НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ МЕРЕЖЕВОГО ЗАХИСТУ ІНФОРМАЦІЇ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Чумаченко Андрій Вадимович

Керівник: к.т.н., доцент
Ахмаметьєва Ганна Валеріївна

Рецензент: к.т.н., доцент
Бойко Віктор Дмитрович

Одеса – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Чумаченко Андрію Вадимовичу

1. Тема роботи: «Дослідження Сучасних методів мережевого захисту інформації»
Керівник роботи: к.т.н, доцент Ахмаметьєва Ганна Валеріївна
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «19» травня 2025 року
3. Дата видачі завдання«16 » вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Підбір матеріалів за темою кваліфікаційної роботи	19.03.2025-11.04.2025	
2	Аналіз теоретичних основ мережевого захисту інформації (розділ 1)	11.04.2025-21.04.2025	
3	Аналіз стратегій і сучасних підходів до захисту інформації (розділ 2)	21.04.2025-01.05.2025	
4	Дослідження характеристик засобів мережевого захисту інформації (розділ 3)	01.05.2025-11.05.2025	
5	Оформлення пояснювальної записки	11.05.2025-21.05.2025	
6	Подання роботи до захисту	27.05.2025	
7	Захист роботи	12.06.2025	

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Дослідження сучасних методів мережевого захисту інформації» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 1 рисунок, 1 таблицю, 15 літературних джерел за переліком посилань. Робота виконана на 47 сторінках загального тексту і 36 сторінках основного тексту.

Мета роботи - дослідити методи забезпечення конфіденційності, цілісності та доступності інформації в комп'ютерних мережах та реалізувати комплексну систему захисту на практиці.

У роботі розглянуто правові й методологічні основи мережевого захисту, модель конфіденційність–цілісність–доступність. Проаналізовано сучасні парадигми захисту - багаторівневий захист, модель «нульової довіри» та розподілену безпеку - і описано організаційні, технічні й програмні підходи до зниження ризиків у мережевому середовищі.

Також у роботі наведено класи технічних засобів захисту, та описано стратегії запобігання загрозам, виявлення інцидентів і реагування на них. Увагу приділено мережевій ізоляції, сегментації, використанню віртуальних локальних мереж і демілітаризованих зон, а також принципам побудови архітектури «нульової довіри».

Робота містить практичну реалізацію: вибір і налаштування міжмережевого екрану нового покоління, впровадження системи Suricata для виявлення і попередження мережевих вторгнень, застосування криптографії та протоколів TLS/SSL, організацію незмінних резервних копій, побудову гнучких моделей контролю доступу на основі ролей і атрибутів із багатоетапною автентифікацією і централізацією через каталогові служби, а також використання антивірусних шлюзів і політик регулярного оновлення. Оцінено економічну доцільність обраних рішень.

МЕРЕЖЕВИЙ ЗАХИСТ ІНФОРМАЦІЇ, КОНФІДЕНЦІЙНІСТЬ ДАНИХ, МІЖМЕРЕЖЕВИЙ ЕКРАН, СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ, ШИФРУВАННЯ, РЕЗЕРВНЕ КОПІЮВАННЯ, КОНТРОЛЬ ДОСТУПУ

ABSTRACT

The qualification work on the topic "Study of Modern Methods of Network Information Protection" for obtaining the first (bachelor’s) level of higher education in the specialty 125 Cybersecurity. Contains 1 figure, 1 table, 15 references in the bibliography. The work was completed on 47 pages of the general text and 36 pages of the main text.

The objective of the work is to investigate methods of ensuring confidentiality, integrity, and availability of information in computer networks and to implement a comprehensive protection system in practice.

The work examines the legal and methodological foundations of network protection, the confidentiality–integrity–availability model. Modern protection paradigms are analyzed—multilayered defense, the zero trust model, and distributed security—and organizational, technical, and software approaches to risk reduction in the network environment are described.

The work also presents classes of technical protection tools and describes strategies for threat prevention, incident detection, and response. Attention is paid to network isolation, segmentation, use of virtual local area networks (VLANs) and demilitarized zones (DMZs), as well as principles for building a zero trust architecture.

The work includes practical implementation: selection and configuration of a next-generation firewall, deployment of the Suricata system for network intrusion detection and prevention, application of cryptography and TLS/SSL protocols, organization of immutable backups, construction of flexible access control models based on roles and attributes with multi-factor authentication and centralization through directory services, as well as use of antivirus gateways and regular update policies. Economic feasibility of the chosen solutions is evaluated.

NETWORK INFORMATION PROTECTION, DATA CONFIDENTIALITY, FIREWALL, INTRUSION DETECTION SYSTEM, ENCRYPTION, BACKUP, ACCESS CONTROL

ЗМІСТ

ВСТУП

У епоху стрімкого розвитку інформаційних технологій значна частина комунікацій, обміну даними та збереження інформації відбувається через комп’ютерні мережі. Водночас із розширенням цифрової інфраструктури зростає і кількість кіберзагроз, які можуть призводити до порушення конфіденційності, цілісності та доступності інформації. Проблема мережевого захисту є однією з ключових у сфері інформаційної безпеки, адже саме вона визначає здатність системи протистояти як зовнішнім, так і внутрішнім загрозам.

У сучасному цифровому суспільстві питання забезпечення безпеки інформації, що передається через комп’ютерні мережі, є надзвичайно актуальним. Стрімкий розвиток інфокомунікацій, глобалізація інформаційного простору та збільшення обсягів переданої й оброблюваної інформації спричинили значне зростання ризиків, пов’язаних з її несанкціонованим доступом, викраденням, модифікацією або знищенням. Це зумовлює необхідність впровадження надійних методів захисту в мережевому середовищі.

Комп’ютерні мережі стали базою для функціонування державних структур, бізнесу, медицини, освіти, фінансових установ і приватного сектору. У цьому контексті конфіденційність, цілісність та доступність інформації набувають ключового значення. Кіберзлочини, зокрема фішинг, DDoS-атаки, перехоплення трафіку, впровадження шкідливого програмного забезпечення та крадіжка персональних і корпоративних даних, становлять серйозну загрозу для користувачів мережевих технологій.

Інформаційна безпека в мережах потребує постійного вдосконалення, оскільки зловмисники активно застосовують новітні техніки атаки, зокрема з використанням штучного інтелекту, машинного навчання та соціальної інженерії. Зі свого боку, захисні технології повинні бути адаптивними, ефективними, масштабованими й такими, що забезпечують безперервний контроль за станом мережевої інфраструктури.

Додатковим фактором, що посилює актуальність теми, є посилення державного і міжнародного законодавства у сфері захисту інформації. Закони про захист персональних даних та стандарти безпеки зобов’язують організації впроваджувати ефективні механізми захисту та відповідати вимогам прозорості й відповідальності у сфері інформаційної безпеки.

Зростання ролі хмарних обчислень, мобільних пристроїв, Інтернету речей, електронної комерції та цифрових сервісів загалом лише підкреслює необхідність побудови стійких систем мережевого захисту. Кількість даних, які зберігаються і передаються через мережі зростає, що створює додаткове навантаження на існуючі засоби безпеки та вимагає розробки нових, інноваційних підходів.

Сутність наукової задачі полягає у виявленні та аналізі існуючих методів захисту інформації в комп’ютерних мережах, їх ефективності у різних сценаріях використання, а також у визначенні напрямів удосконалення цих методів із урахуванням сучасних викликів, таких як поширення IoT-пристроїв, зростання складності атак, використання штучного інтелекту в хакерських інструментах тощо.

Вихідними даними для дослідження є науково-технічна література, міжнародні стандарти у сфері інформаційної безпеки, аналітичні звіти з кібербезпеки, технічна документація провідних виробників рішень мережевої безпеки, а також практичний досвід впровадження сучасних технологій захисту інформації.

Необхідність проведення дослідження зумовлена як зростанням частоти та складності кіберзлочинів, так і недостатньою обізнаністю багатьох організацій щодо наявних рішень та засобів захисту. Крім того, швидкий розвиток мережевих технологій вимагає постійного оновлення методів безпеки та перегляду підходів до побудови захищеної інфраструктури.

Актуальність теми обумовлена постійним збільшенням кількості кіберінцидентів та розвитком нових типів атак, що потребує більш глибокого вивчення, систематизації та вдосконалення існуючих методів мережевого захисту. Сучасні технології, такі як хмарні сервіси, віртуалізація, мобільні пристрої,

розширюють периметр мережі, що ускладнює її захист традиційними засобами. У таких умовах дослідження сучасних підходів до побудови систем захисту набуває важливого практичного значення.

Метою дослідження є аналіз, порівняння та класифікація сучасних методів мережевого захисту інформації, а також виявлення їх переваг, недоліків і перспектив розвитку в умовах змінного кіберпростору.

Об’єктом дослідження є мережевий захист інформації

Предметом дослідження є сучасні методи й технічні засоби захисту інформації в комп’ютерних мережах — зокрема криптографічні алгоритми, системи мережевих екранів, виявлення та запобігання вторгненням, резервне копіювання, контроль доступу, мережева ізоляція та сегментація

Завдання дослідження:

– Розглянути основи побудови систем мережевої безпеки та їх роль в інформаційній інфраструктурі.

– Провести аналіз сучасних методів захисту інформації в комп’ютерних мережах.

