http://www.moderntechno.de/index.php/meit/article/view/meit41-01-066
DOI: 10.30890/2567-5273.2025-41-01-066

УДК 004.42-021

INFORMATION SECURITY PROCEDURE

МЕТОДИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Al-Ammori Ali / Аль-Амморі Алі
d.t.s., prof. / д.т.н., проф.
ORCID: 0000-0002-0375-6108
National Transport University, Kyiv, Mykhaila Omelianovycha - Pavlenka Str. 1, 01010
Національний транспортний університет, Київ, вул. М. Омеляновича-Павленка, 1, 01010
Dyachenko P.V. / Дяченко П.В.
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0001-8475-5854
Cherkasy state technological university, Cherkasy, Shevchenko Blvd., 460, 18006
Черкаський державний технологічний університет, Черкаси, б-р Шевченка, 460, 18006
Klochan A.Ye. / Клочан А.Є.
PhD, as.prof. / д-р філософії, доц.
ORCID: 0000-0002-4225-9382
National Transport University, Kyiv, Mykhaila Omelianovycha - Pavlenka Str. 1, 01010
Національний транспортний університет, Київ, вул. М. Омеляновича-Павленка, 1, 01010
Tumanova I.V. / Туманова І.В.
senior lecturer / старший викладач
National Transport University, Kyiv, Mykhaila Omelianovycha - Pavlenka Str. 1, 01010
Національний транспортний університет, Київ, вул. М. Омеляновича-Павленка, 1, 01010
Oliinuk V.L. / Олійник В.Л.
assistant / асистент
National Transport University, Kyiv, Mykhaila Omelianovycha - Pavlenka Str. 1, 01010
Національний транспортний університет, Київ, вул. М. Омеляновича-Павленка, 1, 01010

Анотація. *В статті розглядаються питання формування та впровадження науково обґрунтованих підходів до побудови складних систем захисту. Сформульовано головну мету будь-якої системи інформаційної безпеки підприємства та низку ключових, науково обґрунтованих завдань, за умови виконання яких стає можливим досягнення поставлених цілей. Сформовано модель взаємодії елементів інформаційної безпеки, яка ілюструє, що інформаційна безпека – це не ізольований процес, а динамічна взаємодія між трьома групами компонентів. Розроблено модель оцінки можливих інформаційних ризиків, яка базується на принципах циклічного управління ризиками, визначених у міжнародних стандартах. Показано, що ефективне забезпечення інформаційної безпеки українських підприємств можливе лише за умови інтеграції міжнародних стандартів та національних нормативів, на основі застосування комплексного підходу до аналізу ризиків, що поєднує якісні та кількісні методи їх оцінювання.*

Ключові слова: *система інформаційної безпеки, міжнародні стандарти, національні нормативи, модель взаємодії, інформаційна надійність, ризики.*

Вступ.

Головною метою будь-якої системи інформаційної безпеки підприємства є забезпечення сталого функціонування об’єкта, запобігання загрозам його діяльності, захист законних інтересів від протиправних посягань, недопущення розкрадання фінансових ресурсів, витоку, втрати, викривлення чи знищення

службової інформації, а також створення умов для безперебійної роботи всіх структурних підрозділів [1].

У сучасних умовах глобалізації та цифрової трансформації роль інформаційної безпеки набуває стратегічного значення. Зростання обсягів оброблюваної та переданої інформації, інтеграція інформаційних систем у глобальні мережі, а також збільшення кількості та складності кіберзагроз вимагають впровадження науково обґрунтованих підходів до побудови комплексних систем захисту. Ефективність таких систем визначається не лише технічними засобами, а й нормативно-правовими засадами, організаційними заходами, підготовкою персоналу та постійним моніторингом ризиків [1].

Міжнародні стандарти, зокрема ISO/IEC 27001 та рекомендації NIST Cybersecurity Framework, а також національні нормативи України ДСТУ ISO/IEC 27001:2015 створюють основу для системного підходу до управління інформаційною безпекою, забезпечуючи інтеграцію міжнародного досвіду та адаптацію до специфіки національних умов [2].

