Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Аналіз методів виявлення вразливостей у бездротових мережах"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Вощило Руслан Олексійович
підпис (прізвище та ініціали)

Керівник Кульчицький Т. Р.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

АНОТАЦІЯ

Аналіз методів виявлення вразливостей у бездротових мережах// Дипломна робота ОР «Бакалавр» // Вощило Руслан Олексійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-42 // Тернопіль, 2024 // С. 68 , рис. – 20, табл. – 9 , кресл. – - , додат. – -.

КЛЮЧОВІ СЛОВА: ОС, Загрози, Безпровідні мережі, Аномалії, TLS, IPSEC, SSL, WI-FI, Ризики.

Ця кваліфікаційна робота написана для вивчення методів ідентифікації загроз у бездротових мережах. Було здійснено дослідження методів і механізмів гарантування інформаційної безпеки та надійності даних у середовищі бездротових мереж.

Для одержання оцінки кібератак і їх класифікації, було вирішено застосувати відому просторову ознакову класифікацію. Такий підхід дозволяє розширити простір ознак для опису невідомих класів кібератак.

У дослідженні запропоновано класифікатор загроз, що дозволяє створити уніфікований підхід до визначення загрози та її обліку під час виявлення аномальної діяльності або відхилень від звичайної роботи в середовищі бездротових мереж на прикладі АВС.

У першому розділі наведено теоретичні відомості тематики кваліфікаційної роботи.

У другому розділі здійснено аналіз протоколів конфіденційності, цілісності та автентичності даних.

У третьому розділі представлено метод моделювання процесів кібербезпеки.

У розділі "Охорона праці" описано вимоги безпеки під час роботи з електронно-обчислювальними машинами. У розділі "Безпека життєдіяльності" висвітлено окремі аспекти безпеки у приміщеннях виробництва.

ABSTRACT

Investigation of methods for identifying threats in a wireless network environment// Bachelor's Thesis // Voshchylo Ruslan // Ternopil Ivan Puluj National Technical University, Department of Computer Information Systems and Software Engineering, Department of Cybersecurity // Ternopil, 2024 // P. 68 fig. – 20, tab. - 9, chair. - , added. – -.

Keywords: OS, Threats, Wireless Networks, Anomalies, TLS, IPSEC, SSL, WI-FI, Risks.

An qualification work is dedicated to the investigation of threat identification methods in networks. The study involved an examination of the techniques and mechanisms to ensure security of information and data integrity within wireless network environments. To achieve a high-quality assessment of cyberattacks and their subsequent classification, a well-known feature space classification was proposed. This approach enabled the expansion of the feature space to describe unknown classes of cyberattacks.

The work proposed a threat classifier that provides an approach for defining threats and accounting for them when detecting anomalous or abnormal operations in wireless network environments, exemplified by ABC.

The first chapter presents the main theoretical information on the topic of the work.

The second chapter analyzes the protocols ensuring data confidentiality, integrity, and authenticity.

The third chapter details the methodology for modeling cybersecurity processes using the framework of cyberattack classes.

The fourth chapter, "Occupational Safety," examines the safety regulations for operating electronic computing machines, while the subsection "Life Safety" addresses specific safety concerns in production environments.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ,СКОРОЧЕНЬ І ТЕРМІНІВ

ОС	—	Операційна система
РЧ	—	Радіочастотне поле
ФС	—	Файлова система
AID	—	Application Identifier – унікальний ідентифікатор сервісу-обробника NFC-команд
APDU	—	Application Protocol Data Unit - формат команд обміну даними між NFC-пристроями
GUI	—	Graphical User Interface - графічний інтерфейс користувача
HCE	—	Host-Card Emulatio – емуляція смарткарт на мобільних пристроях
Message-reply	—	Протокол повідомлення-відповідь
MITM	—	Man-in-the-middle - атака «людина посередині»
NFC	—	Near Field Communication - технологія передачі даних на невеликих відстанях
RFID	—	Radio Frequency Identification- технологія радіочастотної ідентифікації

ВСТУП

Комп'ютерні системи та телекомунікаційні технології мають ключове значення для стабільного функціонування численних інформаційних систем різного призначення. Багато з цих систем містять конфіденційну інформацію, тому автоматизація обробки даних породжує питання інформаційної безпеки. Зокрема, важливе місце займає виявлення аномалій у роботі програмного забезпечення і захист бездротових мереж [1, 2, 10, 11, 13–17, 19–23]. Банки з моменту їхнього виникнення завжди були привабливими для злочинців через зберігання не лише грошових коштів, але й важливої та часто інформацію про фінансову діяльність осіб, яка являється секретною, компаній, організацій і навіть держав. Комп'ютеризація банківського сектору значно підвищила продуктивність праці банківських працівників і дозволила впровадити нові технології і продукти фінансів. Однак, технологічний прогрес також призвів до зростання кількості кібератак. Сьогодні понад 90% злочинів у банківській сфері спричинені використанням систем автоматизованиї обробки інформації (АСОІ) [11].

Для захисту банківських систем необхідно застосовувати сильні засоби автентифікації та дієвий контроль як для клієнтів, так і для внутрішніх користувачів. Загальноприйнятим є використання двофакторної автентифікації, наприклад, електронних ключів (токенів) або генераторів паролів одноразового використання. Збереження даних вимагає застосування шифрування на рівні сховищ і окремих компонентів системи, таких як таблиці баз даних, для забезпечення їх безпеки [1, 19, 28]. Захист банкоматів і терміналів платежів повинен забезпечуватися антивірусним захистом та створенням "замкненого програмно-апаратного середовища", яке виключає можливість встановлення програмного забезпечення зі сторони і під'єднання зовнішніх пристроїв.

Для забезпечення належного рівня захисту інформації доцільно використовувати принципи ризик-менеджменту [17, 18]. Цей підхід дозволяє раціонально визначити та класифікувати загрози, а також оцінити ймовірність

настання негативних наслідків і можливі втрати для банку, створюючи ефективну систему захисту. Інформаційна безпека забезпечується в умовах випадкового впливу факторів, які неможливо повністю передбачити під час проєктування системи захисту інформації.

Однією з ключових труднощів у проектуванні та експлуатації захисних систем є недостатня увага до методології системного аналізу, зокрема до засобів та інструментів захисту. Об'єктивна оцінка ефективності захисної інформаційної системи є складною через нестачу нормативно-методичного забезпечення, особливо в частині визначення показників та критеріїв. Міжнародний стандарт EMV для операцій з банківськими картками з чіпом, що введений у 2005 році, регулює фізичну, електронну та інформаційну взаємодію між карткою та платіжним терміналом на основі стандартів ISO/IEC 7816 для контактних карт та ISO/IEC 14443 для безконтактних карт [3, 11, 14, 18, 19, 25].

Інтернет-банкінг став дуже популярним серед банків та їх клієнтів. Використання Інтернет-ресурсів для передачі PIN-коду клієнта до банку є альтернативою, яка дозволяє знижувати витрати на передачу даних, підвищувати конкурентоспроможність банків і збільшувати їхню гнучкість у взаємодії з клієнтами. Основними бар'єрами перед розвитком інтернет-банкінгу є забезпечення безпеки системи, відсутність довіри та нестача правової підтримки. Дослідження підкреслюють, що досягнення інформаційної безпеки можливе лише за умови комплексного застосування всіх доступних засобів захисту на кожному етапі технологічного циклу обробки інформації у всіх структурних компонентах виробничої системи. Максимальний ефект досягається завдяки інтеграції усіх використовуваних засобів, методів та заходів у єдиний цілісний механізм — систему захисту інформації (СЗІ). Важливо, щоб така система постійно контролювалася, оновлювалася та доповнювалася відповідно до змін у зовнішніх та внутрішніх умовах [11, 12].

Мета [7] цієї роботи полягає у моделюванні процесів ідентифікації кібератак і формалізації принципів створення класифікатора загроз для компонентів безпеки. Для досягнення цієї мети необхідно вирішити наступні завдання:

1. Проаналізувати основні загрози у середовищі бездротових мереж.
2. Дослідити методи виявлення аномалій та зловживань.
3. Оцінити методики оцінки ризиків.
4. Вивчити засоби та механізми забезпечення інформаційної безпеки та достовірності даних у бездротових мережах.
5. Змоделювати процеси кібербезпеки на основі класифікації кібератак.
6. Формалізувати принципи створення класифікатора загроз для таких аспектів безпеки, як інформаційна безпека, інформаційний захист, кібербезпека.

1 ТЕОРЕТИЧНА ЧАСТИНА

1.1 Аналіз основних загроз у середовищі безпровідних мереж

Для аналізу основних загроз безпеки інформації у бездротових мережах використовується модель, відома як тріада CIA (Confidentiality, Integrity, Availability). Ця модель розглядається через три профілі: безпека інформації, інформаційна безпека та кібербезпека на прикладі автоматизованої банківської системи, де банківська інформація використовується як ресурс.

Інформаційна безпека визначається як процес забезпечення конфіденційності, цілісності та доступності інформації для клієнтів банку. Конфіденційність забезпечує доступ до інформації лише авторизованим користувачам, цілісність гарантує достовірність та повноту інформації для авторизованих користувачів, а доступність дозволяє авторизованим користувачам отримувати доступ до інформації та пов'язаних з нею активів за потреби.

Безпека інформації визначається як стан захищеності даних, що забезпечує їх конфіденційність, доступність та цілісність. Це означає відсутність недопустимого ризику, спричинено з інформаційним витоком через технічні канали, несанкціонованими або ненавмисними діями щодо даних чи інших ресурсів автоматизованої системи інформації.

Кібербезпека охоплює широкий спектр засобів, стратегій, принципів безпеки, гарантій, підходів до управління ризиками, технологій, дій, професійної підготовки, страхування та інших заходів, які застосовуються для захисту кіберсередовища, ресурсів організацій та користувачів. Основна мета кібербезпеки - забезпечити безпеку ресурсів організацій або користувачів від кіберзагроз, включаючи захист особистої інформації та реагування на атаки. Стандарт ISO/IEC 27032:2012 "Information technology – Security techniques – Guidelines for cybersecurity" чітко встановлює зв'язок між термінами як Інтернет-безпекою, "кібербезпека", застосунковою безпекою та мережевою безпекою, який зображений на рисунку 1.1 [24].

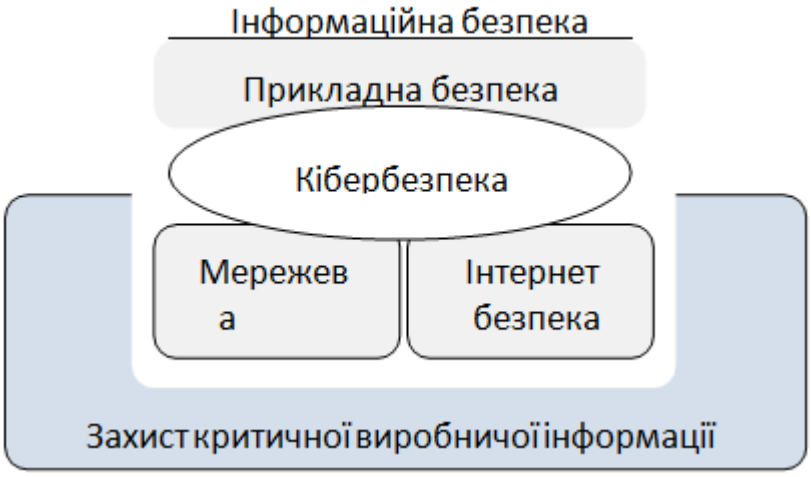


Рисунок 1.1 – Зв’язок кібербезпеки та доменамів

Трійна CIA, що є загальновідомою моделлю для АБС, зображена на рисунку 1.2:

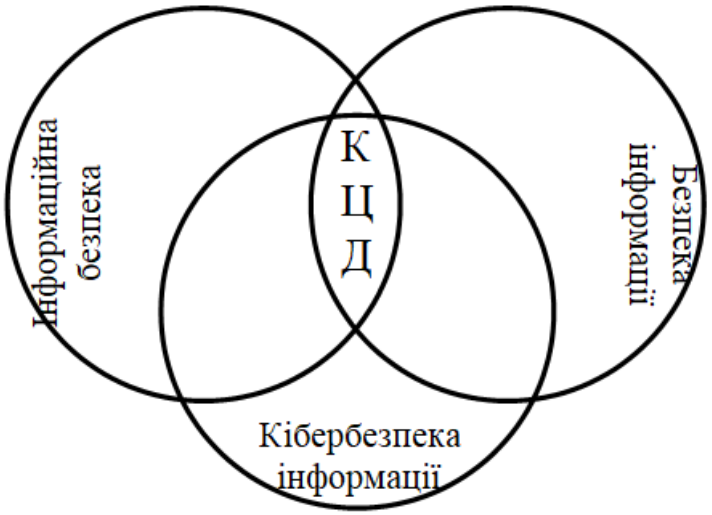


Рисунок 1.2 – Модель трійної CIA

Не дивлячись на розповсюджене застосування різноманітних алгоритмів шифрування на різних рівнях безпеки автоматизованих банківських систем (АБС), ця система продовжує відчувати різні загрози. Ці загрози можна класифікувати у трьох основних сферах безпеки, представлених на рисунку 1.3.