– Класифікувати засоби захисту за принципами дії та сферою застосування.

– Визначити сильні та слабкі сторони досліджуваних методів.

– Розробити рекомендації щодо ефективного використання сучасних засобів захисту в умовах сучасного цифрового середовища.

1 ТЕОРЕТИЧНІ ОСНОВИ МЕРЕЖЕВОГО ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Предметна область дослідження та її складові

Мережевий захист інформації - це комплекс організаційних і технічних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, що передається або зберігається в комп'ютерних мережах. У сучасних умовах цей напрям є критично важливим, адже порушення безпеки інформаційних потоків може призвести до значних фінансових та репутаційних втрат.

Інформація з обмеженим доступом - це сукупність відомостей, до яких мають право доступу лише визначені особи, тоді як їх розголошення заборонено відповідно до вимог чинного законодавства та рішення розпорядника інформації. Обмеження доступу до таких даних запроваджується з метою забезпечення національної безпеки або захисту прав та інтересів фізичних чи юридичних осіб. Важливо зазначити, що обмеження стосується саме змісту інформації, а не всього документа загалом. Відповідно, якщо в одному документі міститься відкрита і закрита інформація, то відкрита інформація може бути надана на ознайомлення зацікавленій особі у вигляді окремого документу[3].

Згідно зі статтею 6 Закону України «Про доступ до публічної інформації», інформація з обмеженим доступом може бути наступною:

1. Конфіденційна інформація - інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням, відповідно до передбачених ними умов.

2. Таємна інформація – інформація, доступ до якої обмежується і розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу передбачену законом таємницю.

3. Службова інформація - що міститься в документах суб'єктів владних повноважень, які становлять внутрішньовідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму

діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню або прийняттю рішень; зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці [4].

Управління захистом інформації в мережах в Україні ґрунтується на низці законодавчих актів, які встановлюють правові вимоги до забезпечення конфіденційності, цілісності та доступності даних. Закон України «Про захист інформації в інформаційно‑комунікаційних системах» визначає базові терміни, суб'єктів і об'єкти захисту, а також зобов'язує власників і користувачів систем запроваджувати відповідні технічні та організаційні заходи безпеки[2]. Додатково, закон «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163‑VIII формалізує національну систему реагування на кіберінциденти, створює мережу команд реагування на комп'ютерні надзвичайні події (CERT‑UA) та встановлює обов'язок операторів критичної інформаційної інфраструктури обмінюватися даними про загрози[5]. Вимоги щодо розмежування публічної та обмеженої інформації визначає Закон «Про доступ до публічної інформації» від 13.01.2011 № 2939‑VI, у статті 6 якого чітко перераховані категорії інформації з обмеженим доступом і порядок її захисту без заборони на розкриття відкритої частини документа[4]. Водночас Кримінальний кодекс України та Кодекс України про адміністративні правопорушення передбачають відповідальність за несанкціоноване розголошення й порушення режиму захисту інформації, що стимулює дотримання встановлених норм[6].

На міжнародному рівні побудова системи інформаційної безпеки має спиратися на ISO/IEC 27001:2013, який задає вимоги до впровадження, моніторингу та безперервного вдосконалення систем управління інформаційною безпекою (ISMS). Рамкова модель NIST Cybersecurity Framework, розроблена Національним інститутом стандартів і технологій США, структурована за п'ятьма основними функціями-ідентифікація, захист, виявлення, реагування та відновлення-що дозволяють організаціям системно управляти ризиками.

Незважаючи на те, що Європейський регламент GDPR (General Data Protection Regulation) безпосередньо не імплементований в українське законодавство, він встановлює сучасні стандарти обробки персональних даних і слугує орієнтиром для компаній, які працюють із громадянами ЄС. Поєднання вітчизняних норм і міжнародних стандартів створює цілісну правову основу для захисту мережевої інфраструктури та персональних даних у цифровому середовищі.

Основою мережевого захисту є модель тріади CIA (Confidentiality, Integrity, Availability), яка передбачає:

1. Конфіденційність: Цей принцип стосується забезпечення конфіденційності інформації, що означає, що лише уповноважені особи мають доступ до конфіденційних даних. Дані повинні бути захищені від несанкціонованого ознайомлення або розповсюдження. Для цього використовують механізми шифрування, автентифікацію користувачів та системи контролю доступу.

2. Цілісність: Цей принцип полягає у збереженні достовірності й незмінності інформації. Дані повинні бути захищені від випадкових або навмисних змін, що можуть порушити їх зміст. Для досягнення цього застосовують технології перевірки цілісності, резервне копіювання та системи виявлення несанкціонованого втручання.

3. Доступність: Цей принцип полягає в тому, що інформація та ресурси мають бути доступні для авторизованих користувачів у будь-який момент, коли це необхідно. Інформаційні системи повинні бути захищені від збоїв, технічних несправностей або атак, які можуть порушити їх роботу. Для забезпечення постійного доступу використовуються методи резервного копіювання, реплікації даних та інструменти аварійного відновлення[1].

Крім технічних засобів, значну роль відіграють організаційні заходи, такі як політики безпеки, навчання персоналу, аудит та моніторинг подій. Комплексне поєднання технічних та організаційних засобів дозволяє забезпечити високий рівень захисту інформації в мережевому середовищі.

Розвиток сучасних технологій, зокрема хмарних сервісів, мобільних пристроїв та штучного інтелекту, ставить нові виклики перед системами мережевої

безпеки. Постійне оновлення знань про методи захисту, їх ефективність та адаптація до нових умов є необхідною умовою підтримання високого рівня безпеки.

1.2 Огляд сучасних методів і моделей захисту інформації в мережах

Захист інформації в мережах є критично важливою складовою загальної системи інформаційної безпеки. З розвитком кіберзагроз з’являються нові методи та моделі захисту, які дозволяють ефективно протидіяти зловмисним діям, мінімізувати ризики витоку інформації та забезпечити безперебійну роботу інфокомунікаційних систем.

Методи захисту інформації в мережах можна поділити на організаційні, правові, та технічні.

Організаційні методи:

- створення політик безпеки;
- управління доступом до ресурсів;
- аудит безпеки;

Правові методи:

- Нормативно-правове регулювання
- Ліцензування та сертифікація
- Міжнародне правове регулювання

Технічні методи:

- використання мережевих екранів (фаєрволів);
- криптографічні методи
- системи виявлення та запобігання вторгненням (IDS/IPS);
- застосування віртуальних приватних мереж (VPN);
- сегментація мережі;
- антивірусний захист;
- автентифікація та авторизація користувачів

Сучасні моделі захисту базуються на концепції “глибокоешелонованого захисту” (Defense in Depth), яка передбачає багаторівневе застосування різних механізмів безпеки для забезпечення надійного бар’єру від загроз. Такий підхід враховує можливість порушення одного з рівнів і компенсується наступними.

Ще одним актуальним підходом є Zero Trust Model, модель побудови інформаційних систем, що виходить з того, що систему вже зламано, і тому довіряти не можна нікому. У такій моделі доступ до ресурсів надається тільки після багаторівневої перевірки і з мінімально необхідними правами.

Важливою є також концепція розподіленої безпеки (Distributed Security), що передбачає захист не лише периметра, а й безпосередньо кожного вузла, пристрою чи програми в мережі. Це особливо актуально в умовах широкого впровадження хмарних сервісів, мобільних пристроїв та Інтернету речей (IoT).

До новітніх методів також належать засоби, що використовують штучний інтелект та машинне навчання, для:

- виявлення аномальної поведінки в мережі;
- автоматичного реагування на кіберінциденти;
- прогнозування потенційних загроз.

Згідно з міжнародними стандартами, зокрема ISO/IEC 27001 та NIST Cybersecurity Framework, ефективне впровадження системи захисту інформації потребує поєднання політик, процесів, технологій та постійного моніторингу загроз.

Таким чином, сучасні методи захисту інформації в мережах постійно вдосконалюються, відповідаючи на нові виклики цифрової епохи. Аналіз існуючих рішень дозволяє визначити ключові напрями для подальшого дослідження та розробки більш ефективних підходів до забезпечення конфіденційності, цілісності та доступності інформації.

Метрики й показники ефективності.

Щоб об’єктивно оцінювати стійкість мережі та ефективність впроваджених заходів безпеки, організації використовують набір чітко визначених показників. Найважливіші з них - це середній час виявлення інцидентів (Mean Time To Detect),

середній час реагування на інциденти (Mean Time To Respond), частка інцидентів, спричинених людським фактором, кількість знайдених вразливостей та швидкість їх усунення, а також рівень відповідності дій корпоративним політикам безпеки.

Середній час виявлення інциденту вимірює проміжок від початку атаки до моменту її виявлення командою безпеки. Чим менший цей показник, тим швидше спрацьовують системи моніторингу та аналітики і тим менше збитків завдають зловмисники.

Середній час реагування відображає проміжок від виявлення інциденту до його повного нейтралізування та відновлення нормальної роботи системи. Ефективні процедури реагування та наявність чітких планів інцидент‑респонсу скорочують цей час і мінімізують тривалість простоїв[8].

Частка інцидентів, зумовлених людським фактором, дозволяє оцінити ефективність навчання персоналу та впроваджених політик безпеки. Соціальна інженерія, фішинг та помилкові налаштування користувачів часто стають причиною більшості витоків та атак, тому зниження цього показника свідчить про якісну програму підготовки й комунікацій.