Основна частина.

Досягнення цілей забезпечення інформаційної безпеки можливе лише за умови виконання низки ключових завдань, кожне з яких має вагоме наукове та практичне обґрунтування:

1. *Класифікація інформації за рівнями доступу та визначення категорій службової таємниці.* Така класифікація забезпечує диференційований підхід до захисту даних залежно від їхньої критичності. Наприклад, ISO/IEC 27001 передбачає визначення категорій даних: public, internal, confidential, secret та відповідних режимів доступу. В Україні подібний підхід закріплено у Законі «Про інформацію» та ДСТУ 3396.2-96, що визначають порядок віднесення відомостей до комерційної таємниці [3].

2. *Прогнозування та своєчасне виявлення загроз інформаційним ресурсам.* Прогнозування ґрунтується на аналізі тенденцій розвитку кіберзлочинності та технологічних вразливостей. Дослідження ENISA (2022) показують, що раннє виявлення аномальної активності знижує ризик інциденту на 40–60%. У практиці

це реалізується через системи SIEM (Security Information and Event Management) та інструменти машинного навчання для поведінкового аналізу.

3. *Створення умов функціонування інформаційних систем, які мінімізують ймовірність реалізації загроз.* Це передбачає впровадження принципу «безпека за проєктом» (security by design), коли захист закладається ще на етапі архітектурного планування системи, а не додається постфактум.

4. *Оперативне реагування на інциденти інформаційної безпеки.* Включає формування команд CSIRT/CERT, наявність планів реагування на інциденти (Incident Response Plans), тестування сценаріїв реагування. За даними IBM X-Force (2023), підприємства з відпрацьованим планом реагування скорочують збитки від кібератак у середньому на 58%.

5. *Формування механізмів відшкодування та локалізації шкоди.* Тут важливими є як технічні (backup та disaster recovery), так і правові інструменти (страхування кіберризиків, договори з провайдерами послуг). Модель взаємодії елементів інформаційної безпеки зображено на рис. 1.

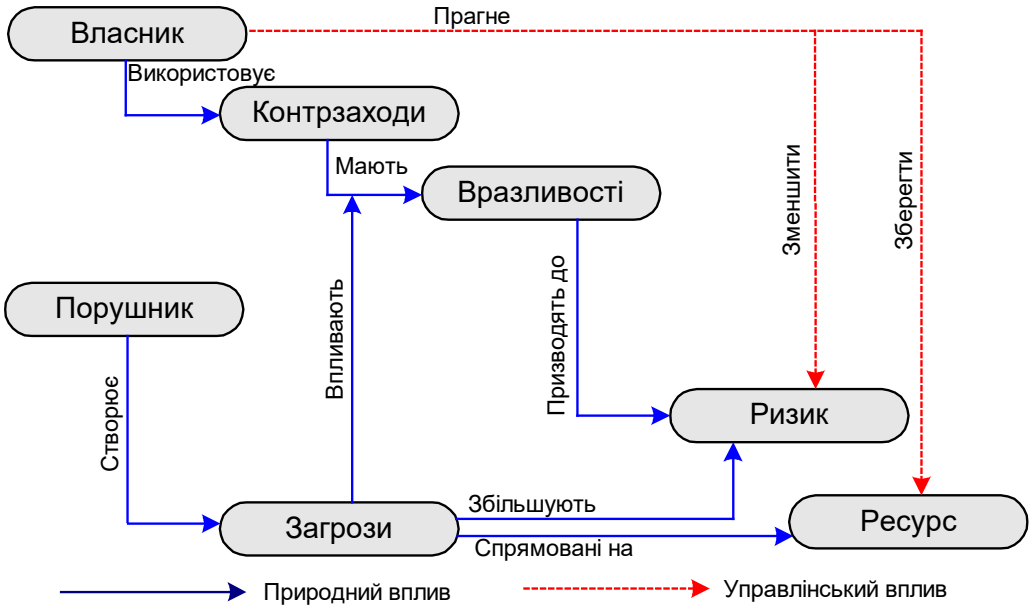

Рис. 1. Модель взаємодії елементів інформаційної безпеки

Модель ілюструє, що інформаційна безпека – це не ізольований процес, а динамічна взаємодія між трьома групами компонентів:

