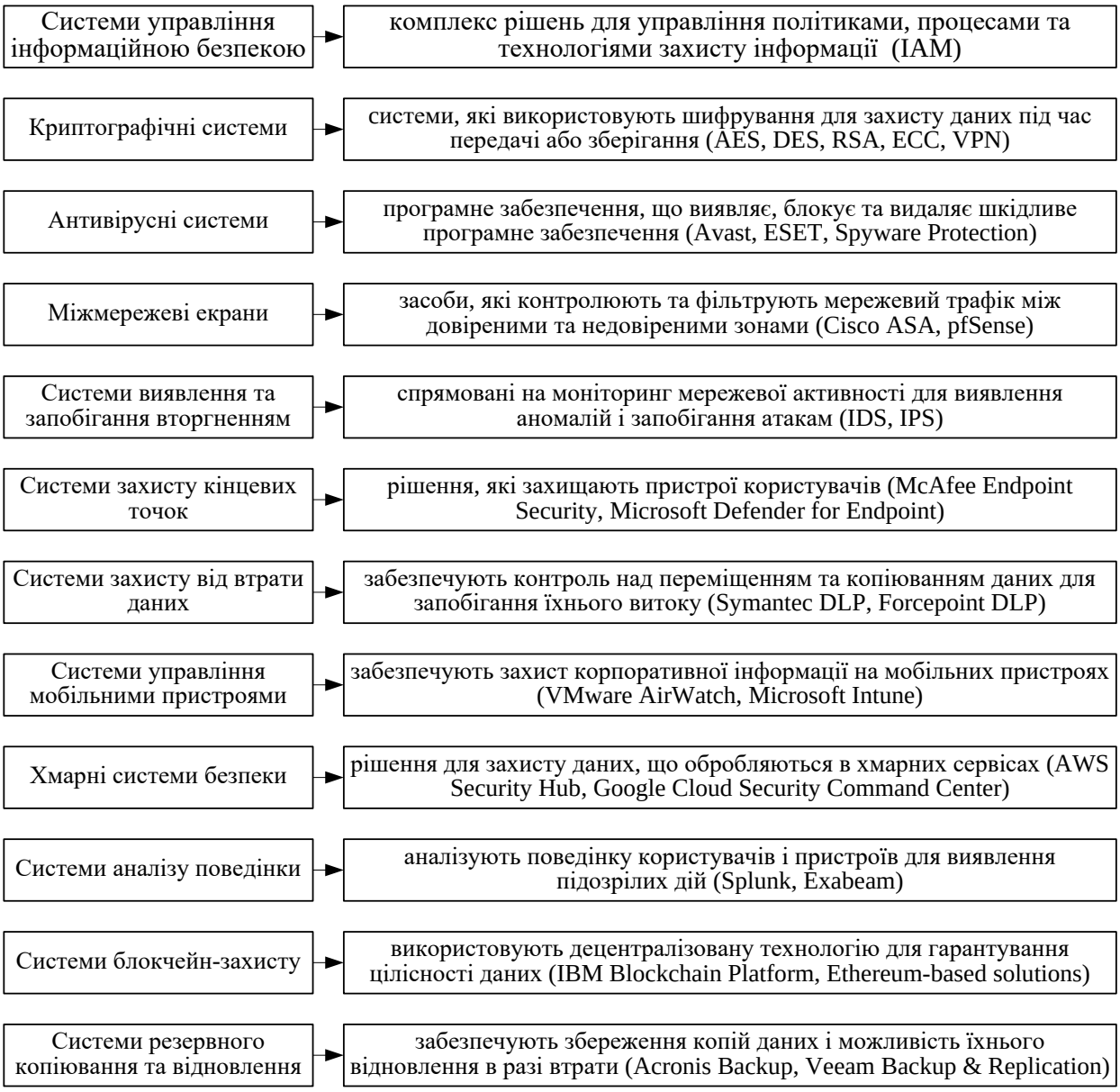

Рис. 2. Сучасні технології захисту даних

Джерело: узагальнено та побудовано автором.

Стратегія захисту даних – це організована робота, яка поєднує всі заходи, вжиті з метою захисту даних [8]. Стратегія захисту даних може допомогти стандартизувати безпеку конфіденційних даних і корпоративної інформації, гарантуючи конфіденційність клієнтів і співробітників і безпеку комерційної таємниці.

Стратегії захисту даних, зазвичай, поєднують багатоетапні процеси, які визначають, як реалізуються та підтримуються заходи безпеки. Метою даної процедури є мінімізація слідів конфіденційних даних й захист критично важливих для бізнесу даних. Зокрема, бізнес використовує стратегії захисту даних з метою запобігання отриманню несанкціонованого доступу зловмисникам. Основні етапи та компоненти стратегії захисту даних представлено на рис. 3.