Кількість виявлених вразливостей і темп їх усунення показують, наскільки оперативно організація реагує на нові ризики. Своєчасне сканування, патч‑менеджмент та управління конфігураціями забезпечують зменшення «вікна вразливості» та підвищують загальну безпеку.

Рівень відповідності корпоративним політикам безпеки вимірює, наскільки налаштування мережевих пристроїв, систем виявлення вторгнень, контролю доступу та інших засобів відповідають затвердженим стандартам і внутрішнім процедурам. Висока відповідність мінімізує ризик пропуску критичних налаштувань та забезпечує єдину основу для аудиту і скринінгу.

Застосування цих показників у комплексі дає змогу організаціям моніторити розвиток загрозового ландшафту, вчасно оптимізувати механізми захисту та приймати обґрунтовані рішення щодо інвестицій у безпеку.

Моделювання загроз Це структурований підхід, який допомагає ідентифікувати, оцінити та розставити пріоритети серед потенційних загроз для

захисту ресурсів організації. Воно складається з кількох етапів: визначення цінних активів, з’ясування меж довіри, побудова карти потоків даних, класифікація загроз та формулювання контрзаходів.

Ключовим результатом моделювання є пріоритезація ресурсів: ідентифікувавши найкритичніші загрози, можна спрямувати зусилля й бюджет на найбільш ефективні контрзаходи та уникнути неефективного розпилювання сил. Одночасно цей процес зменшує площу атаки, усуваючи зайві компоненти й шляхи доступу, які не відповідають бізнес‑цілям і створюють додаткові ризики.

Важливим ефектом є формування у команди культури безпеки: розробники, тестувальники та архітектори включають безпеку в свої щоденні практики, стають свідомими щодо можливих сценаріїв атаки та долучаються до пошуку контрзаходів. Це сприяє створенню цілісної системи, де безпека розглядається не як обтяжлива додаткова умова, а як невід’ємна складова якості й надійності продукту.

Також моделювання загроз забезпечує відповідність нормативним вимогам і стандартам управління ризиками. Використання його результатів у процесі оцінки та коригування політик безпеки гарантує, що організація не лише реагує на існуючі загрози, а й передбачає майбутні, підтримуючи свій захист на сучасному рівні[7].

1.3 Загрози конфіденційності даних в інформаційних мережах

У сучасних інформаційних мережах захист конфіденційності даних є важливою задачею, оскільки зростання обсягів переданої та обробленої інформації відкриває нові можливості для різних видів атак. Різноманітні типи обладнання, а також специфіка мережевих технологій визначають різні категорії загроз, які можуть виникати під час передачі, зберігання або обробки конфіденційної інформації.

Класи загроз.

Загрози конфіденційності можна класифікувати на кілька основних категорій:

1. Загрози, пов’язані з людським фактором:

Фішинг та соціальна інженерія: Зловмисники використовують техніки маніпуляції для отримання конфіденційної інформації від користувачів. Це можуть бути спроби отримати паролі або доступ до систем через шахрайські електронні листи чи вебсайти.

Внутрішні загрози: Співробітники компанії, що мають доступ до конфіденційних даних, можуть зловживати своїми правами або ненавмисно розголошувати важливу інформацію.

Недостатня кваліфікація персоналу: призводить до неправильного налаштування систем безпеки, використання слабких паролів і ігнорування політик доступу, що відкриває шлях для зловмисників.

Помилки користувачів (наприклад, відправка внутрішніх документів не тим адресатам або залишення флешок у публічному просторі) можуть викликати витік і втрату даних, а також порушення цілісності інформації.

2. Технічні загрози:

Атаки типу "man-in-the-middle" (MITM): Вони відбуваються, коли зловмисник перехоплює або змінює дані, що передаються між двома сторонами.

Шкідливе програмне забезпечення (Malware): Віруси, трояни, шпигунські програми та інше ПО можуть використовуватись для отримання доступу до конфіденційної інформації або для її викрадення.

DDoS-атаки (Distributed Denial of Service) полягають у масовому надсиланні запитів на цільовий сервер або мережевий пристрій з безлічі зламаних або проксі-систем, щоб вичерпати ресурси (процесор, пам’ять) і зробити сервіс недоступним.

Витоки даних через вразливості в системах зберігання та передачі: Неналежне шифрування, неправильні налаштування серверів та інші технічні помилки можуть призвести до витоку інформації[12].

3. Загрози, пов’язані з фізичним доступом до обладнання:

Фізичне втручання: Зловмисники можуть здобути доступ до серверів, баз даних або інших пристроїв, що зберігають конфіденційну інформацію, та викрасти або знищити її.

Невірне управління вразливими пристроями: Перехоплення інформації через слабкі або непідключені до захисту пристрої може призвести до порушення конфіденційності.

Класифікація загроз на основі типів використовуваного обладнання

Загрози конфіденційності можуть також бути класифіковані за різними типами обладнання, що використовуються для доступу до захищених масивів інформації. Це дозволяє розрізняти загрози, пов’язані з різними технічними засобами, що впливають на безпеку даних:

1. Загрози для мережевого обладнання:

Несправності в мережевих пристроях: Пошкодження маршрутизаторів, комутаторів, можуть призвести до втрати контролю над передачею або обробкою даних.

Атаки на комунікаційні канали: Зловмисники можуть використовувати слабкі місця в мережевих протоколах для несанкціонованого доступу до даних. Це включає атаки на протоколи передачі даних.

2. Загрози для кінцевих пристроїв (комп’ютери, мобільні пристрої):

Використання шкідливих додатків та програм: Шкідливі програми можуть проникати в системи через незахищені додатки або ненадійні джерела.

Загрози через мобільні пристрої: Мобільні телефони, планшети та інші портативні пристрої, що мають доступ до корпоративних мереж, можуть стати мішенню для кібератак, оскільки вони часто мають вразливі комунікаційні канали.

3. Загрози для серверів та сховищ даних:

Неавторизований доступ до серверів: Хакери можуть отримати доступ до серверів через слабкі паролі, вразливості в програмному забезпеченні або фізичне вторгнення.

Викрадення або модифікація даних в базах даних: Вразливості в системах управління базами даних можуть призвести до несанкціонованого доступу або зміни інформації.

4. Загрози для каналів зв’язку:

Шифрування каналів зв’язку: Якщо канали зв’язку між пристроями не зашифровані, то передана інформація може бути перехоплена зловмисниками.

Атаки на бездротові мережі: Бездротові технології, такі як Wi-Fi або Bluetooth, можуть бути вразливими для атак, що дозволяють перехоплювати або підміняти інформацію.

5. Загрози для хмарних сервісів:

Хмарні технології: Хоча хмарні сервіси забезпечують гнучкість, вони також несуть загрози через слабкі місця в системах безпеки або неправильне управління даними, що зберігаються на сторонніх серверах.

Класифікація загроз за типами технічних засобів доступу

1. Мережеві технічні засоби:

Загрози від атак на маршрутизатори, брандмауери, проксі-сервери та інші мережеві пристрої, що здійснюють контроль над трафіком і доступом до мережі.

Атаки через мережеві протоколи, такі як TCP/IP або DNS, що дозволяють отримати несанкціонований доступ до інформації або її змінити.

2. Програмні засоби:

Програмне забезпечення, яке використовується для шифрування даних, управління доступом або моніторингу безпеки, може стати вразливим через помилки в коді або невірні налаштування.

Зловмисники можуть розробляти програмне забезпечення, яке обминає захист або викрадає дані, використовуючи уразливості в програмних продуктах.

3. Апаратні засоби:

Загрози, пов’язані з апаратними засобами, можуть виникати через фізичне вторгнення або підробку. Використання невідомих або ненадійних пристроїв для підключення до мережі може створювати вразливості для витоку даних.

2 СУЧАСНІ ПІДХОДИ ДО ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Технічні засоби забезпечення безпеки інформації в мережі

Забезпечення інформаційної безпеки в сучасних інформаційно-комунікаційних системах вимагає використання широкого спектра технічних засобів, що здатні протидіяти різноманітним загрозам - від несанкціонованого доступу до витоку або втрати критичних даних. Технічні методи захисту інформації становлять основу функціонування комплексної системи захисту інформації (КСЗІ), оскільки забезпечують реалізацію практичних заходів контролю, шифрування, моніторингу та відновлення даних.

До основних технічних засобів належать міжмережеві екрани (фаєрволи), системи виявлення та запобігання вторгненням (IDS/IPS), криптографічні інструменти, системи резервного копіювання, системи контролю доступу, а також антивірусне програмне забезпечення. Кожен з цих компонентів виконує окрему, але взаємопов’язану функцію в межах загальної стратегії захисту, що дозволяє ефективно знижувати ризики інформаційної безпеки як у мережевому, так і в локальному середовищі.

У цьому розділі детально розглянуто принципи роботи, класифікацію, ключові особливості та приклади реалізації основних технічних засобів захисту інформації, що застосовуються в сучасних ІТС.

1. Міжмережеві екрани (фаєрволи)

Міжмережеві екрани - це програмні або апаратні засоби, що контролюють трафік, який надходить до комп’ютерної мережі або виходить з неї, на основі заданих правил безпеки.