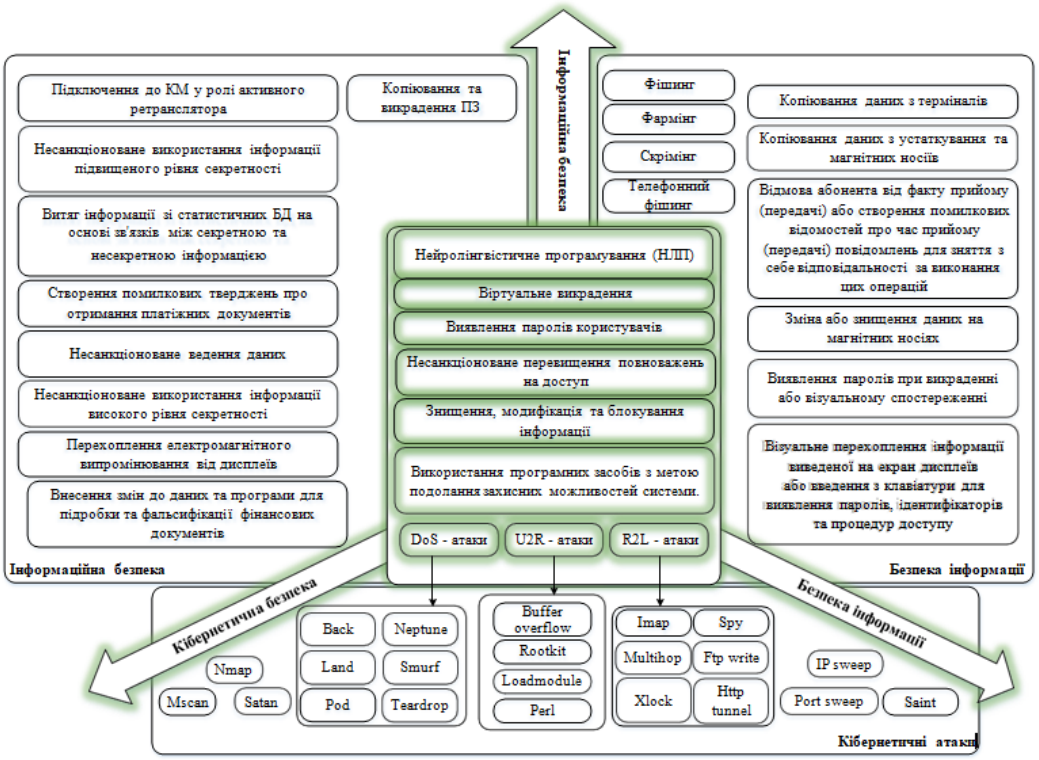


Рисунок 1.3 – Класифікація загроз АБС

Загрози для банків, які зображені на рисунку 1.4, можуть мати потенційний або реальний характер і виникати як з внутрішніх, так і зовнішніх джерел. Вони поділяються на економічні, фізичні та інтелектуальні категорії.

Економічні загрози включають корупцію, шахрайство, недобросовісну конкуренцію та низьку ефективність технологій у банківській діяльності. Наслідки таких загроз можуть бути у вигляді фінансових втрат або зниження прибутків.

Фізичні загрози охоплюють крадіжки, грабежі майна та коштів, поломки обладнання та його неправильну експлуатацію. Це може спричинити втрати майна та додаткові витрати на відновлення ресурсів [11, 15, 22].

Інтелектуальні загрози пов'язані з розголошенням або неправомірним використанням банківської інформації, дискредитацією ринкового банку та соціальними конфліктами. Такі загрози можуть призвести до фінансових втрат, погіршення репутації банку та створення напруженості серед персоналу.

Аналіз показав, що одним з найбільш вразливих місць у складних автоматизованих банківських системах є передача платіжних та інших повідомлень між банком і банкоматом, банками, а також між клієнтом і банком. Ця проблема поєднана із наступними особливостями:

1. Внутрішні системи одержувача та відправника повинні бути налаштованими для передавання та приймання електронних документів із безпекою у обробному процесі (захист кінцевих систем).
2. Взаємодія між одержувачем і відправником електронного документа відбувається через канал зв'язку.

Ці особливості призводять до наступних проблем:

1. Взаємне визначення абонентів: перевірка на автентичность при з'єднанні.
2. Захист електронних документів: забезпечення конфіденційності документів та їх цілісності, які передаються каналами зв'язку.
3. Захист обмінного процесу електронними документами: підтвердження відправлення та доставки документа.
4. Забезпечення виконання документа: рішення проблеми взаємної недовіри між одержувачем і відправником через їхню належність до різних організацій.

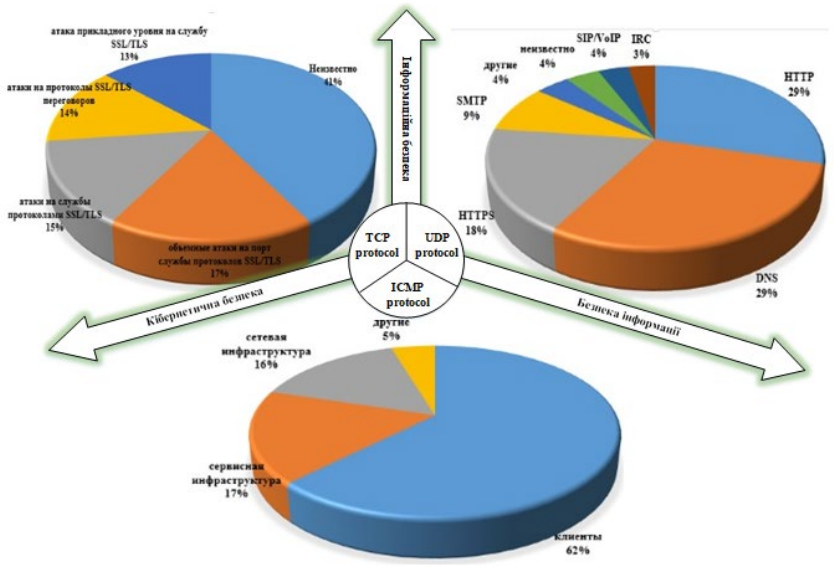


Рисунок 1.4 – Дослідження загроз IP-мереж

Зі зростанням кількості кіберзлочинів і покращенням доступних зловмисникам обчислювальних ресурсів, не лише вдосконалюються відомі кібератаки, але також з'являються нові види атак. Класифікація кібератак намальованав у схемі на рисунку 1.5.

Атаки, які використовуються для здійснення проникнення, діляться на чотири основні категорії. Кожна з цих категорій містить кілька типів атак, спрямованих на досягнення певної мети цього проникнення. Кожен тип атаки становить загрозу для мережі на відповідних рівнях мережевої моделі OSI і має власні методи завдання деструктивного впливу на мережі [4-7, 17].

До цих категорій атак належать:

1. Атаки відмови в обслуговуванні (DoS) – це мережеві напади на комп'ютерні системи, метою яких є зробити комп'ютерні ресурси недоступними для користувачів. Такі атаки призводять до ситуацій, коли відбувається відмова в обслуговуванні. Вони характеризуються заповненням системи великою кількістю з'єднань, зловживанням системними ресурсами, виникненням помилок через зміну параметрів конфігурації системи. Це призводить до перевантаження та блокування сервера комп'ютерної системи.
2. Інші категорії атак також мають свої специфічні особливості та методи реалізації. Кожна з них може мати різний вплив на різні рівні мережевої моделі OSI, спричиняючи різноманітні загрози для мережевої інфраструктури.

Рисунок 1.5 – Кібератаки та їх класифікація

Якщо здійснюється атака з величезної кількості IP-адрес водночас, це називається розподіленою атакою відмови в обслуговуванні (DDoS).

U2R атаки (User to Root) – атаки відбуваються, коли хакер здобуває доступ до облікового запису звичайного користувача та, використовуючи уразливості системи, намагається отримати несанкціонований доступ до привілейованих ресурсів і функцій.

R2L атаки (Remote to Local) – це атаки, що дозволяють незареєстрованому користувачеві отримати доступ у мережевий простір з віддаленої станції, використовуючи вразливості в системі.

Probe-атаки – передбачають сканування портів мережі з ціллю одержання конфіденційної інформації про мережу та компоненти у ній.

Зазначені типи атак мають здатність чинити вплив на різні аспекти мережевої діяльності, такі як:

1. Дозвіл на кодування.
2. Керування передачею даних.
3. Організація з'єднань.
4. Обмін пакетами.
5. Міжмережевий обмін.
6. Керування інформацією та інше.

Цей вплив класифікують за різнорівневими мережевими моделями OSI, що забезпечує систематичний підхід до аналізу та захисту мережевої інфраструктури. Таблиця 1.1 демонструє, як різні типи атак співвідносяться з рівнями моделі OSI [21, 22].

Таблиця 1.1 – Атаки на різнорівневі мережеві моделі OSI та їх вплив

Категорії атак	Типи атак	Рівні мережевої моделі OSI				
		Прикладний	Транспортний	Мережевий	Канальний	Фізичний
DoS	back	+	+	+	+	+
	land	+	+	+	+	+
	neptune		+	+		
	pod		+	+	+	+
	smurf			+	+	+
	teardrop	+	+	+	+	+
U2R	buffer_overflow		+	+		+
	loadmodule		+	+		+
	perl	+	+	+		+
	rootkit	+	+	+	+	
R2L	ftp_write	+			+	
	guess_passwd	+	+		+	
	imap	+	+		+	
	multihop	+		+		+
	phf	+	+			
	spy	+			+	
	warezclient	+			+	+
	warezmaster	+				+
Probe	ipsweep			+	+	
	nmap			+	+	
	portsweep		+	+		
	satan	+		+		

Кожен із рівнів OSI підтримує певний особливий протоколів мережі (табл. 1.2):

Таблиця 1.2 – Протоколи мережі рівнів OSI

Рівень	Протоколи	Атаки	Приклад
Прикладний: доступ до мережевих служб	HTTP, gopher, Telnet, DNS, DHCP, SMTP, SNMP, CMIP, FTP, TFTP, SSH, IRC, AIM, NFS, NNTP, NTP, SNTP, XMPP, FTAM, APPC, X.500, AFP, LDAP, SIP, IETF, RTP,.	rootkit, back, land,teardrop, phf, perl,warezclient, imap, guess_passwd, warezmaster, ftp_write, spy, satan	Атаки відмови в обслуговуванні, розсилка спама електронною поштою
Транспортний: безпечне "точка – точка"	ASP, ADSP, DLC, Named Pipes, NBT, NetBIOS, NWLink, Printer Access Protocol, Zone Information Protocol, SSL, TLS, SOCKS, PPTP	back, land, teardrop, imap, guess_passwd,pod, phf, buffer_overflow,per l load_module, rootkit,neptun, port_sweep	АтакаSYN-пакетами(SYN Flood), атака ICMP-запитамизі зміненими адресами(Smurf Attack)
Мережевий: визначення маршруту і IP (логічна адресація)	TCP, UDP, NetBEUI, AEP, ATP, IL, NBP, RTMP, SMB, SPX, SCTP, DCCP, RTP, STP, TFTP	back, land, teardrop, satan, buffer_overflow, perl, load_module, rootkit, ip_sweep, nmap, neptun, port_sweep, smurf, pod	Атака IC MP- запитами (ICMPFlooding)
Канальний: MAC и LLC (фізична адресація)	IPv4, IPv6, ICMP, IGMP, IPX, NWLink, NetBEUI, DDP, IPSec, ARP, SKIP	back, land, teardrop, ftp_write, spy, imap, guess_passwd, warezclient, rootkit, ip_sweep, nmap, smurf, pod	Атака пакетами з різними MAC-Адресами (MAC Flooding)
Фізичний: кабель, сигнали, бінарна передача	ARCnet, ATM, DTM, SLIP, SMDS, Ethernet, FDDI, Frame Relay, LocalTalk, Token Ring, PPP, PPPoE, StarLan, WiFi, PPTP, L2F, L2TP, PROFIBUS	back, land, teardrop, warezmaster, warezclient, buffer_overflow, load_module, smurf, pod	Атака спеціально сформованими пакетами (DummyPacket Attack)

Аналіз показує, що з кожним роком кількість кібератак збільшується. Це безпосередньо пов'язано з розвитком обчислювальних технологій та зростанням рівня комп'ютерних навичок серед зловмисників.

1.2 Аналіз методів фіксування аномалій і зловживань

На стадії ризикового аналізу інформаційної безпеки застосовуються спеціалізовані програмні комплекси, які автоматизують процес оцінки вихідних даних та обчислення ризиків. Розглянемо кілька прикладів таких комплексів і їх особливостей:

1. Програмні продукти " Кондор і Гриф " від Digital Security спеціалізуються на комплексному аналізі інформаційної безпеки, зокрема виявленні аномалій в інформаційних системах. Вони дозволяють оцінювати загрози конфіденційності, цілісності та доступності даних.
2. Метод CRAMM (CCTA Risk Analysis and Management Method), розроблений у Великобританії, використовується для оцінювання ризикованості інформаційної безпеки. Він дозволяє ідентифікувати потенційні загрози та визначати заходи для зменшення ризиків.
3. RiskWatch - американський комплекс, що надає інструменти для аналізу та управління ризиками в інформаційній безпеці. RiskWatch допомагає виявляти потенційні слабкі місця та проводити оцінку ризиків на різних рівнях IT-інфраструктури.

Основу безпечної IT-інфраструктури складає тріада сервісів: конфіденційність, цілісність та доступність, відома як модель CIA. Ці принципи визначають основні аспекти безпеки інформації, що включають захист від несанкціонованого доступу, забезпечення цілісності даних і їх доступності для авторизованих користувачів.