– об’єкти захисту (інформаційні ресурси, системи, мережі);

– суб’єкти захисту (адміністратори, користувачі, служби безпеки);

– порушники (зовнішні та внутрішні, умисні та випадкові).

Вплив зовнішніх факторів (геополітичні ризики, економічні кризи, технологічні зміни) та внутрішніх (організаційна структура, кваліфікація персоналу, культура безпеки) формує постійно змінне поле ризиків. Саме тому модель підкреслює важливість безперервного моніторингу та адаптації заходів захисту.

Фактори та методи аналізу ризиків. Аналіз ризиків є фундаментальною складовою управління інформаційною безпекою, оскільки дозволяє визначити пріоритети та обґрунтувати доцільність впровадження конкретних захисних заходів. У сучасних концепціях кіберзахисту (ISO/IEC 27005:2022, NIST SP 800-30 Rev.1) виділяють три ключові категорії факторів, що визначають рівень ризику [4].

1. Загрози. Загроза – це потенційна подія або дія, здатна спричинити шкоду інформаційним активам. Вони поділяються за походженням (внутрішні/зовнішні), за мотивами (умисні/випадкові) та за складністю реалізації (від простих технічних збоїв до складних цілеспрямованих атак):

- прості загрози: випадкове видалення даних співробітником, поломка жорсткого диска;
- загрози середнього рівня: вірусні інфекції, фішингові кампанії;
- загрози високого рівня: APT-атаки (Advanced Persistent Threats), що передбачають тривалу присутність зловмисника в системі з метою шпигунства чи саботажу.

Дослідження Verizon Data Breach Investigations Report (2023) показує, що 74% інцидентів пов’язані з людським фактором, що підкреслює важливість навчання персоналу [5].

2. Вразливості. Вразливості – це слабкі місця, що можуть бути використані для реалізації загроз. Вони можуть мати:

➢ технологічний характер: відкриті порти, відсутність багатофакторної

автентифікації, використання застарілого програмного забезпечення;

- організаційний характер: відсутність політики паролів, незадокументовані процедури резервного копіювання.
- кадровий характер: низький рівень обізнаності персоналу, відсутність культури безпеки.

Згідно з ENISA Threat Landscape (2022), 90% успішних атак експлуатують відомі, але не закриті вразливості [6].

3. Ризик-фактор. Ризик-фактор відображає очікуваний рівень збитків і розраховується у міжнародній практиці за формулою Ризик=Ймовірність події× Величина збитку [7]. Тут ймовірність оцінюється на основі історичних даних і прогнозних моделей, а величина збитку – у фінансових, репутаційних та операційних показниках.

Методи аналізу ризиків умовно поділяються на дві групи:

а) якісні методи: базуються на експертних оцінках, аналізі сценаріїв, методі Delphi, SWOT-аналізі. Вони є швидкими та зручними на початкових етапах, але мають суб'єктивний характер;

б) кількісні методи: передбачають використання математичного моделювання (метод Монте-Карло, байєсівський аналіз), статистичних даних і формалізованих критеріїв. Їх перевага – висока точність і можливість порівняння альтернатив, але вони потребують великого масиву даних.