Фаєрволи базуються на принципі білої або чорної списку - дозволяють або блокують трафік відповідно до заданих правил. Важливо правильно налаштувати правила, щоб уникнути як надмірного блокування, так і відкриття небажаних шляхів для атак. Зазвичай налаштування ведеться з урахуванням мінімально необхідного доступу (принцип найменших привілеїв).

Фаєрволи аналізують пакети даних, які проходять через мережевий інтерфейс, порівнюючи їх з попередньо визначеними правилами доступу. Якщо пакет відповідає дозволеним правилам, він пропускається, якщо ж ні - блокується або відхиляється.

Фаєрвол може працювати на різних рівнях моделі OSI (наприклад, мережевому, транспортному, прикладному) та реалізовувати як фільтрацію за IP-адресами, портами, так і глибокий аналіз пакетів (DPI - Deep Packet Inspection).

Типи Мережевих екранів:

Пакетні фільтри (Packet-filtering firewalls) - працюють на мережевому рівні (L3), аналізуючи IP-адреси, порти, протоколи.

Станові (Stateful inspection) - контролюють стан з'єднання, пам'ятають контекст сеансу.

Проксі-брандмауери (Application layer firewall) - функціонують на рівні додатків (L7), фільтруючи HTTP, FTP, SMTP, DNS трафік.

Next-Generation Firewall (NGFW) - поєднують декілька механізмів: IDS/IPS, DPI (глибоку перевірку пакетів), антивірусні функції.

Виклики та обмеження фаєрволів

Фаєрволи не можуть повністю захистити від атак, що здійснюються через легітимні відкриті порти або протоколи.

Висока складність налаштування у великих мережах може призводити до помилок і вразливостей.

Для шифрованого трафіку (наприклад, HTTPS) потрібне використання додаткових технологій для аналізу (SSL/TLS-інспекція), що збільшує навантаження на систему.

2. Системи виявлення та запобігання вторгненням (IDS/IPS).

IDS (Intrusion Detection System) і IPS (Intrusion Prevention System) - це засоби виявлення або запобігання несанкціонованим діям в інформаційній системі.

Принцип роботи IDS:

IDS здійснює моніторинг мережевого трафіку або дій у системі, шукаючи шаблони, які відповідають відомим загрозам або аномаліям. При виявленні

підозрілої активності система надсилає повідомлення адміністратору, але не втручається в трафік.

Принцип роботи IPS:

IPS працює подібно до IDS, але з додатковою функцією активного блокування виявлених загроз. Система автоматично перериває шкідливі сесії або змінює конфігурацію фаєрвола для запобігання атаці.

Методи роботи :Сигнатурний аналіз - порівняння з базою відомих атак. Аномалійний аналіз - виявлення відхилень від «нормальної» поведінки системи. Гібридні методи - поєднання вищезгаданих.

Протоколи та стандарти:

SNORT (стандарт для сигнатурного аналізу)

Suricata - IDS/IPS з підтримкою багатопотоковості

RFC 4765 - Intrusion Detection Message Exchange Format (IDMEF)

Крім класичних функцій, IDS/IPS часто інтегруються з системами управління подіями безпеки (SIEM), що дозволяє централізовано корелювати події безпеки з різних джерел і прискорювати реагування на інциденти. Також існують рішення, що поєднують функціонал IDS/IPS і фаєрволів (наприклад, NGFW), забезпечуючи багаторівневий захист.

3. Криптографічні методи (шифрування).

Криптографічні методи є фундаментальним засобом забезпечення конфіденційності інформації в інформаційно-комунікаційних системах. Вони дозволяють перетворювати відкриті дані у зашифровану форму, яка недоступна для несанкціонованого доступу або перехоплення під час передачі через незахищені канали. Конфіденційність досягається за рахунок використання криптографічних алгоритмів, які гарантують, що лише уповноважені суб’єкти з відповідним ключем можуть отримати доступ до вихідної інформації.

Криптографічні методи - це програмні або апаратні інструменти, що забезпечують конфіденційність, цілісність і автентичність даних шляхом перетворення інформації в недоступну для несанкціонованого користувача форму.

Нижче розглядаються основні методи шифрування, їх класифікація та принципи роботи.

Симетрична криптографія - це тип шифрування, в якому для перетворення відкритого тексту в шифрований (шифрування) і назад (дешифрування) використовується один і той самий секретний ключ. Основна перевага симетричної криптографії - висока швидкість обробки даних, що робить її ефективною для шифрування великих обсягів інформації. Проте головною проблемою є необхідність безпечної передачі секретного ключа між сторонами. Серед поширених алгоритмів цього типу:

– AES (Advanced Encryption Standard) - сучасний стандарт симетричного шифрування, прийнятий як міжнародний стандарт. Працює з блоками даних розміром 128 біт і підтримує ключі довжиною 128, 192 або 256 біт. Застосовується в більшості сучасних систем безпеки через свою надійність та ефективність.

– DES (Data Encryption Standard) - раніше широко використовувався стандарт, який сьогодні вважається застарілим через невелику довжину ключа (56 біт), що робить його вразливим до атак методом повного перебору.

Алгоритми симетричного шифрування зазвичай перевершують асиметричні за швидкодією та ефективністю, однак їх використання передбачає наявність спільного секретного ключа в обох сторін обміну - відправника і одержувача.

Вони також вважаються менш безпечними, оскільки для шифрування та дешифрування використовується один і той самий ключ. У разі його компрометації під загрозою опиняється безпека всієї криптосистеми.

Асиметрична криптографія - це система, в якій використовуються два ключі: публічний і приватний. Публічний ключ використовується для шифрування, а приватний - для дешифрування. Така схема забезпечує можливість безпечної передачі інформації без потреби попереднього обміну секретами. Асиметричні алгоритми мають вищу обчислювальну складність і зазвичай повільніші, тому їх часто застосовують для захисту симетричних ключів, а не для шифрування великих обсягів даних.

На відміну від симетричних алгоритмів, які використовують один і той самий ключ для шифрування та розшифрування даних, асиметричні алгоритми застосовують пару ключів - відкритий і закритий. Такий підхід забезпечує вищий рівень безпеки та зручність при обміні інформацією.

Відкритий (публічний) ключ - це криптографічний ключ, який доступний будь-кому і може бути використаний для шифрування повідомлень, що надсилаються конкретному адресатові. Розшифрувати ці повідомлення може лише власник відповідного закритого (приватного) ключа, який зберігається в таємниці.

Коли хтось хоче надіслати зашифроване повідомлення, він отримує публічний ключ одержувача і використовує його для шифрування повідомлення. Після доставки повідомлення лише одержувач, який має відповідний приватний ключ, зможе його розшифрувати.

У сучасному цифровому середовищі найчастіше застосовуються два основних асиметричних алгоритми - RSA та ECC.

– RSA (Rivest–Shamir–Adleman) - один із найвідоміших алгоритмів, заснований на складності факторизації великих простих чисел. Підтримує цифровий підпис, шифрування і забезпечення цілісності даних.

Ключі RSA зазвичай мають розмір 1024 або 2048 біт, однак фахівці в галузі безпеки вважають, що 1024-бітові ключі вже незабаром можуть стати вразливими до зламу. У зв’язку з цим урядові структури та промислові організації поступово переходять на використання ключів довжиною не менше 2048 біт як нового мінімального стандарту.

– ECC (Elliptic Curve Cryptography) - криптографія на еліптичних кривих. Забезпечує таку саму безпеку, як RSA, при значно меншій довжині ключа, що знижує навантаження на процесор і пам’ять. Особливо популярна у мобільних пристроях, смарт-картах та IoT.

Гібридна криптографія - поєднує симетричну і асиметричну криптографію для досягнення оптимального рівня безпеки і продуктивності. У такій схемі спочатку використовується асиметричне шифрування для безпечної передачі симетричного ключа, а далі для шифрування даних використовується вже цей

симетричний ключ. Це дозволяє уникнути проблем із безпекою при передаванні ключа і забезпечити швидке шифрування великих обсягів інформації.

– TLS (Transport Layer Security) - типовий приклад гібридної криптосистеми, що використовується для захисту з’єднань в інтернеті (наприклад, HTTPS). На початку сеансу клієнт і сервер використовують асиметричне шифрування для обміну симетричним ключем, після чого весь трафік шифрується симетрично.

4. Системи резервного копіювання та відновлення.

Принцип роботи: Ці системи зберігають копії критичних даних, які можна швидко відновити у випадку втрати, знищення або пошкодження основної інформації. Застосовуються в рамках політик безперервності бізнесу (BCP) та відновлення після катастроф (DRP).

Типи резервного копіювання:

Повне (Full)

Інкрементне (Incremental)

Диференційне (Differential)

Реплікація в реальному часі (real-time replication)

5. Системи контролю і управління доступом (СКУД) - це сукупність організаційних, програмних та апаратних засобів, що забезпечують управління правами користувачів і пристроїв на доступ до інформаційних ресурсів, об’єктів інфраструктури або окремих функцій у межах мережі. Головна мета таких систем - гарантувати, що доступ до конфіденційної або критично важливої інформації надається лише уповноваженим особам відповідно до заздалегідь визначених правил і політик.

Класифікація СКУД за методом доступу.