Автоматизація аналізу ризиків за допомогою таких спеціалізованих програмних комплексів дозволяє підвищити ефективність заходів інформаційної

безпеки та своєчасно реагувати на загрози, забезпечуючи високий рівень захисту інформаційних ресурсів [8, 14].

На рисунку 1.6. показані ризики інформаційної безпеки та моделі їх аналізу.

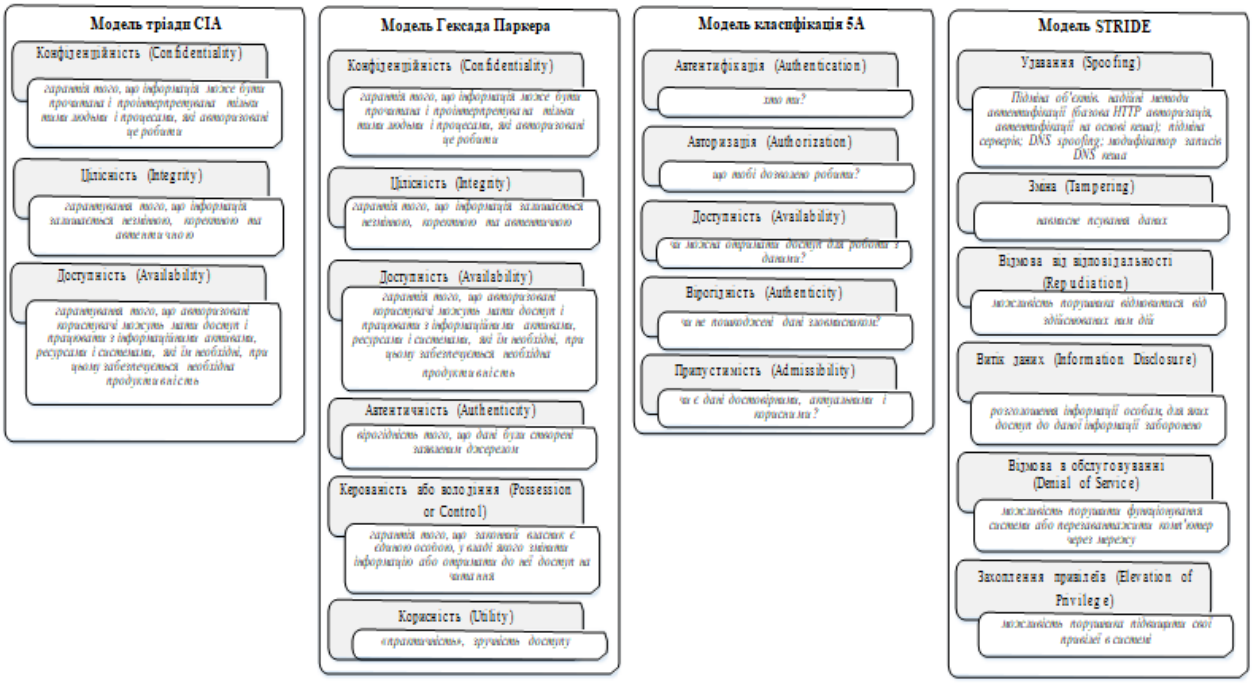


Рисунок 1.6 – Ризики інформаційної безпеки та моделі їх аналізу

Аналіз моделей для оцінювання ризиків безпеки інформації показує, що вони базуються на моделі тріади CIA, яка включає цілісність, конфіденційність та інформаційна доступність. Проте ці підходи часто обмежені лише аспектами безпеки інформації і не надають повного огляду кібербезпеки в реальному часі.

Аналіз ризиків є ключовим елементом керування безпекою інформації, що враховує ефективність існуючих заходів захисту від потенційних інформаційних атак. Для оцінки ризиків використовуються дві методологічні підгрупи. Перша група оцінює рівень ризику на основі відповідності вимогам щодо забезпечення інформаційної безпеки. Інша група методів ґрунтується на оцінці ймовірності атак та можливих збитків. Збитки визначаються власником інформаційних ресурсів, а ймовірність атаки оцінюється експертами під час аудиту [4-5, 17, 24].

Такий підхід дозволяє комплексно оцінювати потенційні загрози та

вибирати відповідні заходи захисту, що забезпечує безпеку інформаційних активів у реальному часі. Методи фіксування атак являються одними із ключових критеріїв оцінки систем захисту інформації. Головна методологічна класифікація показана у вигляді схеми на рисунку 1.7.

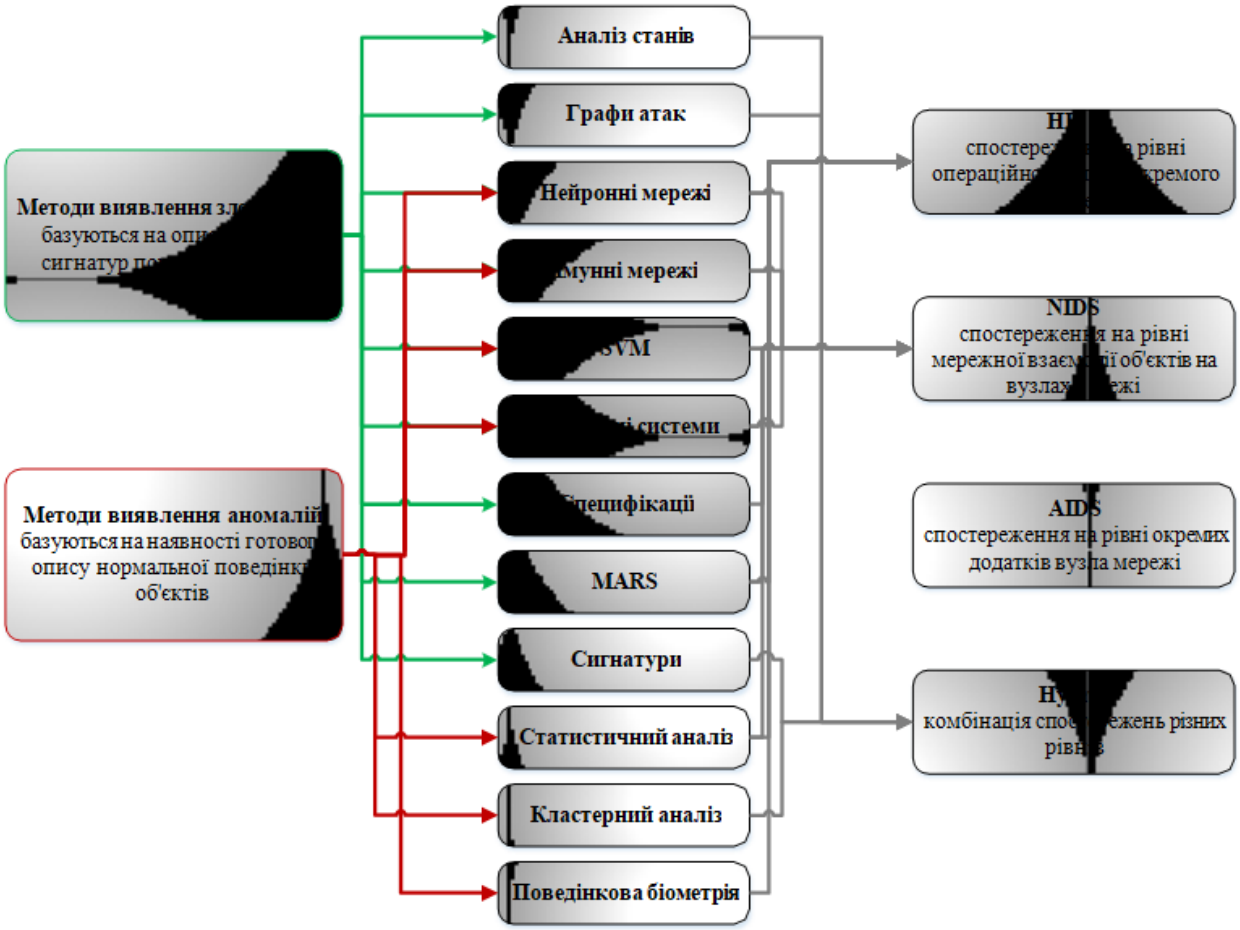


Рисунок 1.7 – Розподіл методів фіксування зловживань та аномалій

Головні параметри методів показані в табл. 1.3.

Таблиця 1.3 – Методи фіксування зловживань та аномалій

Метод	Вхідні дані	Математичний апарат	Опис	Вихідні дані	Економ. ефективність	Обчислювальна складність
1	2	3	4	5	6	7
Аналіз систем станів	Шаблони нормальної поведінки системи, шаблони атаки	Теорія графів	Функціонування системи, що підлягає захисту, представляється через множину станів і множину переходів між ними.	Ймовірнісна оцінка реалізації атаки	Якісна оцінка	P
Графи сценарії в атак	Модель системи, властивість коректності	Теорія графів	Множина поведінок ділиться на два класи - припустимі неприпустимі	Ймовірнісна оцінка реалізації атаки	Якісна оцінка	NP
Нейронні мережі	Траєкторії в деякому числовому просторі ознак	Алгоритми навчання нейронних мереж	Нейронні мережі навчаються на прикладах атак кожного класу надалі розпізнають приналежність поведінки одному з класів атак.	Ймовірнісна оцінка реалізації атаки	Якісна оцінка	P
Імунні мережі	Шаблони нормальної поведінки	Специфічні імунологічні теорії	Метод є механізмом класифікації і будується за аналогією з імунною системою живого організму.	Ймовірнісна оцінка реалізації атаки	Якісна оцінка	P
Support vector machines (SVM)	Вектори ознак нормальної поведінки системи, шаблони атаки	Алгоритми навчання і перенавчання	Метод подання та розпізнання шаблонів, який дозволяє формувати шаблони в результаті навчання, дозволяє обробляти вектори ознак великої розмірності.	Ймовірнісна оцінка реалізації атаки	Якісна оцінка	NP
Експертні системи	Факти про події в системі та правила виведення	Зіставлення фактів і правил	На підставі фактів і правил виводу система робить висновок про наявність чи відсутність атаки.	Ймовірнісна оцінка реалізації атаки	Якісна оцінка	NP

Продовження таблиці 1.3

1	2	3	4	5	6	7
Заснований на специфікаціях	Специфікації атак	Аналіз даних	Невідповідність поведінки специфікації вважається атакою.	Ймовірнісна оцінка реалізації атаки	Якісна оцінка	NP
Сигнатурний	Події в системі, сигнатури атак	Аналіз даних	Методи працюють на найнижчому рівні абстракції і аналізують безпосередньо передані мережею дані, параметри системних викликів і записи файлів журналів.	Ймовірнісна оцінка реалізації атаки, кількісні показники	Кількісна оцінка	NP
Multivariate Adaptive Regression Splines (MARS)	Простір ознак	Апроксимація функцій	Будується оптимальна апроксимація поведінки за заданою історією у вигляді навчальної множини векторів. Побудований сплайн є «шаблоном» атаки	Ймовірнісна оцінка реалізації атаки, кількісні показники	Кількісна оцінка	P
Статистичний аналіз	Статистичні дані про систему на деякому часовому проміжку	Математична статистика	Побудова статистичного профілю поведінки системи протягом періоду «навчання», при якому поведінка системи вважається нормальною. Відхилення, що перевищують визначені межі допустимих значень, фіксуються як факт аномалії (атаки).	Ймовірнісна оцінка реалізації атаки, кількісні показники	Якісна та кількісна оцінка	P
Кластерний	Вектори властивостей системи	Кластерний аналіз	Використання певної метрики дозволяє оцінювати приналежність вектору властивостей системи до одного з кластерів або вихід за межі відомих кластерів.	Ймовірнісна оцінка реалізації атаки, кількісні показники	Якісна та кількісна оцінка	P
Поведінкова біометрія	Профіль нормальної поведінки системи	Порівняльний аналіз	На базі побудованого профілю нормальної поведінки для даного користувача, виявляються відхилення від цього профілю.	Ймовірнісна оцінка реалізації атаки	Якісна та кількісна оцінка	P

Аналіз, проведений щодо виявляючої систем аномалій, виявив, що головною проблемою багатьох комерційних СВА сучасності є їх обмежена ефективність у виявленні нових типів кібератак. Це пов'язано з тим, що більшість таких системам підвласно використання сигнатурних методів, які вимагають постійного оновлення для виявлення нових загроз, що зумовлює затримки у виявленні аномалій. В обох підходах до виявлення кібератак використовуються шаблони поведінки, що формуються на основі вхідних параметрів системи. Головне завдання полягає у розпізнанні цих шаблонів і вчасному виявленні початку аномальної поведінки. Однак, важливим аспектом є об'єктивна оцінка інформативності кожного параметра. Наразі евристичний підхід являється домінуючим методом формування інформативних параметрів, що має свої недоліки у вигляді неформалізованості і суб'єктивності процедур відбору цих параметрів [13, 17, 18].

1.3 Аналіз методик оцінки ризиків

Давайте розглянемо різні методи оцінки інформативності параметрів та подамо їх схематичний вигляд (див. рисунок 1.8).