Моделювання ризиків дозволяє продумати методи захисту системи ще на етапі її проектування. Моделювання ризиків – це неперервний процес, який допомагає знаходити та зменшувати кількість загроз у системі шляхом прийняття певних дій. Під величиною ризику умовно розуміють настання ймовірності негативної події і розміру збитку. У свою чергу під ймовірністю події розуміється настання ймовірності реалізації загрози інформаційній безпеці, а також вразливостей інформаційної безпеки, виражені в якісній або кількісній формі. Умовно це може бути висловлено за наведеною вище логічною формулою [7]: величина_ризику=Ймовірність_події * Розмір_збитку, де Ймовірність_події

= Ймовірність_загрози * Величину_вразливості. Модель оцінювання інформаційних ризиків зображено на рис. 2.

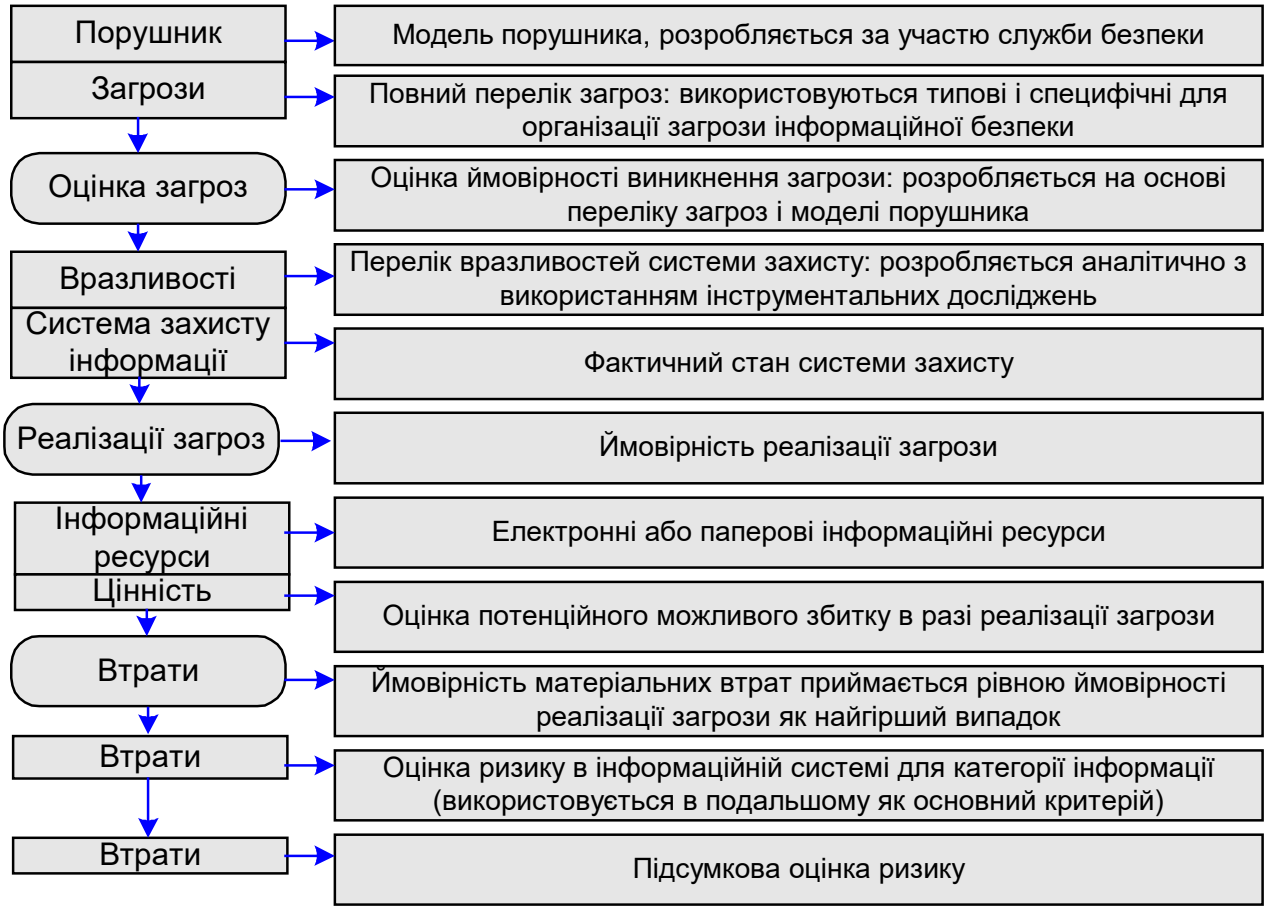

Рис. 2. Модель оцінювання можливих інформаційних ризиків

Запропонована модель ґрунтується на принципах циклічного управління ризиками, визначених у міжнародних стандартах (ISO/IEC 27005, NIST RMF). Вона передбачає ітеративний процес, який можна розділити на шість етапів [8]:

1. Ідентифікація активів. Необхідно скласти повний реєстр інформаційних активів (даних, систем, сервісів) з визначенням їхньої критичності. На цьому етапі використовують інвентаризацію та категоризацію даних згідно з політикою доступу.