– Дискреційний метод контролю доступу (DAC) - доступ до ресурсів визначається власником ресурсу. Кожен об’єкт має список користувачів та їхніх прав (читання, запис, виконання тощо). Приклад: файлові системи Windows NTFS, Unix/Linux. Такий підхід є гнучким, але менш безпечним, оскільки користувачі можуть самостійно змінювати права доступу.

– Мандатний метод контролю доступу (MAC) - доступ до інформації регламентується централізовано за допомогою політик безпеки. Кожному об’єкту та суб’єкту привласнюється рівень секретності, і лише ті користувачі, які мають належний рівень допуску, можуть отримати доступ. Широко застосовується в державних органах і критично важливих IT-системах.

– Рольовий метод контролю доступу (RBAC) - права доступу надаються на основі ролей, які закріплені за користувачами. Користувач отримує доступ до ресурсів відповідно до своєї ролі (наприклад, «адміністратор», «оператор», «аналітик»), що спрощує керування великими системами. Цей підхід є зручним у корпоративних середовищах.

– Атрибутний метод контролю доступу (ABAC) - рішення про доступ приймається на основі атрибутів користувача, ресурсу, середовища або дії. Наприклад, атрибутами можуть бути місце входу, час доступу, пристрій, група користувача. Це найбільш гнучка модель, яка дозволяє реалізовувати динамічні політики безпеки.

Принцип роботи систем контролю доступу.

СКУД функціонують за типовим циклом:

ідентифікація → автентифікація → авторизація → аудит.

Ідентифікація - процес визначення користувача або пристрою за унікальним ідентифікатором (логін, ID-картка, токен, MAC-адреса).

Автентифікація - перевірка достовірності заявленої особи. Здійснюється за допомогою пароля, біометричних даних, смарт-картки, токена, багатофакторної автентифікації (2FA/MFA).

Авторизація - надання або заборона доступу до об’єктів системи відповідно до прав користувача або політик безпеки.

Аудит - фіксація дій користувача, журналювання спроб доступу, виявлення аномалій і порушень. Важливий елемент для виявлення інцидентів безпеки.

СКУД можуть реалізовуватись за допомогою програмних рішень (наприклад, систем управління ідентифікацією та доступом), апаратних засобів (електронні ключі, біометричні сканери) або комбінованих підходів. У сучасних ІТС велике

значення має багатофакторна автентифікація, яка підвищує надійність контролю доступу.

6. Антивірусне програмне забезпечення - це засіб захисту інформації, що забезпечує виявлення, блокування та видалення шкідливих програм (вірусів, троянів, шпигунів, криптолокерів тощо).

Основні функції:

– Сканування файлів і системи

– Захист у реальному часі

– Виявлення нових загроз за поведінкою

– Карантин заражених об’єктів

– Регулярне оновлення сигнатур

Принципи роботи:

– Сигнатурний аналіз - пошук відомих вірусів за базою

– Евристичний аналіз - виявлення нових загроз за поведінкою

– Хмарні технології - перевірка файлів на сервері виробника

– Ізоляція загроз - запобігання їхньому поширенню

Типи антивірусів:

– Резидентні (працюють постійно)

– Сканери на вимогу

– Онлайн-сканери

– Корпоративні рішення з централізованим управлінням

Антивіруси - базовий компонент безпеки, особливо ефективний у поєднанні з фаєрволами, IDS/IPS і контролем доступу.

Отже, технічні засоби захисту інформації є критичним елементом забезпечення безпеки інформаційно-комунікаційних систем. Їхнє комплексне застосування - від фаєрволів і IDS/IPS до криптографічних модулів, резервного копіювання та систем контролю доступу - дозволяє ефективно протидіяти широкому спектру загроз. Сучасні вимоги до захисту інформації зумовлюють необхідність інтеграції зазначених засобів у єдину інфраструктуру, що забезпечує

як захист периметра, так і глибоке багаторівневе управління ризиками інформаційної безпеки.

2.2 Стратегії захисту: превентивна, виявлення, реагування

Побудова ефективної системи захисту інформації базується на трьох фундаментальних стратегіях: превентивній, стратегії виявлення та стратегії реагування. Їх поєднання забезпечує цілісне, багаторівневе забезпечення безпеки ІТС, дозволяючи не лише запобігати атакам, а й ефективно реагувати на інциденти, що все ж відбулися.

1. Превентивна стратегія (запобігання загрозам)

Мета цієї стратегії - недопущення виникнення загроз шляхом створення бар’єрів до інформаційних ресурсів системи. До основних превентивних заходів належать:

– Аутентифікація та авторизація користувачів - забезпечують доступ до ресурсів лише авторизованим суб’єктам із відповідними правами;

– Шифрування даних - захищає конфіденційність інформації під час зберігання та передавання;

– Мережева ізоляція - сегментація мережі, застосування VLAN, DMZ для обмеження розповсюдження атак;

– Механізми контролю доступу - реалізуються через ACL, політики безпеки, MAC/RBAC/ABAC-моделі;

– Фаєрволи та системи фільтрації трафіку - блокують небажані або шкідливі з’єднання;

– Оновлення ПЗ та усунення вразливостей - критичний елемент у запобіганні експлуатації відомих уразливостей;

– Навчання персоналу - дозволяє уникнути атак соціальної інженерії, фішингу тощо.

Превентивна стратегія зменшує ймовірність успішного здійснення атаки, однак не гарантує абсолютного захисту, оскільки завжди існує ризик появи нових, ще невідомих загроз (zero-day атак).

2. Стратегія виявлення

Ця стратегія спрямована на якнайшвидше виявлення фактів порушень безпеки або аномальної активності, що може свідчити про атаку. Основні інструменти реалізації:

– Системи виявлення вторгнень (IDS) - аналізують трафік або журнали подій для виявлення підозрілої активності;

– Системи моніторингу (SIEM, NIDS, HIDS) - централізовано збирають, корелюють та аналізують події безпеки з різних джерел;

– Журнали подій і аудит - дозволяють виявити підозрілу поведінку користувачів або процесів;

– Системи поведінкового аналізу (UEBA) - фіксують відхилення від нормальної поведінки користувача чи пристрою.

Час виявлення інциденту - критично важливий параметр, що безпосередньо впливає на збитки від інциденту. Чим швидше виявлена атака, тим менші її наслідки.

3. Стратегія реагування (відновлення та протидія)

Ця стратегія передбачає вжиття заходів після виявлення інциденту безпеки з метою мінімізації його наслідків, відновлення нормального функціонування системи та запобігання повторним подіям. Основні складові:

– План реагування на інциденти (IRP) - набір документованих процедур для оперативного реагування на різні типи загроз;

– Ізоляція уражених компонентів - обмеження поширення атаки шляхом блокування доступу до заражених систем;

– Форензіка (розслідування інциденту) - вивчення причин і способів атаки для покращення захисту в майбутньому;

– Відновлення з резервних копій - відновлення даних і систем після знищення або модифікації;

– Оповіщення відповідальних осіб та держорганів - відповідно до вимог законодавства та політик безпеки;

– Аналіз ефективності реагування - з метою коригування політик та оновлення процедур IRP.

Реагування повинно бути швидким, чітким і узгодженим - від цього залежить стійкість ІТС до атак і її здатність до відновлення.

Взаємодія трьох стратегій

Жодна зі стратегій не є самодостатньою. Успішна система захисту реалізує їх як єдиний безперервний цикл, наведений на рис.2.1

Рисунок 2.1 – Взаємодія стратегій захисту

Такий підхід забезпечує багаторівневий захист і дає змогу ефективно протидіяти навіть складним і комплексним атакам.

Аналіз стратегій захисту показав, що кожна з них виконує ключову роль у забезпеченні цілісності, конфіденційності та доступності інформації. Превентивна стратегія зменшує ймовірність успішної атаки шляхом впровадження технічних і організаційних заходів захисту. Стратегія виявлення дозволяє оперативно ідентифікувати інциденти безпеки завдяки використанню сучасних аналітичних інструментів. Реагування забезпечує мінімізацію шкоди та швидке відновлення функціонування системи після інциденту. Застосування цих стратегій у сукупності забезпечує гнучкість і адаптивність Систем захисту до змін у загрозовому середовищі.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ

3.1 Опис вибраних технічних засобів і їх налаштування

Забезпечення інформаційної безпеки в сучасному цифровому середовищі є критично важливим завданням для організацій та державних структур. Зростання кіберзагроз, витоків даних та несанкціонованого доступу до інформації вимагає впровадження ефективних технічних засобів захисту. Ці засоби повинні гарантувати конфіденційність, цілісність та доступність інформації, а також забезпечувати своєчасне виявлення та реагування на потенційні загрози.

У цьому контексті важливими компонентами системи інформаційної безпеки є фаєрволи, системи виявлення та запобігання вторгнень, криптографічні методи, системи резервного копіювання та відновлення, системи контролю доступу та антивірусне програмне забезпечення. Кожен з цих елементів відіграє ключову роль у захисті інформаційних ресурсів від різноманітних загроз та забезпечує надійне функціонування інформаційних систем.

У далі буде розглянуто призначення, функціональні можливості та особливості впровадження кожного з вищезазначених технічних засобів захисту інформації.

1. Міжмережеві екрани (фаєрволи)

Міжмережевий екран нового покоління (Next‑Generation Firewall, NGFW) поєднує традиційну фільтрацію пакетів із глибинним аналізом трафіку й інтегрованим IDS/IPS-модулем.