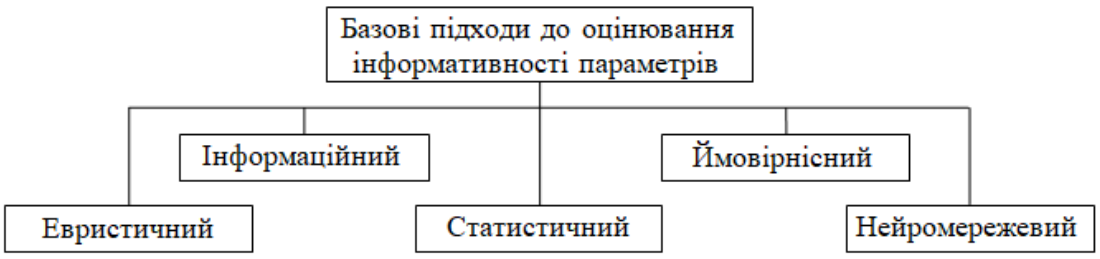


Рисунок 1.8 – Інформативність параметрів

Для обирання одного із вищезгаданих підходів та його адаптації для створення множини інформаційних параметрів для систем забезпечення інформаційної безпеки (СЗІ), потрібно враховувати декілька поділів якості. Порівнюючи різні підходи, ми застосовуємо такі критерії:

1. Ступінь трактування (крит. 1): Цей критерій визначає наукові основи підходу, його теоретичну обґрунтованість та методологічну чіткість.
2. Складність впровадження (крит. 2): Цей критерій визначає, наскільки складно та часомісткою є впровадження методу в практичні умови.
3. Швидкість процедур оцінки параметрів інформаційності (крит. 3): Цей критерій визначає час, необхідний для виконання процедур процедур оцінки параметрів інформаційності за обраним підходом.
4. Якість оцінюваних параметрів (крит. 4): Цей критерій оцінює рівень корисності та значущості параметрів, що використовуються для виявлення аномалій та зловживань.

Лінгвістичні оцінки, що представлені у вказаних джерелах, використовуються для порівняння різних підходів згідно з вищезазначеними критеріями якості, що ілюструється у вигляді стовпчастої діаграми, яка зображена на рисунку 1.9.

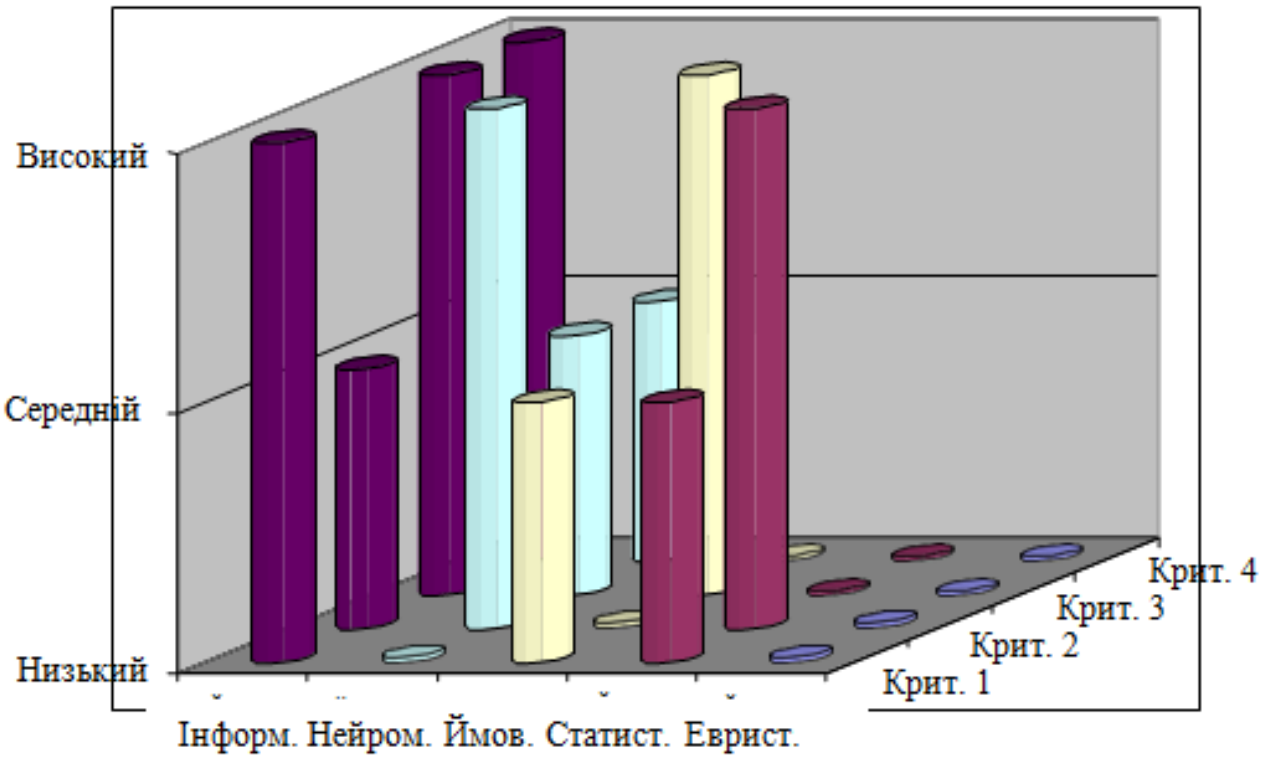


Рисунок 1.9 – Графік розподілу критеріїв якості

Опираючись на вищезгаданий аналіз, в таблиці 1.4 подано дані по результатах оцінювання ефективності підходів дослідження.

Таблиця 1.4 – Дані по результатах оцінювання ефективності підходів дослідження

Підходи	Оцінка ефективності	
	кількісна	якісна
Інформаційний	0.22	достатня
Нейромережевий	0.36	достатня
Ймовірнісний	0.4	задовільна
Статистичний	0.4	задовільна
Евристичний	0.5	низька

На підставі аналізу наданої інформації (див. таблицю 1.4), можна зробити висновок, що інформаційний підхід виявився найбільш ефективними серед досліджених методів в усіх однакових початкових умовах. Отже, це свідчить про те, що його можна рекомендувати для включення у процес створення кількості параметрів інформації. Оцінка ризиків в інформаційній безпеці є ключовим етапом, оскільки її результати пов’язані із наступним кроками організації. Методи оцінки ризиків представляють собою систематизовану послідовність дій і процедур, що дозволяють оцінити потенційні загрози [1, 2, 19].

Кількісні підходи використовують інформацію для оцінки активів, втрат і ризиків, що з ними пов'язані. Якісні підходи використовують шкали для оцінки рівня ризику, такі як категоріальні або рейтингові шкали, які визначаються у термінах низького, середнього та високого ризику, або числові шкали від 1 до 10, що відображають ступінь загрози чи її важливість.

Комбіновані методи поєднують переваги кількісного і якісного підходів, забезпечуючи комплексну оцінку ризиків, ураховуючи їх різні природні та характеристики.

Оскільки загрози для банківської системи мають різну природу, необхідно розглянути різні підходи до оцінки ризиків. (див. таблицю 1.5).

Таблиця 1.5 – Підходи оцінки ризиків

Методика оцінки	Переваги	Недоліки	Підходи
1	2	3	4
NIST	- Детальний опис можливих ризиків інформаційних активів - Для підприємств різного розміру	- Довготривалий процес аналізу - Деякі функції не автоматизовано	Евристичний
FAIR	- Комплексний аналіз - Симуляційна модель - Висока ефективність	- Для крупних банків та підприємств	Ймовірнісний
IT-Grundshutz	- Гнучкість методу надає змогу проводити аналіз для будь-якої організації - Налаштовується на нові або існуючі активи	- Потребує теоретичної обізнаності процесу аналізу ризиків - Висока вартість ліцензії	Евристичний
OCTAVE	- Швидке впровадження - Обслуговує малі та середні за розміром підприємства	- Відсутність автоматизації - Не враховує специфіку банківської сфери	Евристичний
IRAM	- Відносна простота впровадження - Легкість в експлуатації менеджерами банківських установ	- Висока вартість ліцензії - Робота тільки з існуючими інформаційними активами	Інформаційний
EBIOS	- Велика кількість користувачів - Генерація звітів	- Лише для комерційних та державних установ	Інформаційний
RISK WATCH	- Простота впровадження та експлуатації - Гнучкість - Висока ефективність	- Аналіз ризиків лише на програмно-технічному рівні - Висока вартість ліцензії	Інформаційний
MEHARI	- Заснований на аналізі формул та параметрів - Формує оптимальну множину контрзаходів - У вільному доступі	- Застосовуваний до систем, що побудовані тільки за стандартом ISO	Евристичний
MAGERIT	- Систематичний метод аналізу - Кількісна оцінка - Гнучкість	- Результуючі дані залежать від людського фактору	Евристичний
CRAMM	- Детальне визначення існуючих ризиків - Ефективність використання	- Важкість у розумінні - Висока вартість ліцензії - Робота тільки з існуючими інформаційними активами	Ймовірнісний
Методика НБУ	- Детальний аналіз ресурсів банківської системи - Використання ризик-орієнтованого підходу	- Заснований на множині стандартів - Враховує специфіку лише українських банківських систем	Інформаційний

Продовження таблиці 1.5

Методика Корченко	- Застосування ознакового принципу для опису різних класів КБа - Дозволяє розширювати ознаковий простір для опису нових класів	-Не дає можливості зробити оцінку матеріальної втрати від реалізованої загрози	Інформаційний

На підставі таблиці 1.6 можна зробити висновок, що для подальшої оцінки ризиків у відповідності з еквівалентом грошового капіталу і прямим відображенням рівня захищеності рекомендується застосовувати методики, які використовують комплексний підхід до оцінки ризиків. До таких методик відносяться CRAMM і FAIR, які мають структурні схеми, зображені на рисунках 1.10 і 1.11.

Таблиця 1.6 – Результати досліджень методик оцінки ризиків

Методика	Атрибути							
	Якісна оцінка	Кількісна оцінка	Комплексна оцінка	Країна походження	Застосування у БС	Програмна реалізація	Ефективність контрзаходів	Простота розуміння
NIST	+			США	+	+	-	-
FAIR			+	США			+	+
EBIOS	+			Франція	+	+	+	-
MEHARI			+	Франція				
OCTAVE	+			США	+			
IT-GRUNDSHULTZ	+			Німеччина			+	
IRAM	+			Європа				+/-
RISK WATCH		+		США	+	+	+	+
FRAP	+			США				
CRAMM			+	Великобританія	+	+	+/-	+/-
MAGERIT	+	+		Іспанія	+	+		
Методика НБУ	+			Україна	+		-	+
Методика Корченко	+			Україна			+/-	+

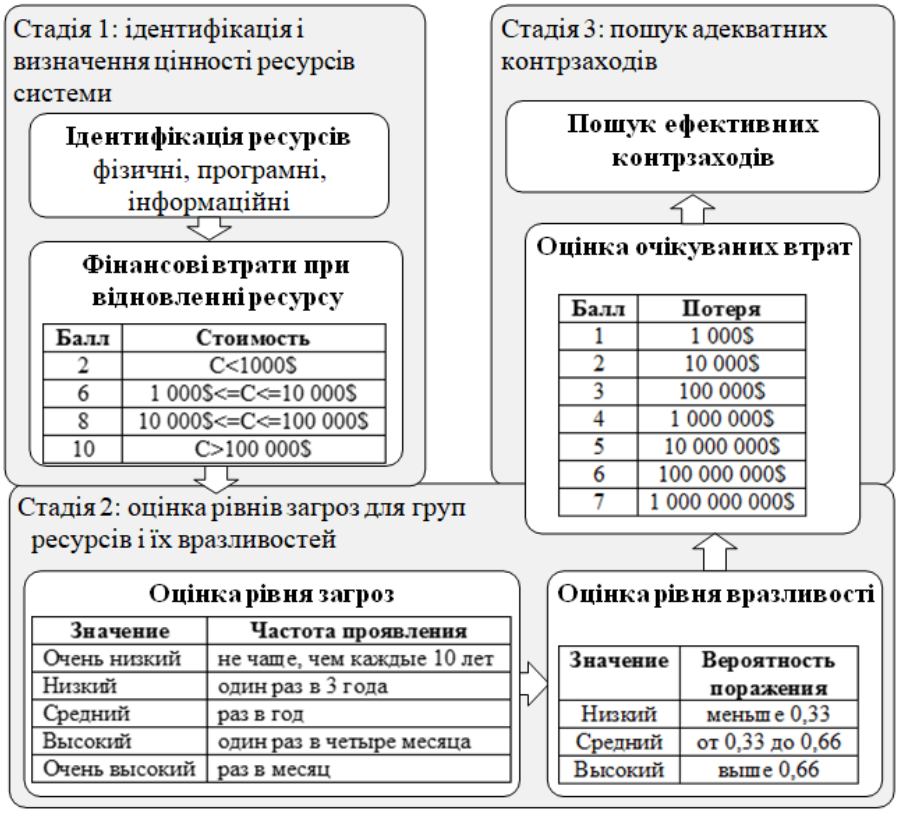


Рисунок 1.10 – Методика CRAMM

Рисунок 1.11 – Методика FAIR

Методики комплексного підходу до оцінки ризиків зазвичай включають наступні етапи:

1. Ідентифікація ресурсів системи:
    - Аналізується та визначається все, що стосується виявлення та оцінки цінності ресурсів системи.
    - Встановлюються межі досліджуваної системи, включаючи її конфігурацію, осіб, відповідальних за ресурси, численність користувачів та їх права доступу.
    - Визначаються фізичні, програмні та інформаційні ресурси в межах системи.
    - Створюється моделювання системи інформації з точки зору інформаційної безпеки.
2. Оцінка вразливостей і загроз:
    - Виявляються загрози, яким піддаються ресурси системи.
    - Оцінюються загрози для різних груп вразливостей і самих ресурсів.
    - Встановлюється залежність між послугами, наданими користувачам, і конкретними групами ресурсів.
    - Обчислюються ризики і проводиться аналіз результатів, які отримали.
    - Замовник одержує оцінені та ідентифіковані рівні ризиків для системи.
3. Пошук контрзаходів:
    - Здійснюється пошук ефективних заходів безпеки, що найкраще відповідають виявленим ризикам.
    - Формуються різні варіанти заходів протидії, які відповідають вимогам замовника та адекватні виявленим ризикам.