1	Ідентифікація та класифікація даних	визначення типів даних та їхня класифікація за рівнями важливості та чутливості
2	Контроль доступу	упровадження політик обмеження доступу та використання багатофакторної автентифікації
3	Шифрування даних	захист даних у стані спокою та під час передачі за допомогою сильних алгоритмів шифрування
4	Резервне копіювання та відновлення	резервування даних для захисту від втрати та відновлення після збоїв, атак або випадкового видалення
5	Моніторинг і аудит	відстеження дій користувачів і змін у системах, виявлення загроз або спроб несанкціонованого доступу
6	Навчання персоналу	підвищення обізнаності співробітників про ризики витоку даних та способи захисту, тренінги з кібербезпеки
7	Реакція на інциденти	планування дій у разі витоку даних, інтеграція автоматизованих систем виявлення загроз

Рис. 3. Елементи та основні етапи побудови стратегії захисту даних

Джерело: розроблено автором.

З метою належного захисту даних відбувається ідентифікація та оцінка ризиків й загроз, які можуть вплинути на дані. Стратегія захисту даних має враховувати ці ризики та загрози й містити заходи, спрямовані на їхню мінімізацію та пом’якшення. Однією зі складових стратегії захисту є реалізація

заходів із кібербезпеки, які запроваджуються з метою запобігання атакам на внутрішні мережі, периметри мережі, дані в дорозі та дані в спокої. Як правило, ці заходи включають шифрування даних, впровадження антивірусного програмного забезпечення, захист від програм-вимагачів, обладнання та програмне забезпечення безпеки периметра та програмне забезпечення управління доступом.

Разом з тим, захист даних має різні інструменти та підходи. Так, фізичний захист передбачає контроль доступу до серверних приміщень, використання сейфів, захищених серверних шаф та захист обладнання від пожеж, затоплень та інших фізичних загроз. Розробка політик доступу, паролів і роботи з даними, оцінка ризиків і аудит відповідності стандартам безпеки, навчання працівників та контроль дотримання політик є елементами адміністративного захисту. Використання брандмауерів та SIEM-систем, програмного забезпечення з метою виявлення та усунення шкідливих програм та шифрування даних є вимогою – технічного (програмного) захисту.

Юридичний захист передбачає дотримання вимог законодавства та міжнародних стандартів, укладання угод із працівниками та партнерами щодо конфіденційності даних. Управління ролями й доступом до інформації – організаційний захист, а захист даних, що зберігаються або обробляються в хмарі з використанням інструментів хмарної безпеки є елементами хмарного захисту тощо.

З метою вдосконалення використання інформаційних систем у захисті даних необхідно впроваджувати сучасні технології, підвищувати ефективність управління безпекою та застосовувати комплексний підхід до кіберзахисту.

Висновки. Отже, виконане дослідження визначили, що з розвитком сучасних технологій та цифровізації усіх галузей зростає загроза несанкціонованого використання даних, яка вимагає розробки сучасних інструментів захисту даних.

Основними причинами витоку даних, наразі, є – використання слабких паролів, відсутність багатофакторної автентифікації та неконтрольований доступ до адміністративних облікових записів, які призводять до отримання, зміни чи видалення даних зловмисникам за допомогою довільних SQL-запитів. Ураховуючи значну вартість ліцензійних програм захисту, більшість користувачів використовую застарілі версії управління даними. Також, однією з проблем є використання незашифрованих каналів передачі даних.

Наразі найбільш популярними інструментами захисту даних є:

використання протоколів TLS/SSL для захисту мережевої передачі даних;

використання параметризованих запитів (та ORM (Object-Relational Mapping);

запровадження багатофакторної автентифікації (MFA) для доступу до баз даних;

впровадження IDS/IPS для моніторингу аномальної активності в базах даних;

застосування SIEM для аналізу подій у реальному часі, кореляції логів та швидкого реагування на інциденти;

використання хмарних сервісів, що підтримують вбудоване шифрування;

перевірка системи на відповідність стандартам, таким як ISO/IEC 27001, GDPR або PCI DSS;

використання децентралізованих рішень з метою забезпечення цілісності даних;

впровадження алгоритмів AI для автоматичного виявлення аномалій і прогнозування загроз.

Застосування цих інструментів дозволяє суттєво підвищити рівень захисту даних, забезпечити їхню цілісність, конфіденційність та доступність інформації.

Отже, сучасна проблема використання інформаційних систем у захисті даних полягає в забезпеченні адекватного рівня безпеки в умовах стрімкого розвитку загроз і технологій.