NGFW забезпечує application awareness, що дозволяє ідентифікувати й блокувати конкретні додатки незалежно від порту чи протоколу.

Засоби Threat Intelligence у NGFW отримують оновлення з хмарних сервісів, що дозволяє оперативно реагувати на нові загрози.

NGFW підтримують глибоку інспекцію пакетів (DPI), що виявляє атаки на прикладному рівні, наприклад SQL‑ін’єкції чи експлойти протоколів[13].

Вибір фаєрвола:

Вибір між апаратним та програмним фаєрволом залежить від кількох факторів:

Розмір та складність мережі: Для великих мереж з високими вимогами до продуктивності та безпеки доцільно використовувати апаратні фаєрволи, які забезпечують централізований захист і не навантажують системні ресурси окремих пристроїв. Для менших мереж або окремих пристроїв можуть бути достатніми програмні фаєрволи.

Бюджет: Апаратні фаєрволи зазвичай мають вищу вартість, включаючи витрати на обладнання та обслуговування. Програмні фаєрволи можуть бути більш економічними, особливо для малих підприємств або домашніх користувачів.

Технічна експертиза: Апаратні фаєрволи можуть вимагати спеціалізованих знань для налаштування та обслуговування, тоді як програмні фаєрволи зазвичай мають більш інтуїтивно зрозумілий інтерфейс.

Налаштування фаєрвола:

Політики доступу: Визначення чітких правил, які дозволяють або забороняють трафік на основі IP-адрес, портів та протоколів.

Моніторинг та ведення журналів: Регулярний аналіз журналів фаєрвола для виявлення аномальної активності та потенційних загроз.

Оновлення та підтримка: Забезпечення своєчасного оновлення програмного забезпечення фаєрвола для захисту від нових вразливостей.

2. Системи виявлення та запобігання вторгненням (IDS/IPS)

Для наочності розглянемо систему Suricata - відкрите високопродуктивне рішення, яке поєднує NIDS/NIPS (Network - based Intrusion Prevention, NIPS) і підтримує багатопотоковий аналіз мережевого трафіку.

Система використовує сигнатурний аналіз для виявлення відомих загроз і аномалійний аналіз для відстеження невідомих атак.

У режимі IPS Suricata здатна активно блокувати шкідливі пакети, модифікуючи правила на фаєрволі чи одночасно відхиляючи підозрілий трафік.

Для ефективного захисту рекомендується регулярно оновлювати сигнатурні бази з офіційних репозиторіїв Suricata (рис.3.1) або Emerging Threats.

Інтеграція з SIEM-системою дозволяє проводити кореляцію подій та швидше реагувати на складніші багатостадійні атаки.

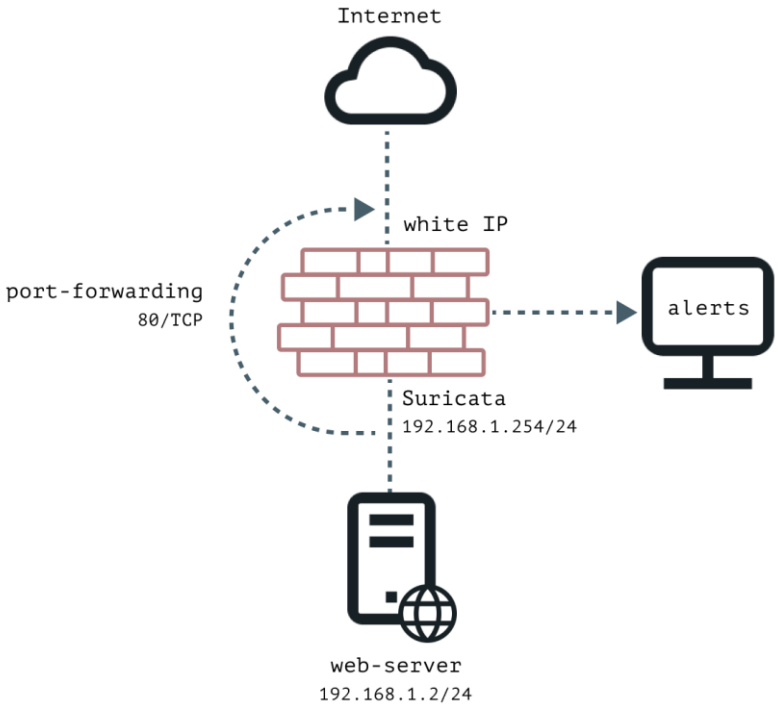

Рисунок 3.1 – Мережева схема на основі Suricata

У цій схемі (рис.3.1) між цільовим веб-сервером та Інтернетом встановлено систему виявлення та запобігання вторгненням (IDPS). Вона виконує функції маршрутизації та переадресації портів. Завдяки такому розміщенню, за умови правильної конфігурації, можливо блокувати шкідливий трафік у разі спрацювання відповідних сигнатур[14].

3. Криптографічні методи

Криптографія забезпечує конфіденційність та цілісність даних за допомогою симетричних і асиметричних алгоритмів.

Симетричні алгоритми (наприклад, AES‑256) швидкі та ефективні для шифрування великих обсягів даних; їх безпечний обмін ключами реалізується через асиметричне шифрування (RSA, ECC).

Асиметричні методи (RSA з мінімальною довжиною ключа 2048 біт, ECC) використовуються для обміну ключами та цифрових підписів.

Протоколи TLS/SSL застосовуються для захисту веб‑сервісів, забезпечуючи гібридне шифрування, коли асиметрія використовується для передачі симетричного ключа, а далі трафік шифрується симетрично.

Відповідність стандартам (TLS 1.3, NIST SP 800‑57) гарантує стійкість до сучасних криптоатак.

Вибір алгоритмів:

Симетричне шифрування: Використання алгоритмів, таких як AES, для шифрування великих обсягів даних.

Асиметричне шифрування: Використання алгоритмів, таких як RSA або ECC, для безпечного обміну ключами та цифрового підпису.

Управління ключами:

Системи управління ключами (KMS): Забезпечення безпечного зберігання та обміну ключами.

Ротація ключів: Регулярна зміна ключів для зменшення ризику компрометації.

Ієрархія ключів: Використання майстер-ключів та користувацьких ключів для спрощення управління та підвищення безпеки.

4. Системи резервного копіювання та відновлення

Технології резервного копіювання передбачають повні, диференційні та інкрементні копії даних для швидкого відновлення систем після інцидентів.

Системи повинні підтримувати незмінниі знімки (immutable snapshots), що захищають резервні копії від модифікації зловмисниками та програмами‑вимагачами (ransomware).

Для корпоративних рішень важливо використовувати реплікацію в реальному часі (real‑time replication) та географічно розподілені сховища для забезпечення безперервності бізнес-процесів.

Додатково впроваджують план відновлення після катастроф (Disaster Recovery Plan) з тестуванням процедур відновлення не рідше ніж раз на квартал.

Стратегії резервного копіювання:

Повне резервне копіювання: Копіювання всіх даних.

Інкрементальне копіювання: Копіювання лише змінених даних з моменту останнього резервного копіювання.

Диференційне копіювання: Копіювання змінених даних з моменту останнього повного резервного копіювання.

Налаштування системи:

Автоматизація: Налаштування автоматичного створення резервних копій за розкладом.

Зберігання копій: Застосування правила 3-2-1: три копії даних, на двох різних носіях, одна з яких зберігається поза основним місцем роботи.

Тестування відновлення: Регулярне перевіряння можливості відновлення даних з резервних копій для забезпечення їх надійності.

5. Системи контролю доступу

Основні моделі: дискреційна (DAC), мандатна (MAC), рольова (RBAC) та атрибутна (ABAC) контроль доступу.

RBAC дозволяє централізовано керувати правами на основі ролей користувачів, що спрощує адміністрування в великих організаціях.

ABAC забезпечує динамічне прийняття рішень на підставі атрибутів користувача, ресурсу та середовища (час, місце, пристрій тощо).

Для аутентифікації використовують багатофакторну автентифікацію (MFA), що поєднує пароль, смарт-картку або OTP-додаток.

Централізоване управління політиками через LDAP/Active Directory інтегрується з SIEM для аудиту і виявлення порушень політик доступу.

Налаштування системи:

Ідентифікація та автентифікація: Впровадження механізмів двофакторної автентифікації та єдиного входу (SSO).

Політики доступу: Створення політик доступу відповідно до ролей або атрибутів користувачів.

Аудит: Регулярний перегляд прав доступу та їх оновлення при зміні ролей або обов’язків.

6. Антивірусне програмне забезпечення

Антивіруси здійснюють сигнатурний аналіз для виявлення відомих шкідливих програм і евристичний аналіз для виявлення нових загроз.

Резидентні сканери забезпечують реальний час захисту, автоматично перевіряючи файли та процеси при доступі до них.

Онлайн‑сканери і керовані корпоративні рішення централізовано оновлюють бази даних загроз і розподіляють політики безпеки на всі пристрої.

Антивірусні шлюзи на рівні електронної пошти та веб-фільтри блокують шкідливі вкладення й посилання до їхньої доставки кінцевому користувачеві.

Рекомендовано підтримувати активні оновлення сигнатур і періодично проводити повні сканування критичних серверів і робочих станцій.