Ці етапи включають систематичний підхід до оцінки ризиків і їх управління, що дозволяє забезпечити ефективніший захист ресурсів інформації у реальному часі (див. рисунок 1.12).

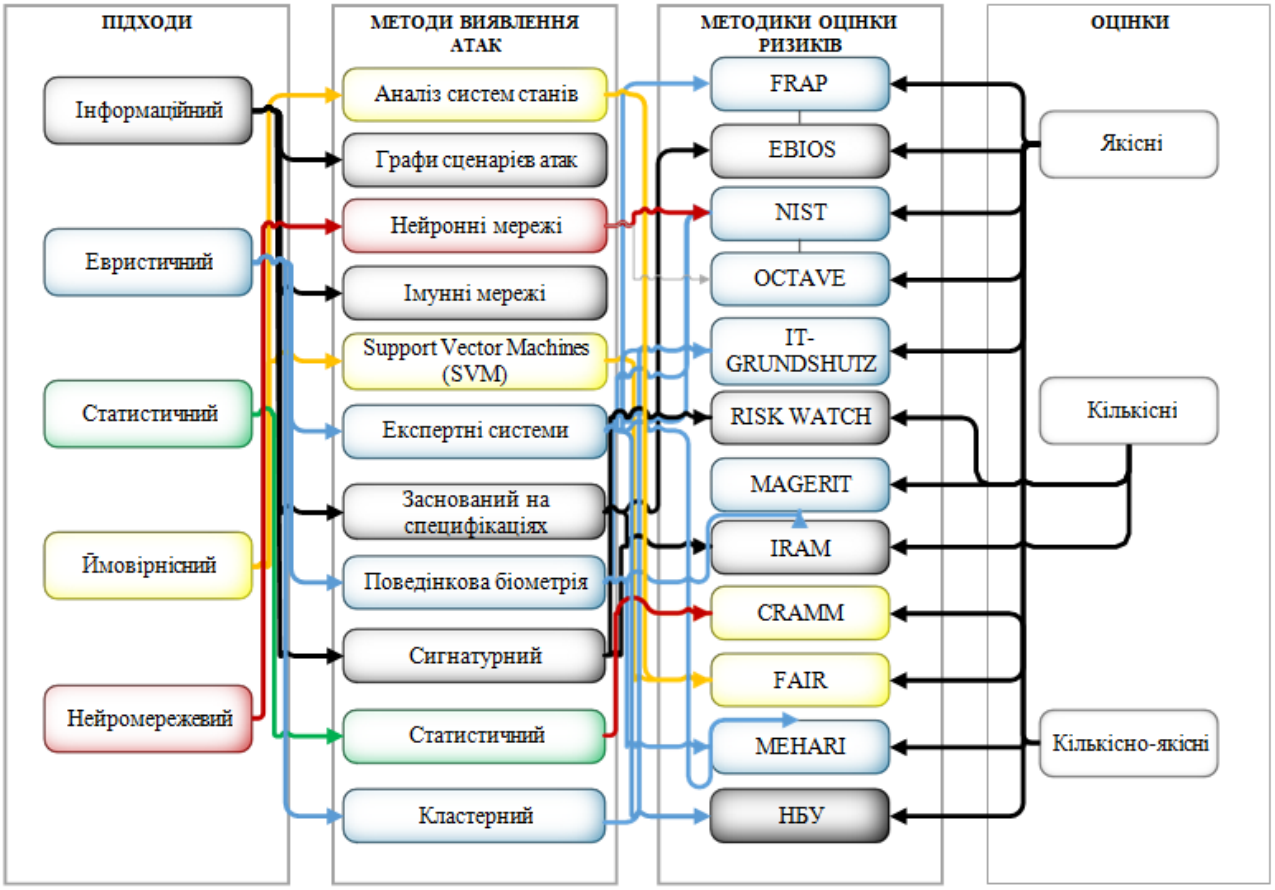


Рисунок 1.12 – Зв’язок між методами виявлення атак та оцінки ризиків

Для підвищення ефективності систем аномальних виявлень важливо продовжувати розвивати класифікатори кібератак на основі дерев прийняття рішень. Це ефективний метод, який забезпечує надійні результати класифікації при невеликих обчислювальних витратах.

Основою для створення таких класифікаторів є вхідні дані, які відіграють ключову роль у процесі класифікації кібератак. Рекомендується використовувати широкодоступну базу даних KDD99 для навчання та тестування цих класифікаторів. Ця база включає більше 5 мільйонів класифікованих екземплярів атак за 22 типами, які характеризуються 41 ознакою [20, 21].

Продовження досліджень і розвитку класифікаторів кібератак на основі дерев прийняття рішень допоможе підвищити точність виявлення аномалій в комунікаційних системах та забезпечить більш ефективну захист від кібератак (див. таблицю 1.7).

Таблиця 1.7 – 41 ознака вектору мережевого з’єднання

№	Ознака	Опис
1	2	3
Основні ознаки		
1	Duration	Тривалість з’єднання (секунди)
2	Protocol type	Тип протоколу (tcp, udp и др.)
3	Service	Мережева служба отримувача (http, telnet и др.)
4	Flag	Стан з’єднання
5	Src bytes	Число байтів, переданих від джерела отримувачу
6	Dst bytes	Число байтів, переданих від отримувача джерелу
7	Land	1 якщо з’єднання по ідентичних портах; 0 в інших випадках
8	Wrong fragment	Кількість «невірних» пакетів
9	Urgent	Кількість пакетів з прапором URG
Ознаки, пов’язані із вмістом		
10	Hot	Кількість «hot» індикаторів, вміст яких: вхід до системної директорії, створення та виконання програм
11	Num failed logins	Кількість невдалих спроб входу
12	Logged in	1 якщо успішний вхід; 0 в інших випадках
13	Num compromised	Кількість вдалих спроб входу.
14	Root shell	1 якщо досягнуто кореневої оболонки; 0 інших випадках
15	Su attempted	1 якщо команда «su root» використовується; 0 в інших випадках
16	Num root	Число підключень під «root» або число операцій, виконуваних від цього імені
17	Num file creations	Число операцій створення файлів у період з’єднання
18	Num shells	Кількість shell повідомлень
19	Num access files	Кількість операцій доступу до контрольних файлів
20	Num outbound cmds	Кількість вихідних команд у період FTP- сессії
21	Is hot login	1 якщо вхід виконано під «root» або «admin» правами; 0 в іншому випадку.
22	Is guest login	1 якщо гостьовий вхід; 0 в іншому випадку
Ознаки, пов’язані з часом		
23	Count	Кількість з’єднань між віддаленим та локальним хостами
24	Srv count	Кількість підключень до локальної служби
25	Serror rate	Відсоткове число з’єднань з помилкою типу SYN для даного хосту-джерела
26	Srv serror rate	Відсоткове число з’єднань з помилкою типу SYN для даної служби джерела
27	Rerror rate	Відсоткове число з’єднань з помилкою типу REJ для даного хосту-джерела
28	Srv rerror rate	Відсоткове число з’єднань з помилкою типу REJ для даної служби джерела
29	Same srv rate	Відсоткове число підключень до служби
30	Diff srv rate	Відсоткове число підключень до різних служб
31	Srv diff host rate	Відсоткове число підключень до різних хостів
Ознаки, пов’язані з особливостями трафіку		
32	Dst host count	Кількість з’єднань з локальним хостом, встановлених віддаленою стороною
33	Dst host srv count	Кількість з’єднань з локальним хостом, встановлених віддаленою стороною, що використовують однакову службу
34	Dst host same srv rate	Відсоткове число підключень до локального хосту, встановлених відділеною стороною, що використовують однакову службу

Продовження таблиці 1.7

1	2	3
35	Dst host diff srv rate	Відсоткове число підключень до локального хосту, встановлених відділеною стороною, що використовують різні служби
36	Dst host same src port rate	Відсоткове число підключень до даного хосту при поточному номері порту джерела
37	Dst host srv diff host rate	Відсоткове число підключень до служби різних хостів
38	Dst host serror rate	Відсоткове число з'єднань з помилкою типу SYN для даного хосту-приймача
39	Dst host srv serror rate	Відсоткове число з'єднань з помилкою типу SYN для даної приймаючої служби
40	Dst host rerror rate	Відсоткове число з'єднань з помилкою типу REJ для даного хосту-приймача
41	Dst host srv rerror rate	Відсоткове число з'єднань з помилкою типу REJ для даної приймаючої служби

Аналіз мережевого трафіку зазвичай включає деталізацію параметрів, таких як частота пакетів, обсяг передачі даних, а також типи протоколів та інші характеристики. Сучасні системи виявлення аномалій використовують складні алгоритми машинного навчання і статистичні методи для аналізу цих даних. Однак іноді деякі параметри можуть містити зайву або надлишкову інформацію.

Головна мета відсіювання надлишкових ознак – зменшення обсягу оброблюваних даних та покращення ефективності виявлення аномалій. Це досягається шляхом відбору лише тих ознак, які дійсно несуть важливу інформацію для виявлення аномалій, та виключення зайвих або менш суттєвих параметрів.

Розподіл інформативності ознак мережевого з'єднання у відсотковому вигляді допомагає визначити, які параметри слід використовувати для ефективного виявлення аномалій та відсіяти надлишкові або менш важливі параметри (див. таблицю 1.8) [9].

Таблиця 1.8 – Відсотковий розподіл інформації про мережеве з’єднання

Ознака	1	2	3	4	5	6
% інформації	52,40	71,67	88,37	91,49	94,21	95,90
Ознака	7	8	9	10	11	12
% інформації	96,96	97,71	98,27	98,73	99,00	99,18
Ознака	13	14	45	16	17	18
% інформації	99,33	99,47	99,59	99,67	99,75	99,81
Ознака	19	20	21	22	23	24
% інформації	99,87	99,90	99,93	99,94	99,95	99,96
Ознака	25	26	27	28	29	30
% інформації	99,97	99,98	99,98	99,99	99,99	99,99
Ознака	31	32	33	34	35	36
% інформації	99,99	99,99	99,99	99,99	99,99	99,99
Ознака	37	38	39	40	41	
% інформації	99,99	100	100	100	100	

Сучасні рекомендації вказують на перехід від використання набору даних KDD99 до NSL-KDD для виявлення кібератак. NSL-KDD є удосконаленою версією KDD99, яка усуває надлишкові записи і концентрується на 22 найбільш важливих ознаках мережевого з'єднання. Нижче наведено перелік цих 22 ознак мережевого з'єднання, які є найбільш значущими для класифікації і виявлення атак за допомогою NSL-KDD:

1. Duration: тривалість мережевого з'єднання.
2. Protocol_type: тип протоколу.
3. Service: тип обслуговування.
4. Flag: прапорці стану.
5. Src_bytes: кількість байт, відправлених від початкового вузла до приймаючого.
6. Dst_bytes: кількість байт, відправлених від приймаючого вузла до початкового.
7. Land: чи походить початкова IP-адреса та порт з одного і того ж вузла.
8. Wrong_fragment: кількість неправильних фрагментів.

9. Urgent: кількість пакетів, для яких встановлено флаг Urgent.
10. Hot: кількість "гарячих" індикаторів.
11. Num_failed_logins: кількість неуспішних спроб входу.
12. Logged_in: чи був успішний вхід в систему.
13. Num_compromised: кількість скомпрометованих систем.
14. Root_shell: чи був отриманий доступ до облікового запису root.
15. Su_attempted: чи були спроби виконання команди su.
16. Num_root: кількість з'єднань, у яких був обліковий запис root (включаючи su).
17. Num_file_creations: кількість створених файлів.
18. Num_shells: кількість оболонок, відкритих за сесію.
19. Num_access_files: кількість файлів доступу.
20. Num_outbound_cmds: кількість вихідних команд.
21. Is_hot_login: чи є це "гарячим" входом.
22. Is_guest_login: чи є це "гостьовим" входом.

Ці ознаки допомагають ідентифікувати та аналізувати різні типи мережевих активностей, що включають як нормальні, так і аномальні дії, що допомагає виявляти потенційні кібератаки (див. таблицю 1.9).

Таблиця 1.9 – Ознаки вектору з’єднання мережі

№	Ознака
1	Duration
2	Protocol type
3	Service
4	Flag
5	Source bytes
6	Destination types
7	Land
8	Wrong fragment
9	Urgent
11	Failed logins
13	Num compromised

Продовження таблиці 1.9

№	Ознака
14	Root shell
17	Num file creations
18	Num shells
22	Is guest login
27	Rerror rate
28	Srv rerror rate
29	Same srv rate
31	Srv diff host rate
32	Dst host count
35	Dst host diff srv rate
37	Dst host srv diff host rate

Для оцінки потрібності використання даних NSL-KDD проводились експерименти, що спрямовані на виявлення різнокатегорійних атак. Результати цих експериментів представлені у таблицях 1.10 до 1.12.