2. Аналіз загроз. Оцінюються внутрішні та зовнішні загрози з використанням бібліотек типових загроз, наприклад, MITRE ATT&CK. Результати аналізу дозволяють встановити, які загрози є найбільш імовірними та небезпечними.

3. Оцінка вразливостей. Виконується тестування на проникнення (penetration testing), сканування вразливостей (vulnerability scanning) та аудит конфігурацій.

4. Кількісна оцінка ризику. Визначаються числові показники ймовірності реалізації загроз та розміру потенційних збитків. Можливе використання CVSS (Common Vulnerability Scoring System) для пріорітизації.

5. Вибір контрзаходів**.** Проводиться аналіз співвідношення витрат на впровадження заходів та очікуваної вигоди у вигляді зниження ризику (cost-benefit analysis). На цьому етапі також формуються плани реагування.

6. Моніторинг та оновлення. Забезпечується постійне відстеження стану безпеки, аналіз інцидентів і корекція політик. Це відповідає концепції PDCA (Plan-Do-Check-Act), яка лежить в основі систем управління безпекою.

В загальному випадку, предметна область оцінки ризиків безпеки інформаційних систем може бути представлена діаграмою класів в нотації Unified Modeling Language (UML) [9], як показано на рис. 3.

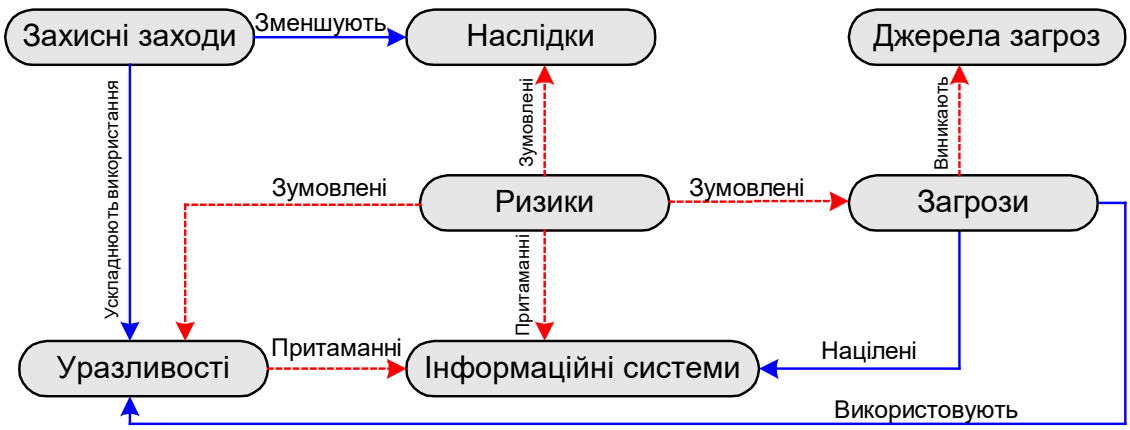

Рис. 3. Предметна область оцінки ризиків безпеки

Під ризиком мається на увазі ризик інформаційної безпеки, що являє собою комбінацію ймовірності виникнення ризикової події (наприклад, реалізації загрози) і завдання при цьому шкоди.