Список використаних джерел:

1. Diffie, W. & Hellman, M. (1976) New directions in cryptography. *IEEE Transactions on Information Theory*, Vol. 22, No. 6 pp. 644-654.

2. ISO/IEC 27001:2013: Стандарт. URL: https://www.dqsglobal.com/uk-ua/sertifikujte/sertifikaciya-iso-27001

3. Regulation (EU) 2016/679 (General Data Protection Regulation) URL: https://gdpr-info.eu/

4. Schneier, B. (1995). Applied Cryptography. Велика Британія: Wiley.

5. Shannon, C. (1948) Mathematical Theory of Communication. *The Bell System Technical Journal*, Vol. 27, pp. 379-423, 623-656 https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

6. Top 5 Methods of Protecting Data URL: https://www.titanfile.com/blog/5-methods-of-protecting-data/

7. Turing, A. (1938). *On Computable Numbers, with an Application to the Entscheidungsproblem: A correction*. Proceedings of the London Mathematical Society. 2 43 (1937). pp. 544–6.

8. What is Data Protection and Privacy? URL: https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

9. Георгіаді, Н.Г. Інформаційні системи управління: сутність, види, функції, принципи побудови. *Вісник Національного університету «Львівська політехніка».* 2006. № 567. С. 28-34.

10. Жупило, М. Дослідження та програмна реалізація системи забезпечення конфіденційності даних хмарних сервісів. *Збірник праць молодих науковців ЦНТУ.* 2023. Вип. 13., С. 229-242. URL: https://dspace.kntu.kr.ua/server/api/core/bitstreams/47e75a64-3b54-4a3d-bfd6-dbbcae39bb36/content

11. Інформаційні системи і технології в економіці: Посібник для студентів ВНЗ / За ред. Пономаренка В.С. К.: Видавничий центр «Академія», 2002. 544 с.

12. Порядок взаємодії органів виконавчоївлади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах: Постанова Кабінету Міністрів України від 16.11.2002 р. № 1772. (Редакція від 07.09.2022). URL: https://zakon.rada.gov.ua/laws/show/1772-2002-%D0%BF#Text

13. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР (Редакція від 28.06.2024). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

14. Про технічний захист інформації в Україні: Положення, Указ Президента України від 27.09.1999 № 1229/99. (Редакція від 04.05.2008) URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text

15. Пурій Г. М. Інформаційні системи і технології в управлінні діяльністю підприємства. *Ефективна економіка*. 2019. № 6. URL: http://www.economy.nayka.com.ua/?op=1&z=7127

16. Ральф К. Меркл. URL: https://ralphmerkle.com/

17. Яценко, Р.М., Ніколаєв І.В. Інформаційні системи в логістиці: навчальний посібник. Харків: Вид-во ХНЕУ, 2012. 232 с.

Denys TARASENKO
Candidate of Technical Sciences,
Associate Professor of the Department
of Law and Information Affairs,
Private Higher Education Institution
«Rauf Ablyazov East European University»,
Cherkasy, Ukraine
https://orcid.org/0009-0006-0582-1619
denis.tarasenko@gmail.com

MODERN DATA PROTECTION TOOLS IN INFORMATION SYSTEMS: PROBLEMS AND PROSPECTS

Abstract. *The digitalization of society and the development of modern technologies create new requirements for obtaining and storing information. Today, information systems play a key role in the functioning of modern society, but their active use raises significant challenges in the field of data protection. The purpose of the article is to analyze the key aspects of information systems and data protection.*

Methods. The paper uses the method of synthesis and analysis to summarize the research of scientists in the field of data protection. Empirical methods were used to analyze modern information systems and data protection practices.

The article examines the definition of "information systems" and the main aspects of their functioning, and defines their role in data storage and processing. Considerable attention is paid to the security of databases, which are key elements of modern information systems. Threats affecting the confidentiality, integrity, and availability of data are analyzed, and the causes and consequences of data breaches are identified. The study identifies the main methods and technologies of data protection, such as encryption, authentication, copying, etc. The types of data protection are presented, and the expediency of developing a data protection strategy is substantiated, indicating its main elements and stages of implementation.

Results. The author suggests areas for improving the processes of database protection, which include the integration of modern intrusion detection systems, implementation of access policies, raising staff awareness, and ensuring cybersecurity. According to the author, an integrated approach to ensuring data security in the context of the rapid development of information technology and the growth of digital information is gaining particular relevance.

Keywords: *data, threats, protection, information systems, information, cyber threat, privacy, software, strategy, technology, encryption.*