Таблиця 1.10 – Результати фіксування DoS-атак

Back, %	Land, %	Neptune, %	Pod, %	Smurf, %	Teardrop, %
99,5	100,0	100,0	98,1	100,0	100,0
Середнє значення – 99,6 %					

Таблиця 1.11 – Результати фіксування R2L-атак

Ftp write, %	Guess passwd, %	Imap, %	Multihop, %
100,0	94,3	83,3	57,1
Warezclient, %	Warezmaster, %	Phf, %	Spy, %
65,0	90,0	100,0	100,0
Середнє значення – 86,2 %			

Таблиця 1.12 – Результати фіксування Probe-атак

Ipsweep, %	Nmap, %	Portsweep, %	Satan, %
65,2	100,0	99,9	99,3
Середнє значення – 91,1 %			

1.4 Висновки до першого розділу

Важливість вхідних даних у процесі виявлення кібератак стає очевидною при розгляді різних наборів даних. Використання бази даних NSL-KDD, яка містить лише суттєві дані зі зменшеною кількістю ознак мережевого трафіку з 41 до 22, сприяло підвищенню ефективності виявлення атак порівняно з KDD-99. Це поліпшило якість виявлення атак і збільшило продуктивність системи, що є ключовим для успішної роботи систем захисту інформації.

Рекомендується застосування відомих методів ознакової класифікації для якісної оцінки кібератак та їх подальшої класифікації. Цей підхід дозволяє розширити спектр ознак для опису кібератакувальних класів.

Інтеграція якісного та кількісного підходів у процесі класифікації кібератак поєднує переваги кожного з них і відкриває нові можливості для отримання необхідних характеристик для ефективного функціонування систем захисту.

Цей метод аналізу та класифікації кібератак сприяє подальшому вдосконаленню систем захисту інформації та забезпечує високу надійність у виявленні та протидії кіберзагрозам.

2 АНАЛІЗ МЕХАНІЗМІВ І ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНОЇ ДОСТОВІРНОСТІ В БЕЗПРОВІДНОМУ МЕРЕЖЕВОМУ СЕРЕДОВИЩІ

2.1 Аналіз протоколів цілісності та конфеденційності даних

2.1.1 Розгляд протоколу SSL (Secure Socket Layer)

Для забезпечення конфіденційності та цілісності інформації у комп'ютерних та безпровідних мережах актуально використовувати протоколи SSL та IPSec, які зображені на рисунку 2.1.

Рисунок 2.1 – Стек протоколів SSL

Протокол SSL, або Secure Sockets Layer, є ключовим засобом забезпечення безпеки в Інтернеті. Він забезпечує конфіденційність каналу зв'язку та автентифікацію користувача. Протокол SSL складається з двох основних фаз:

1. Встановлення конфіденційного каналу комунікацій: Під час цієї фази відбувається налагодження захищеного каналу для передачі даних між клієнтом і сервером.
2. Автентифікація користувача: Після встановлення захищеного каналу проходить процес перевірки та підтвердження ідентичності обох сторін,

щоб забезпечити безпеку комунікації.

Дані сесії SSL включають:

1. Ідентифікаційний номер сесії: Унікальний номер, який ідентифікує конкретну сесію SSL.
2. Сертифікати обох сторін: Це цифрові документи, що підтверджують ідентичність сервера та клієнта.
3. Параметри алгоритму шифрування: Визначають методи шифрування, що використовуються для захисту даних під час передачі.
4. Алгоритм стиснення інформації: Вказує, який алгоритм стиснення використовується для зменшення обсягу передаваних даних.
5. "Загальний секрет" для створення ключів: Секретний ключ, який використовується для генерації сеансових ключів шифрування.
6. Відкритий ключ: ключ, який використовується для шифрування даних під час процесу обміну ключами, також називається Публічним ключем.

Загальна схема протоколу SSL показана на рисунку 2.2.

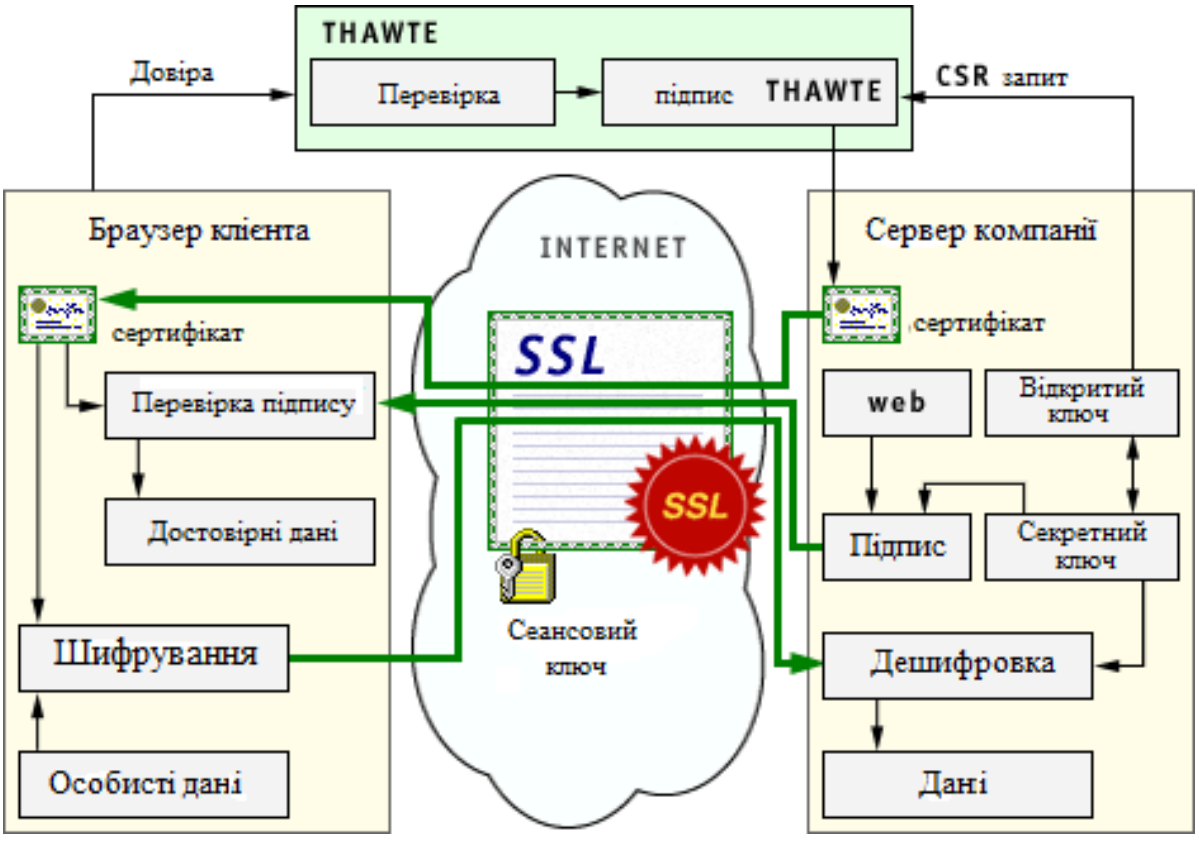


Рисунок 2.2 – Схема протоколу SSL

Протокол SSL (Secure Sockets Layer) або його сучасна версія TLS (Transport Layer Security) використовує різні техніки для забезпечення конфіденційності, цілісності та безпеки даних під час їх передачі через мережу. В основі TLS лежать криптографічні принципи, що забезпечують захищене з'єднання між клієнтом і сервером. Нижче розглянуто деякі з основних принципів роботи протоколу TLS:

1. Використання симетричних та асиметричних криптосистем: для забезпечення конфіденційності використовуються симетричні протоколи шифрування, такі як 3DES, AES-256 тощо. Для обміну ключовими даними застосовуються асиметричні криптосистеми, зокрема Діффі-Геллмана або RSA.
2. Забезпечення цілісності даних: Цілісність даних в протоколі TLS забезпечується за допомогою алгоритмів гешування, таких як SHA і MD5, а також за допомогою HMAC.
3. Протокол записів TLS: Забезпечує конфіденційність даних шляхом використання симетричних алгоритмів шифрування, таких як DES і RC4. Він також гарантує цілісність даних за допомогою геш-функцій SHA-1 або MD5.
4. Протокол діалогу TLS: Забезпечує цифровий підпис, який базується на алгоритмах RSA або DSS. Він гарантує надійність з'єднання через перевірку цілісності даних та використання асиметричних криптосистем.
5. Принципи роботи протоколу TLS: Включають криптографічну безпеку, сумісність, можливість розширення та відносну ефективність, що дозволяє забезпечити захищене з'єднання між двома користувачами мережі незалежно від їх програмних особливостей та ефективно використовувати ресурси.

Урізноманітнення протоколу, шляхом використання різних алгоритмів шифрування та гешування, дозволяє підтримувати високий рівень безпеки та конфіденційності в обміні даними через мережу.

У поточній версії протоколу TLS доступні наступні алгоритми:

1. Обмін ключами: RSA, Diffie-Hellman.
2. Конфіденційність: Advanced Encryption Standard (AES) з ключем довжиною 256 біт.
3. Цілісність: Secure Hash Algorithm (SHA) з хеш-функцією довжиною 256 біт.

Хоча TLS покращує безпеку в порівнянні з SSL, в ньому все ще є недоліки, такі як недостатній рівень криптографічної стійкості кодів контролю цілісності в контексті квантового обчислення.

2.1.2. Аналіз протоколу IPSec

IPsec (Internet Protocol Security) є набором протоколів, розроблених IETF для забезпечення безпеки мережевого з'єднання. Він є прозорим для користувачів і не потребує модифікації існуючих програм для використання. IPsec забезпечує три основні послуги:

1. Аутентифікація (AH) – гарантує ідентифікацію і перевірку цілісності даних.
2. Конфіденційність (ESP) – забезпечує шифрування даних, щоб забезпечити конфіденційність.
3. Обмін ключами – використовується для безпечного обміну ключами для шифрування та аутентифікації.

Для надання цих послуг часто створюється захищений приватний канал (VPN), який шифрує потік інформації користувачів. Загальна схема трансформації даних в IPsec у тунельному режимі показана на рисунку 2.3.

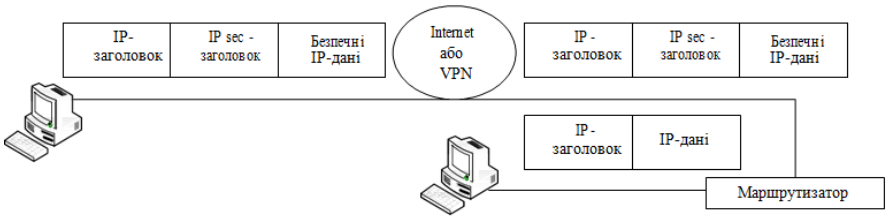


Рисунок 2.3 – Загальна схема трансформація даних в Ipsec

ESP і AH є два головними нижньорівневими протоколами, що використовуються в IPsec для забезпечення аутентифікації та шифрування даних, що передаються через з'єднання. Вони можуть використовуватися окремо або разом, хоча це не є стандартною практикою.

Існують два режими функціонування IPsec:

1. Режим тунелю: інкапсулює весь IP-пакет між шлюзами, створюючи традиційну VPN, яка забезпечує безпечний Інтернетий шлях.
2. Режим транспорту: забезпечує безпечне з'єднання між двома терміналами шляхом інкапсуляції вмісту IP-даних.

Під час процедури аутентифікації пакета виконується розрахунок контрольної суми ICV (Integrity Check Value) за допомогою алгоритмів MD5 або SHA-1. Для цього обидві сторони з'єднання мають використовувати спільний секретний ключ. Якщо значення ICV співпадає, відправник вважається успішно аутентифікованим. Протокол AH завжди виконує аутентифікацію, тоді як ESP може виконувати цю операцію на вибір.

Шифрування використовує спеціальний секретний ключ для зашифрування даних перед їх передачею, що запобігає несанкціонованому доступу до їх змісту з боку потенційних зловмисників. В протоколі IPsec можуть використовуватися різні алгоритми шифрування, такі як DES, 3DES, Blowfish, CAST, IDEA, RC5 і AES, а також інші шифровальні алгоритми.

Місця додаткової інформації показано на рисунку 2.4.

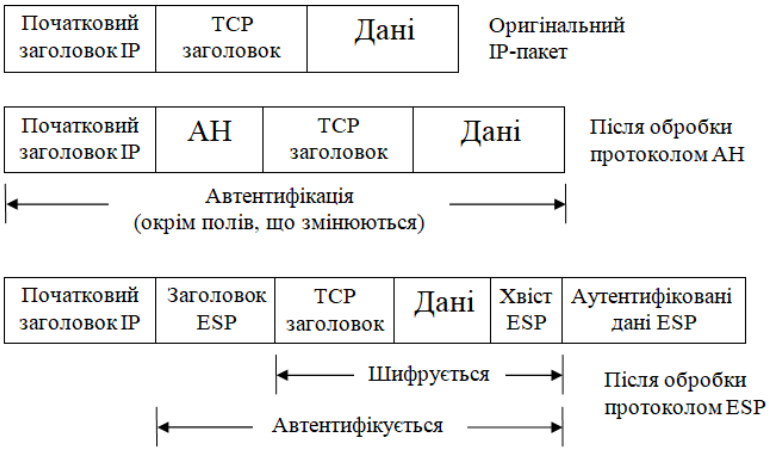


Рисунок 2.4 – Режим транспорту протоколу IPSec

Tunnel mode IPSec використовується для підключення віддалених комп'ютерів до віртуальної приватної мережі (VPN) або для безпечної передачі даних через відкриті комунікаційні канали, такі як Інтернет, між шлюзами для об'єднання різних сегментів віртуальної приватної мережі.