Ризики зазвичай пов'язують з активами, під якими розуміється «що небудь, що має цінність для організації і, отже, потребує захисту». В ISO/IEC 27005:2011

активи поділяються на первинні та вторинні. До первинних активів відносять інформацію і бізнес-процеси, а до вторинних – технічні засоби, програмне забезпечення, мережу, персонал, місця функціонування та організаційну структуру [10].

Організаційна політика безпеки. Організаційна політика безпеки – це базовий документ, який формує «культуру безпеки» в організації. Її розробка та впровадження мають науково-методологічну основу, закріплену у стандартах ISO/IEC 27001 та NIST SP 800-53 [11].

Основні структурні елементи політики:

1. Структура цінності активів. Визначення пріоритетності захисту різних активів. Критичні активи повинні мати найвищий рівень контролю доступу та моніторингу.

2. Ризик-профіль організації. Документований перелік найімовірніших та найбільш шкідливих загроз, актуальних для конкретного підприємства.

3. Правила доступу та контролю. Використання принципу найменших привілеїв (least privilege), багатофакторної автентифікації, розмежування ролей.

4. Процедури реагування на інциденти. Чіткі покрокові алгоритми, які дозволяють швидко локалізувати та усунути наслідки інциденту. Передбачає створення команди реагування на інциденти (Incident Response Team).

5. Навчання персоналу. Регулярне проведення тренінгів з кібергігієни, моделювання фішингових атак для перевірки обізнаності співробітників.

За рекомендаціями NIST CSF, політика повинна переглядатися щонайменше раз на рік, а також після кожного серйозного інциденту чи зміни IT-інфраструктури [6].

Приклади з українських підприємств:

1. Фактори та методи аналізу ризиків:

Енергетика. У ПАТ «Укренерго» у 2021–2022 рр. впроваджено комплексний аудит кіберзахисту, який виявив критичні уразливості в системах управління SCADA. Використовували комбінований метод — якісну експертну оцінку та кількісне моделювання наслідків за сценаріями кібератак типу BlackEnergy

(аналогічно атакам 2015 року). За результатами було модернізовано міжмережеві екрани, впроваджено сегментацію мереж та обов'язкову багатофакторну автентифікацію для операторів.

Фінанси. ПриватБанк у 2022 році посилив політику інформаційної безпеки після зростання кількості фішингових атак на клієнтів. Для оцінки ризиків використовували CVSS для вразливостей у мобільному додатку, а також метод Монте-Карло для оцінки фінансових наслідків масових фішингових кампаній. Це дозволило обґрунтувати інвестиції у впровадження антифішингового шлюзу та розширення програми навчання користувачів.

Держсектор. Міністерство цифрової трансформації України у 2022 році застосувало методику ISO/IEC 27005 для аналізу ризиків у проєкті «Дія». Було виявлено, що найбільш імовірними загрозами є DDoS-атаки та експлуатація вразливостей вебсервісів. В результаті впроваджено додаткові системи WAF (Web Application Firewall) та мережеве резервування [12].

2. Модель оцінювання інформаційних ризиків:

Енергетика. АТ «ДТЕК Енерго» інтегрувало модель управління ризиками, сумісну з NIST RMF, у систему моніторингу виробничих процесів. Це дозволило зменшити час реагування на інциденти в мережах критичної інфраструктури з 6 до 2 годин.

Фінанси. Національний банк України (НБУ) впровадив у 2022 році оцінювання ризиків банківської IT-інфраструктури на основі ітеративної моделі. Щоквартальний аналіз з урахуванням нових даних (включаючи кібератаки на банки в ЄС) дав змогу скоротити ймовірність інцидентів класу ransomware на 35%.