7. Мережева ізоляція та сегментація - це методи підвищення безпеки в інформаційно-комунікаційних системах шляхом поділу мережі на логічні або фізичні частини для обмеження поширення загроз і контролю доступу.

Мережева ізоляція - це процес розділення окремих частин інформаційно-комунікаційної системи таким чином, щоб обмежити або повністю виключити обмін даними між ними. Її мета - мінімізувати ризики поширення шкідливого програмного забезпечення, несанкціонованого доступу або витоку інформації між сегментами мережі. Ізоляція може бути фізичною (окреме обладнання, кабелі) або логічною (віртуальні локальні мережі, фаєрволи, VPN).

Сегментація мережі - це поділ великої комп’ютерної мережі на менші логічні підмережі, або сегменти, з метою підвищення рівня безпеки, продуктивності та керованості. Кожен сегмент може мати власні політики безпеки, правила доступу та моніторингу. Сегментація дозволяє контролювати рух даних між сегментами, швидше виявляти та локалізовувати інциденти, а також зменшує потенційний обсяг збитків у разі компрометації окремої ділянки мережі.

Для реалізації цієї концепції використовуються такі підходи:

VLAN (Virtual Local Area Network)

VLAN дозволяє логічно розділити фізичну мережу на ізольовані сегменти на рівні канального рівня (OSI Layer 2). Це забезпечує ізоляцію трафіку між різними

групами користувачів або службами, навіть якщо вони підключені до одного фізичного комутатора.

Переваги:

Ізоляція трафіку Зменшує ризик несанкціонованого доступу між сегментами.

Гнучкість Дозволяє легко змінювати мережеву структуру без фізичного переміщення обладнання.

Покращена продуктивність Зменшує мережеве навантаження, обмежуючи широкомовні домени.

Приклад: Розділення мережі на окремі VLAN для відділів бухгалтерії, HR та IT, що дозволяє обмежити доступ до конфіденційних даних лише уповноваженим користувачам.

2. DMZ (Demilitarized Zone)

DMZ - це ізольована зона мережі, розташована між внутрішньою мережею організації та зовнішніми мережами, такими як Інтернет. Вона використовується для розміщення публічно доступних сервісів, таких як веб-сервери, поштові сервери або FTP-сервери.

Переваги:

Захист внутрішньої мережі: Навіть у разі компрометації сервера в DMZ, зловмисник не отримає прямого доступу до внутрішньої мережі.

Контрольований доступ: Зовнішні користувачі мають доступ лише до сервісів у DMZ, без можливості проникнення у внутрішню мережу.

Приклад: Розміщення веб-сервера в DMZ, який обробляє запити від клієнтів, при цьому база даних залишається у внутрішній мережі, доступ до якої обмежений.

3. Архітектура Zero Trust

Архітектура Zero Trust базується на принципі "нікому не довіряти за замовчуванням". Це означає, що кожен запит на доступ до ресурсів повинен бути автентифікований, авторизований та перевірений на відповідність політикам безпеки, незалежно від того, чи знаходиться користувач всередині або поза межами мережі.

Ключові принципи:

Мінімальні привілеї: Користувачам надається лише той рівень доступу, який необхідний для виконання їхніх обов’язків.

Постійна перевірка: Кожен запит перевіряється на відповідність політикам безпеки, незалежно від попередніх авторизацій.

Мікросегментація: Розділення мережі на дрібні сегменти для обмеження переміщення зловмисників у разі компрометації.

Застосування мережевої ізоляції та сегментації за допомогою VLAN, DMZ та архітектури Zero Trust дозволяє організаціям створити багаторівневу систему захисту, яка ефективно протистоїть сучасним кіберзагрозам та забезпечує безпеку критичних ресурсів[15].

Перспективні технології мережевого захисту

У швидкозмінному середовищі кіберзагроз найбільш ефективні рішення поєднують традиційні технічні засоби із сучасними автоматизованими та аналітичними платформами. Серед технологій, які вже сьогодні формують наступне покоління систем безпеки, виділяють інтеграцію з хмарними SIEM/SOAR‑сервісами, впровадження User and Entity Behavior Analytics (UEBA) та застосування машинного навчання й штучного інтелекту для виявлення аномалій і автоматизованого реагування.

Хмарні SIEM/SOAR‑сервіси

Системи управління інформацією та подіями безпеки (Security Information and Event Management, SIEM) в хмарному виконанні дозволяють централізувати збір, кореляцію та зберігання великих обсягів логів із різнорідних джерел без необхідності розгортання власної інфраструктури. Хмарні SIEM‑платформи гарантують майже необмежені ресурси обробки й зберігання, автоматичні оновлення сигнатур та політик, а також можливість швидкого масштабування під пікові навантаження.

Сервіси оркестрації, автоматизації та реагування на інциденти (Security Orchestration, Automation and Response, SOAR) доповнюють SIEM‑функціонал сценаріями автоматичного реагування: виявленням загрози → підтвердженням →

блокуванням на межі мережі або вразливому вузлі → створенням задачі для аналітика. Це значно скорочує час від виявлення інциденту до його нейтралізації та знижує навантаження на команду операційної безпеки.

User and Entity Behavior Analytics (UEBA)

UEBA‑ рішення аналізують поведінку користувачів та пристроїв у мережі, створюючи профілі нормальної активності та виявляючи відхилення. У той час, як традиційні системи оперують сигнатурами відомих загроз, UEBA шукає аномалії - нетипові спроби доступу, незвичну інтенсивність передавання даних, використання нових протоколів чи віддалених точок з’єднання. Використання UEBA особливо ефективне для виявлення внутрішніх загроз і атак «людина посередині», які залишають мінімальний слід у сигнатурних базах.

Машинне навчання та штучний інтелект

Моделі машинного навчання (ML) і алгоритми штучного інтелекту (AI) все активніше використовуються для класифікації мережевого трафіку, розпізнавання патернів шкідливої поведінки та прогнозування вразливостей. Статистичні методи та нейронні мережі аналізують потоки даних у реальному часі, автоматично налаштовують пороги спрацювань та рекомендують нові правила фаєрволу або IDS/IPS. Застосування AI також відкриває можливості для самообучувальних систем, які з часом виявляють і придушують атаки, про які ще не відомо сигнатурам.

3.2 Оцінка вартості та доцільності впровадження технічних засобів

У реаліях динамічного зростання кіберзагроз і постійного розширення IT‑ інфраструктур організацій особливого значення набуває не лише технічна спроможність засобів захисту, але й їх економічна обґрунтованість. Аналіз повної вартості володіння (Total Cost of Ownership) та розрахунок рентабельності інвестицій (Return on Investment) дозволяють приймати зважені рішення щодо вибору між відкритими та комерційними рішеннями, планувати бюджет на

придбання й підтримку систем захисту, а також оцінювати доцільність їхнього масштабування.

Перш ніж обирати інструменти для захисту мережі, необхідно зважити не лише їхню технічну ефективність, а й економічну доцільність. Два основні показники тут - повна вартість володіння та рентабельність інвестицій.

1. Повна вартість володіння

Повна вартість володіння включає всі витрати на придбання, впровадження, експлуатацію і підтримку рішення протягом усього його життєвого циклу:

– Прямі витрати

Ліцензійні платежі (для комерційного програмного забезпечення) або закупівля обладнання.

Вартість встановлення й налаштування (зокрема, залучення фахівців чи навчання персоналу).

Контракти з технічної підтримки та обслуговування.

– Непрямі витрати

Вплив на роботу мережі та серверів (затримки, зниження пропускної спроможності).

Супровідні витрати на модернізацію інфраструктури (наприклад, додаткові ресурси для віртуальних машин).

Час і ресурси на тестування оновлень та патчів.

– Витрати, пов’язані з ризиками

Оцінка таких втрат, як простої бізнес-процесів, штрафи за порушення регуляторних вимог, відновлення після кібератак.

Витрати на розслідування та усунення наслідків інцидентів.

2. Рентабельність інвестицій (Return on Investment)

Рентабельність показує, наскільки вкладені кошти виправдовуються з точки зору уникнутих витрат і додаткових вигод:

– Уникнені витрати

Зниження кількості та вартості інцидентів безпеки.

Скорочення простоїв і витрат на відновлення систем.

– Додаткові вигоди

Підвищення продуктивності за рахунок автоматизації захисних процесів.

Зростання довіри партнерів і клієнтів завдяки дотриманню кращих практик безпеки.

Зменшення адміністративного навантаження на IT‑ відділ.

3. Порівняння комерційних і відкритих (open‑ source) рішень наведено в табл. 3.1.

Таблиця 3.1- Порівняння комерційних і відкритих рішень

Критерій	Комерційні рішення	Відкриті рішення
Ліцензійні витрати	Високі, переважно щорічні	Не вимагають ліцензійних платежів
Технічна підтримка	Професійна служба з гарантіями	Спільнотна, зазвичай без формальних угод
Швидкість впровадження	Готові інсталятори та шаблони конфігурацій	Потребує більше часу на налаштування
Масштабованість	Інтегровані апаратно‑ програмні платформи	Гнучкість, але може вимагати ресурсів фахівців
Загальна вартість володіння (TCO)	Залежить від SLA та сервісних контрактів	Нижча при наявності внутрішніх ресурсів
Рентабельність (ROI)	Швидка окупність завдяки підтримці	Вища довгострокова ефективність

Наведена таблиця порівнює комерційні та відкриті (open‑ source) рішення за шістьма ключовими критеріями. Усі вони пов’язані з витратами, підтримкою й масштабованістю, тобто з тими аспектами, які напряму впливають на повну вартість володіння та рентабельність інвестицій.