Переваги та недоліки протоколів AH і ESP згідно з рисунком 2.5: • ESP (Encapsulating Security Payload):

1. Переваги: Забезпечує шифрування даних, що захищає вміст пакета від несанкціонованого доступу.
2. Недоліки: Не забезпечує повної пакетної автентифікації.
3. AH (Authentication Header):
4. Переваги: Забезпечує повну автентифікацію пакета, що гарантує цілісність даних та їх автентичність.
5. Недоліки: Не шифрує дані, що залишає вміст пакета відкритим.

Комбінування цих протоколів для досягнення високого рівня безпеки дозволяє ESP шифрувати дані, а AH автентифікувати весь пакет, що забезпечує максимальний захист даних від несанкціонованого доступу та втручання.

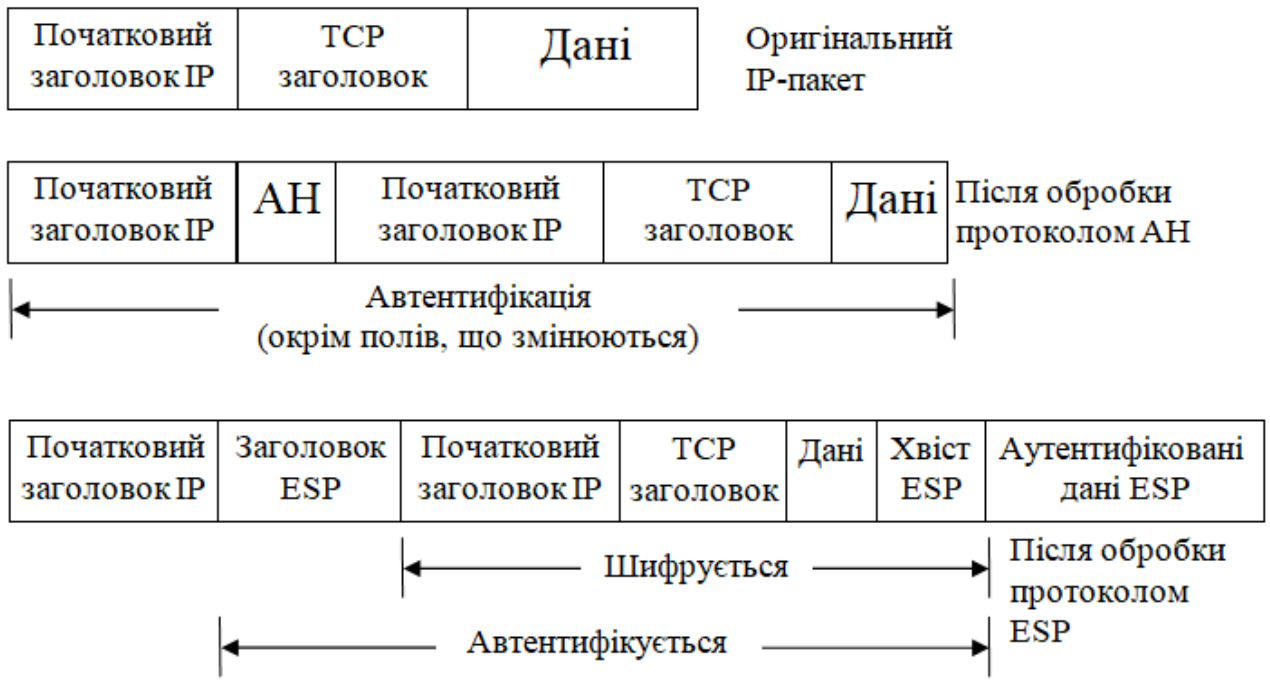


Рисунок 2.5 – Режим тунелю протоколу IPSec

Давайте подивимось на канал захищеності, в основі якого лежить протокол IPSec за схемою "хост-хост". У цій схемі зазвичай використовується режим транспорту між двома кінцевими вузлами мережі телекомунікації. Цей режим дозволяє зашифрувати тільки дані пакета, залишаючи заголовок незашифрованим. Такий підхід забезпечує конфіденційність даних, але не приховує метадані про відправника та отримувача. Для належного функціонування IPSec потрібно налаштувати ключі шифрування та аутентифікації на обох кінцях комунікаційного каналу. Така конфігурація дозволяє забезпечити високий рівень безпеки та інтегритету даних, що передаються між вузлами мережі (див. рисунок 2.6).

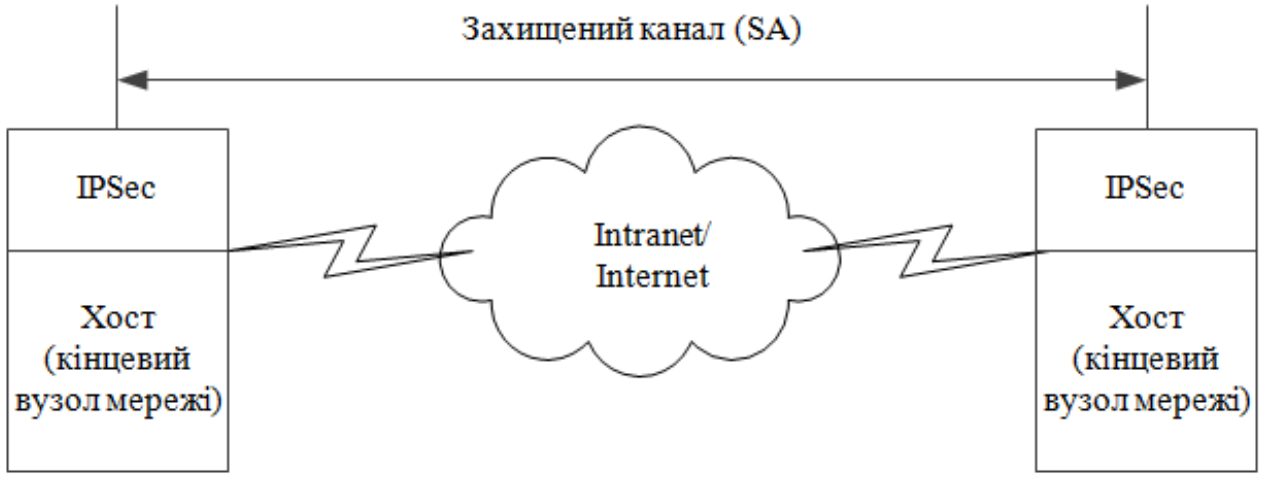


Рисунок 2.6 – Схема організації захищеного каналу “хост-хост”

Схема "шлюз – шлюз" в тунельному режимі IPSec є надійним рішенням для забезпечення безпечної передачі даних через відкриті канали зв'язку. Основні характеристики цього підходу полягають у наступному:

Переваги:

1. Високий рівень безпеки: Шифрування всього пакету даних, що передається між шлюзами, забезпечує ефективний захист від несанкціонованого доступу та перехоплення інформації.

Недоліки:

1. Обмежена гнучкість маршрутизації: Шифрування всього пакету даних призводить до неможливості коригування маршруту руху інформаційного потоку. Це ускладнює процес динамічної маршрутизації і може призвести до обмежень у реагуванні на зміни у мережевому середовищі.

У підсумку, схема "шлюз – шлюз" є ефективним засобом створення захищених тунелів між мережами, проте її обмеження у гнучкості маршрутизації може виявитися недоліком у деяких сценаріях мережевого взаємодії (див. рисунок 2.7).

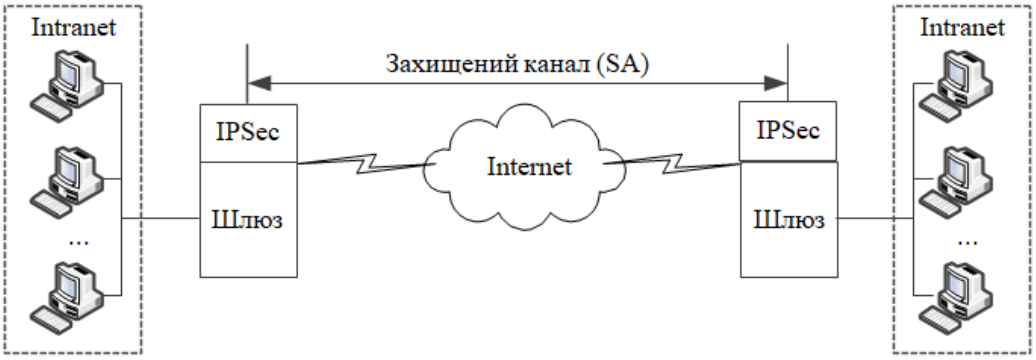


Рисунок 2.7 – Схема організації каналу “шлюз-шлюз”

Схема “хост-шлюз” (див. рисунок 2.8) часто використовуються при дистанційномудоступі.

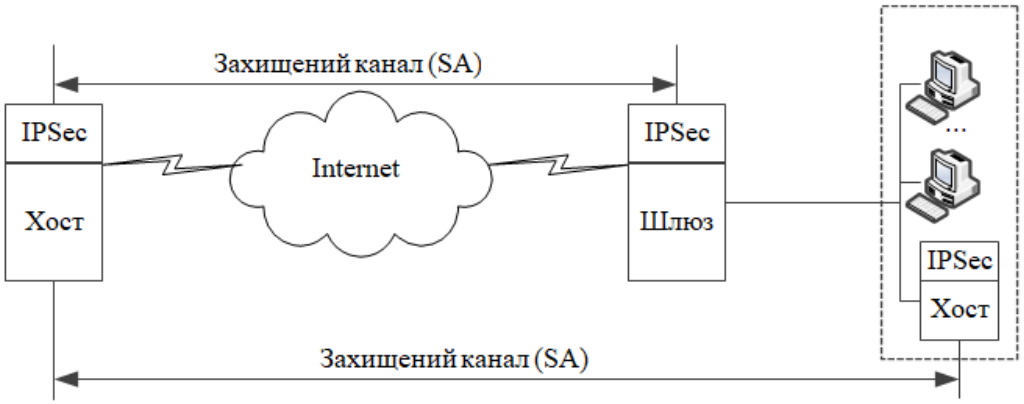


Рисунок 2.8 – Схема організації каналу “хост-шлюз” з додатковимканалом “хост-хост”

За останні роки технології квантового обчислення почали швидко розвиватися, що викликає певні виклики у забезпеченні безпеки традиційними методами, такими як протокол IPSec. Одна з головних причин цього полягає в тому, що квантові комп'ютери можуть швидко розгадувати криптографічні алгоритми, які використовуються для захисту інформації в мережах, такі як RSA і ECC. Це означає, що традиційні методи шифрування, які зараз використовуються в IPSec, можуть бути уразливими перед атаками квантовим комп'ютером.

Для забезпечення безпеки в епоху квантового обчислення потрібні нові методи шифрування, які відповідають цим викликам. Один із способів це зробити – це розвиток квантово-стійких протоколів шифрування, які використовують властивості квантової механіки для забезпечення безпеки передачі інформації. Такі протоколи можуть використовувати квантові ключі для захисту комунікацій та запобігання їх перехопленню або розшифруванню квантовим комп'ютером [13 – 16, 22].

Одним із прикладів такого протоколу є квантовий ключовий дистрибуційний протокол (QKD). QKD використовує принципи квантової механіки, такі як принципи невизначеності та незалежності спостерігачів, для забезпечення безпеки передачі ключів між віддаленими сторонами. Це дозволяє створювати криптографічні ключі, які неможливо перехопити без виявлення самої атаки.

Використання квантово-стійких протоколів шифрування може стати новим стандартом для забезпечення безпеки в мережах у світі квантового обчислення. Однак, наразі ці технології ще знаходяться на стадії досліджень і розробок, і їх широке впровадження може зайняти час. Тим не менш, у міру того як квантове обчислення розвиватиметься, важливо продовжувати дослідження та розвиток нових методів шифрування для забезпечення безпеки мереж.

2.2 Забезпечення автентичності на основі протоколу IPSec

AH (Authentication Header) використовується для забезпечення автентифікації IP-трафіку без шифрування. Він гарантує, що комунікація відбувається з очікуваним відправником і що дані, отримані отримувачем, не були змінені або підроблені під час передачі. Для досягнення цього AH використовує обчислення зашифрованого коду аутентифікації повідомлення (HMAC), який захоплює всі поля IP-пакета, за винятком тих, що можуть змінюватися під час транспортування, таких як TTL або контрольна сума заголовка. Цей код записується в AH-заголовок і передається отримувачу.

Протокол AH забезпечує автентифікацію та цілісність даних, але не забезпечує конфіденційність інформації. Це обмежує його використання в ситуаціях, коли також потрібно захистити зміст переданої інформації (див. рисунок 2.9).