Держсектор. У Державній податковій службі модель оцінювання ризиків застосовують для автоматизованих інформаційних систем обліку платників податків. Моніторинг і оновлення політик здійснюються щомісячно, з урахуванням нових типів загроз, виявлених СБУ та Держспецзв'язку.

3. Організаційна політика безпеки.

Енергетика. Укргідроенерго прийняло оновлену політику безпеки у 2023

році, де впроваджено принцип least privilege, обов'язкове шифрування конфіденційних даних та регламентовану процедуру реагування на інциденти з чітким розподілом ролей.

Фінанси. Ощадбанк впровадив централізовану систему контролю доступу на базі Zero Trust Architecture, де кожен запит до ресурсу перевіряється незалежно від попередніх сеансів.

Держсектор. У Державному підприємстві «Українські спеціальні системи» політика безпеки включає обов'язкове щорічне навчання персоналу з моделюванням реальних сценаріїв атак. Це дозволило підвищити обізнаність співробітників на 65% за даними внутрішніх тестів.

Висновки:

Проведене дослідження засвідчує, що ефективне забезпечення інформаційної безпеки українських підприємств можливе лише за умови інтеграції міжнародних стандартів, таких як ISO/IEC 27001, NIST Cybersecurity Framework, та національних нормативів, зокрема ДСТУ ISO/IEC 27005. Застосування комплексного підходу до аналізу ризиків, що поєднує якісні та кількісні методи оцінювання, дозволяє своєчасно ідентифікувати загрози, визначати їхню ймовірність та прогнозувати можливі наслідки. Використання ітеративних моделей управління ризиками забезпечує адаптивність систем безпеки до змін у загрозовому середовищі та дозволяє підвищити ефективність захисту критичних активів. Досвід українських підприємств у сферах енергетики, фінансів та державного сектору демонструє, що впровадження організаційної політики безпеки як стратегічного документа, доповненої сучасними технічними рішеннями та регулярним навчанням персоналу, значно зменшує вразливість систем і підвищує рівень готовності до реагування на інциденти. У результаті поєднання нормативно-правових, організаційних та технічних заходів формується цілісна система захисту, здатна протистояти як традиційним, так і новітнім кіберзагрозам, що особливо важливо в умовах підвищеного ризику та глобальної цифровізації.

Література.

1. Побудова комплексних систем захисту інформації URL: http://iqusion.com/ua/sistemi-zakhistu-informatsiji

2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

3. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on information security risk management.

4. ДСТУ ISO/IEC 27005:2011. Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки.

5. NIST SP 800-30 Rev.1. Guide for Conducting Risk Assessments. National Institute of Standards and Technology, 2022.

6. ENISA Threat Landscape 2022. European Union Agency for Cybersecurity.

7. Verizon Data Breach Investigations Report 2023. Verizon Communications.

8. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.

9. Закон України «Про інформацію» від 02.10.1992 № 2657-XII.

10. Міністерство цифрової трансформації України. Звіт про кіберзагрози та інциденти 2022 року.

11. IBM X-Force Threat Intelligence Index 2023. IBM Security.

12. MITRE ATT&CK Framework. MITRE Corporation, 2023.

Abstract. *The article considers the issues of forming and implementing scientifically based approaches to building complex protection systems. The main goal of any enterprise information security system and a number of key, scientifically based tasks are formulated, provided that the achievement of the set goals becomes possible. A model of interaction of information security elements is formed, which illustrates that information security is not an isolated process, but a dynamic interaction between three groups of components. A model of assessing possible information risks is developed, which is based on the principles of cyclical risk management defined in international standards. It is shown that effective provision of information security of Ukrainian enterprises is possible only if international standards and national regulations are integrated, based on the application of a comprehensive approach to risk analysis, combining qualitative and quantitative methods of their assessment.*

Keywords: *information security system, international standards, national regulations, interaction model, Information reliability, risks.*

Статтю надіслано: 24.10.2024 р.