По-перше, витрати на ліцензії для комерційних продуктів зазвичай є істотними й повторюваними: щорічні платежі покривають саму програму,

підтримку та оновлення. У випадку open‑source рішень ліцензійних витрат немає, проте організація бере на себе витрати на навчання, настройку та внутрішню підтримку, що теж потрібно враховувати в бюджеті.

По‑друге, рівень технічної підтримки прямо корелює з ліцензійною моделлю: комерційні вендори гарантують швидке реагування та офіційні оновлення в рамках угоди про рівень обслуговування, тоді як open‑source продукти в основному покладаються на спільноту та наявні в організації експертні ресурси.

Третій критерій - швидкість впровадження. Готові пакети, шаблони конфігурацій і професійна підтримка дозволяють комерційним рішенням запрацювати швидко. Open‑source продукти, навпаки, вимагають більше часу на вибір найкращих модулів, інтеграцію та тестування, що збільшує початковий цикл розгортання.

По‑четверте, масштабованість: апаратно‑програмні платформи вендорів зазвичай мають вбудовані механізми кластеризації, балансування навантаження й централізованого управління, що полегшує розширення інфраструктури. У відкритих систем це теж можливо, але значною мірою воно залежить від інженерних навичок команди та часом потребує сторонніх модулів або скриптів.

Фінальні два показники - загальна вартість володіння й рентабельність інвестицій. вартість володіння комерційних рішень вища за рахунок ліцензій і контрактів на підтримку, але швидка окупність досягається завдяки скороченню ризиків та швидкій інтеграції. У випадку open‑source нижчі початкові витрати компенсуються витратами на внутрішню підтримку й довшим періодом налаштування, проте в довгостроковій перспективі рентабельність може бути вищею через відсутність повторних ліцензійних платежів.

4. Метрики ефективності

Для об’єктивної оцінки роботи систем безпеки використовують такі показники:

– Середній час виявлення інциденту (Mean Time To Detect, MTTD) - час від початку атаки до моменту її виявлення.

– Середній час реагування (Mean Time To Respond, MTTR) - час від виявлення інциденту до його повного усунення.

– Кількість заблокованих атак на одиницю часу.

– Рівень хибних спрацювань - відсоток сповіщень, що виявилися помилковими.

Ці метрики збирають у централізованій системі інформації та подій безпеки (Security Information and Event Management), а потім аналізують для оптимізації політик і процесів.

5. Рекомендації з економічної оцінки

Пілотне впровадження

Запуск мінімального функціонального набору в обмеженому сегменті допомагає оцінити реальні витрати та вигоди перед масштабним розгортанням.

Гібридний підхід

Використовувати відкриті рішення для базових і комерційні продукти в критичних зонах з високими вимогами до SLA. Це дозволяє знизити загальні витрати, зберігаючи рівень підтримки там, де він найнеобхідніший.

Автоматизація збору показників

Інтеграція з платформами SOAR (Security Orchestration, Automation and Response) або SIEM для автоматичного збору та обробки KPI дає змогу швидко оцінювати поточний стан безпеки і економити ресурси аналітиків.

Регулярний перегляд фінансових результатів

Періодично проводити фінансовий аналіз, порівнювати фактичні витрати та вигоди з початковими оцінками, коригувати стратегію закупівель і оновлень.

Вибір і впровадження технічних засобів захисту необхідно здійснювати з урахуванням повної вартості їх володіння та очікуваного рівня окупності. Системний підхід до економічної оцінки дозволяє оптимізувати бюджет, підвищити ефективність безпеки та знизити фінансові ризики, пов’язані з кіберінцидентами.

У результаті дослідження ключових технічних засобів захисту інформації - від міжмережевих екранів і систем виявлення/запобігання вторгнень до

криптографічних модулів, резервного копіювання, контрольованого доступу й антивірусних рішень - було підтверджено, що тільки їхня взаємодія в єдиній, узгодженій інфраструктурі здатна гарантувати комплексний захист мережі. Кожний компонент виконує свою специфічну роль: фаєрволи відсікають небажаний трафік на периметрі, IDS/IPS виявляють і блокують шкідливі патерни всередині мережі, криптографія забезпечує конфіденційність і цілісність даних, системи резервного копіювання гарантують оперативне відновлення після інцидентів, а контроль доступу й антивірусне ПЗ мінімізують ризики несанкціонованого проникнення та шкідливої активності на робочих станціях і серверах.

Розрахунок повної вартості володіння та рентабельності інвестицій показав, що економічне обґрунтування вибору між комерційними й відкритими рішеннями сприяє оптимізації бюджету та підвищенню ефективності захисних заходів. Впровадження передових підходів - хмарних SIEM/SOAR‑сервісів, UEBA та ML/AI‑інструментів - відкриває нові можливості для адаптивної й автоматизованої безпеки, здатної протистояти сучасним і майбутнім кіберзагрозам.

Таким чином, практична реалізація технічних засобів захисту інформації повинна здійснюватися за чітко визначеними процедурами конфігурації, оновлення та моніторингу, з урахуванням економічних показників і перспективних технологій. Тільки такий комплексний і системний підхід забезпечить високий рівень стійкості інформаційно-комунікаційних систем до будь‑яких атак та сприятиме безперебійному функціонуванню критичних бізнес‑процесів.

ВИСНОВОК

У результаті дослідження сучасних методів мережевого захисту інформації було обґрунтовано значення правової та методологічної бази, визначено ключові поняття конфіденційності, цілісності та доступності даних, описано категорії інформації з обмеженим доступом відповідно до українського та міжнародного законодавства і стандартів ISO/IEC 27001 та NIST Cybersecurity Framework. Аналіз сучасних методів і моделей захисту, зокрема багаторівневого захисту та моделі «нульової довіри», дав змогу окреслити перелік організаційних, технічних і програмних підходів до зниження ризиків у мережевому середовищі.

У другому розділі було детально розглянуто класи технічних засобів - міжмережеві екрани, системи виявлення та запобігання вторгненням, криптографічні методи, системи резервного копіювання та відновлення, системи контролю доступу та засоби захисту від шкідливого програмного забезпечення - і сформульовано стратегії запобігання загрозам, своєчасного виявлення інцидентів та реагування на них. Виокремлено роль мережевої ізоляції, сегментації, віртуальних локальних мереж, демілітаризованих зон та архітектури «нульової довіри» в побудові багаторівневого захисту.

У третьому розділі продемонстровано вибір і налаштування міжмережевого екрану з глибинним аналізом трафіку та модулями виявлення загроз, приклад впровадження системи виявлення та запобігання вторгненням з інтеграцією в систему централізованого збору і кореляції подій, застосування криптографії за сучасними протоколами, організацію незмінних резервних копій, впровадження контролю доступу на основі ролей і атрибутів з багатофакторною автентифікацією та централізацією через служби каталогів, а також використання антивірусного програмного забезпечення і політик регулярного оновлення. Економічний аналіз довів важливість оцінки повної вартості володіння й рентабельності інвестицій при виборі між комерційними та відкритими рішеннями. Системний підхід, що поєднує нормативні вимоги, технічні засоби та сучасні аналітичні платформи з автоматизацією реагування і аналізом поведінки користувачів, забезпечує високу

стійкість інформаційно-комунікаційних систем до сучасних кіберзагроз. Рекомендовано регулярно оновлювати політики й інструменти, перевіряти плани відновлення після катастроф, а також проводити економічний аудит безпекових рішень для оптимізації балансу між захистом і витратами.

ПЕРЕЛІК ПОСИЛАНЬ

1. CIA Triad – URL: https://www.fortinet.com/resources/cyberglossary/cia-triad
2. Про захист інформації в інформаційно‑комунікаційних системах : Закон України від 05.07.1994 № 80/94‑ВР URL: https://zakon.rada.gov.ua/laws/show/80/94-вр
3. Про інформацію : Закон України від 02.10.1992 № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12
4. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939‑VI URL: https://zakon.rada.gov.ua/laws/show/2939-17
5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163‑VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19
6. Злочини проти інформаційної безпеки розділ X : Кримінальний кодекс України URL: https://zakon.rada.gov.ua/laws/show/2341-14
7. Uncover Security Design Flaws Using The STRIDE Approach - https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach
8. What is mean time to detect (MTTD) - https://www.techtarget.com/searchitoperations/definition/mean-time-to-detect-MTTD
9. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements
10. NIST Cybersecurity Framework – https://www.nist.gov/cyberframework
11. Regulation (EU) 2016/679 (General Data Protection Regulation) – https://eur-lex.europa.eu/eli/reg/2016/679/oj
12. OWASP Top Ten – The Ten Most Critical Web Application Security Risks – https://owasp.org/www-project-top-ten/
13. Cisco “Next‑Generation Firewalls” Documentation URL: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

14. Perform network intrusion detection by using Azure Network Watcher and open-source tools URL: https://learn.microsoft.com/ru-ru/azure/network-watcher/network-watcher-intrusion-detection-open-source-tools
15. Microsoft “Introduction to Zero Trust Architecture” URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-zero-trust-architecture