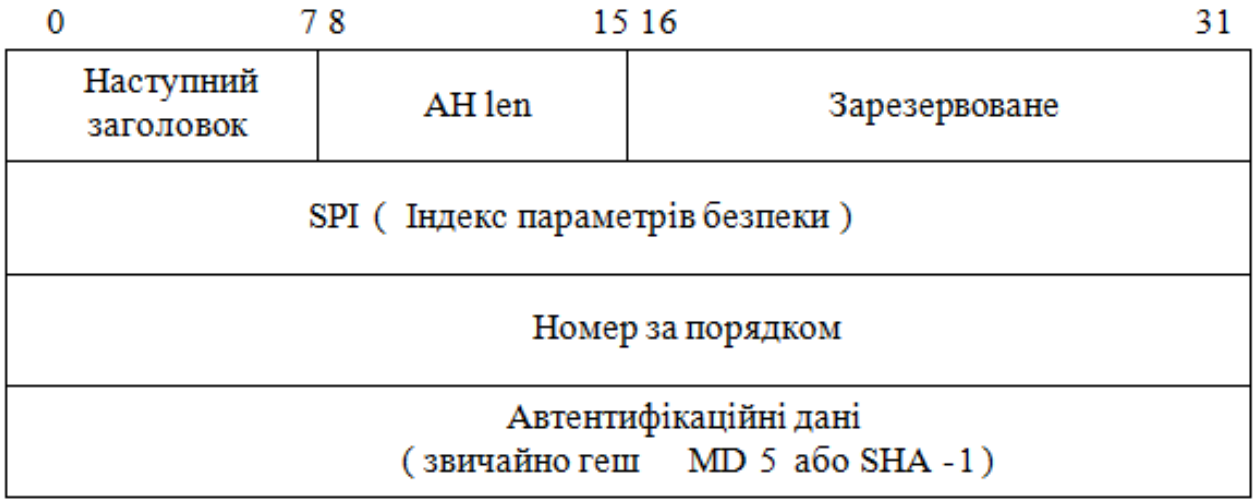


Рисунок 2.9 – Формат заголовка AH

Протокол AH (Authentication Header) використовується для забезпечення автентичності IP-трафіку без шифрування. Його заголовок містить п'ять основних полів:

1. Довжина AH: це поле визначає довжину заголовка пакета, виміряну в 32-бітових словах, за винятком двох слів.

2. Наступний заголовок – це поле, яке ідентифікує тип протоколу, використовуваного для наступного поля даних, що вбудоване в AH (Authentication Header) IPsec.
3. Зарезервоване поле: це поле призначене для майбутнього використання і повинне містити нулі.
4. Безпекопараметровий індекс (SPI): є 32-бітовим ідентифікатором, який допомагає отримувачу вибрати відповідний набір параметрів для обміну даними. Кожен обмін, захищений AH, використовує хеш-алгоритм (наприклад, MD5, SHA-1) та інші необхідні дані. SPI функціонує як індекс таблиці параметрів, що дозволяє визначити потрібний набір параметрів для обміну.

2.3 Висновки до другого розділу

Таким чином, проведений аналіз сучасних протоколів мережної безпеки, застосовуваних в IP-мережах для забезпечення цілісності, автентичності й конфіденційності передачі даних, дозволяє зробити такі висновки:

1. Використання механізмів захисту інформації на верхніх рівнях (рівня прикладного процесу, рівня представлення або сеансового рівня) моделі OSI дозволяє ефективно реалізувати функції безпеки конкретних мережних служб. Такий спосіб захисту інформації не залежить від того, які мережі (IP або IPX, Ethernet або ATM) застосовуються для транспортування даних, що є безсумнівною перевагою такого підходу. У той же час спостерігається залежність реалізації мережних служб і конкретних додатків від версії протоколу мережної безпеки. Зниження рівня (за специфікацією моделі OSI) підвищує універсальність використовуваних засобів захисту для будь-яких додатків і протоколів прикладного рівня, однак виникає залежність протоколу захисту від конкретної мережної технології;
2. Компромісним варіантом є протоколи мережної безпеки IPSec, що

функціонують на мережному рівні. З одного боку, вони “прозорі” для додатків. Протоколи IPSec домінують на сьогоднішній день у більшості реалізацій віртуальних приватних мереж і здійснюються як програмним чином, так і у вигляді програмно- апаратних реалізацій (рішення Cisco, Nokia).

3. Для контролю цілісності й автентичності пакетів даних у протоколах IPSec застосовуються спеціальні механізми захисту. Їх використання дозволяє за рахунок внесення в передані дані спеціально сформованої надмірності (MDC, MAC) ефективно розв’язувати завдання захисту пакетів даних від випадкової й зловмисної зміни. Формування кодів контролю цілісності й автентичності пакетів даних засноване на вживані ключових (MAC) і безключових (MDC)функцій гешування. Зазначені механізми застосовуються за замовчуванням упротоколах IPSec з метою забезпечення цілісності й автентичності пакетів даних у всіх реалізаціях мереж IPv6.

3 МОДЕЛЮВАННЯ ПРОЦЕСУ КІБЕРАТАКИ

3.1 Моделювання процесів кібербезпеки на основі моделі класів кібератак

Для моделювання процесів кібербезпеки важливо розглянути різноманітність класів кібератак (КБа) та їхні особливості у кожному конкретному випадку. Існує різні підходи до класифікації кібератак, але більшість з них мають умовний характер, що ускладнює однозначне визначення приналежності конкретної атаки до певного класу.

Професором О. Г. Корченком була розроблена загальноприйнята класифікація (див. рисунок 3.1), яка дозволяє більш точно виділити різні класи кібератак. Ця класифікація базується на ознаках і особливостях атак, враховуючи їхні характеристики для узагальнення.

Ця система класифікації може бути використана для аналізу та прогнозування ризиків у сфері кібербезпеки, сприяючи покращенню заходів захисту та реагування на потенційні загрози [22, 23].

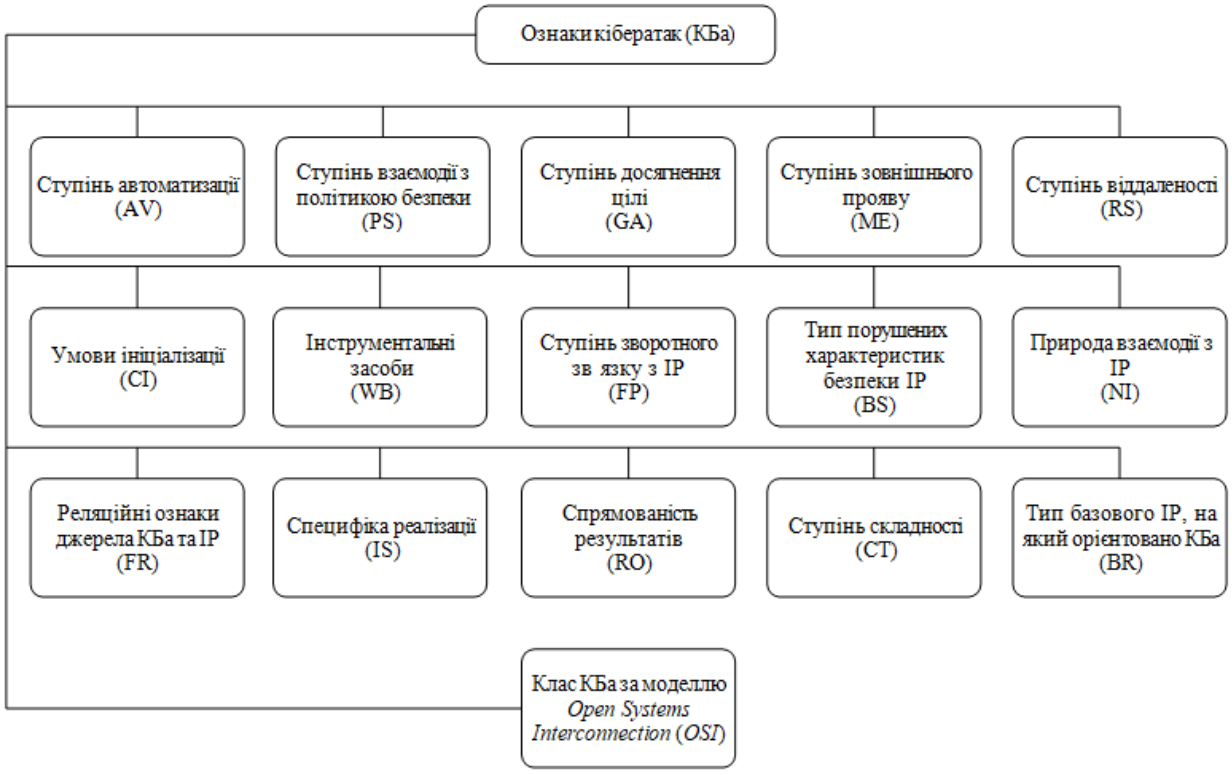


Рисунок 3.1 – Загальна класифікація О. Г. Корченко

В свою чергу, кожна з ознак характеризується певним базовим набором.

$$AV = \bigcup_{i=0}^{3} AV_i = \{\text{"мануальна"}, \text{"автоматизована"}, \text{"автоматична"}\};$$

$$PS = \bigcup_{i=0}^{2} PS_i = \{\text{"постполітизаційна"}, \text{"деполітизаційна"}\};$$

$$RS = \bigcup_{i=0}^{2} RS_i = \{\text{"локальні"}, \text{"віддалені"}\};$$

$$GA = \bigcup_{i=0}^{5} GA_i = \{\text{"інтераптаційні"}, \text{"інтерсептаційні"}, \text{"модифікаційні"}, \text{"фальсифікаційні"}, \text{"вільні"}\};$$

$$ME = \bigcup_{i=0}^{2} ME_i = \{\text{"пасивні"}, \text{"активні"}\};$$

$$CI = \bigcup_{i=0}^{2} CI_i = \{\text{"умовні"}, \text{"безумовні"}\};$$

$$WB = \bigcup_{i=0}^{3} WB_i = \{\text{"програмні"}, \text{"апаратні"}, \text{"нетипові"}\};$$

$$FP = \bigcup_{i=0}^{2} FP_i = \{\text{"зі зворотним зв'язком"}, \text{"без зворотного зв'язку"}\};$$

$$BS = \bigcup_{i=0}^{3} BS_i = \{\text{"К-дії"}, \text{"Ц-дії"}, \text{"Д-дії"}\};$$

$$NI = \bigcup_{i=0}^{2} NI_i = \{\text{"фізичні"}, \text{"логічні"}\};$$

$$FR = \bigcup_{i=0}^{4} FR_i = \{\text{"мономономні"}, \text{"полімономні"}, \text{"монополічні"}, \text{"поліполічні"}\};$$

$$IS = \bigcup_{i=0}^{9} IS_i = \{\text{"фрагментовані"}, \text{"без замовчання"}, \text{"скриті"}, \text{"пігібекінгові"}, \text{"маскарадні"}, \text{"непрямі"}, \text{"соціотехнічні"}, \text{"криптоаналітичні"}, \text{"неспецифічні"}\};$$

$$RO = \bigcup_{i=0}^{8} RO_i = \{\text{"розширюючі"}, \text{"викривляючі"}, \text{"розповсюджуючі"}, \text{"розкрадаючі"}, \text{"перевантажувальні"}, \text{"інформаційні"}, \text{"утримуючі"}, \text{"знищуючі"}\};$$

$$CT = \bigcup_{i=0}^{3} CT_i = \{\text{"прості", "складні", "системні"}\};$$

$$BR = \bigcup_{i=0}^{N} BR_i = \{\text{"ХОМ-ресурсні", "ЛОМ-ресурсні", "НІ-ресурсні", "ОС-ресурсні", "ПВ-ресурсні", "РД-ресурсні", "ПАС-ресурсні", "СА-ресірсні", "ФД-ресурсні"}\};$$

$$OSI = \bigcup_{i=0}^{N} OSI_i = \{\text{"OSI-00", "OSI-01", …, "OSI-36", …, "OSI-5E", "OSI-7F"}\}.$$

Для забезпечення адекватного та точного опису класифікації загроз безпеки банківських інформаційних ресурсів (БІР) згідно прийнятої шістнадцяткової системи параметрів, найбільш відповідними є класифікації I та II рівнів.

Класифікація I рівня характеризується наступними ознаками: автоматизована, постполітизаційна, віддалена, вільна, пасивна, безумовна, програмна, зі зворотнім зв'язком, з ознаками К-дій, логічна, мономономна, неспецифічна, інформаційна, системна, ресурсно-орієнтована за методологією ХОМ та відповідає стандарту ISO-36.

Класифікація II рівня охарактеризована наступними ознаками: автоматизована, постполітизаційна, віддалена, інтерпретаційна, активна, умовна, програмна, без зворотного зв'язку, з ознаками Д-дій, логічна, поліполічна, непряма, перевантажувальна, системна, ресурсно-орієнтована за методологією ХОМ та відповідає стандарту ISO-5E [27].

Ці дві класифікації дозволяють формулювати загрози та виявляти аномальну роботу, враховуючи синергію і гібридність сучасних загроз.

Формування основних принципів побудови (БІР ОБС) має в собі такі визначення:

1. Рівень безпеки ресурсів інформації банків (РББІР): Це оцінка захисту ресурсів інформації банків, яка визначається здатністю технічних пристроїв, користувачів та технологій інформації забезпечувати конфіденційність, цілісність, аутентичність і доступність під час обробки в автоматизованих банківських системах (АБС).
2. Захист інформаційних ресурсів банків (ЗІР БІР): Це рівень захисту

середовища інформації в сфері банків, який забезпечує його створення, розвиток і використання у організаційних і громадських інтересах.

3. Кібербезпека інформаційних ресурсів банків (КБ БІР): Це комплекс заходів, стратегій та технологій, що потрібні для захисту середовища банківських систем, їх користувачів та ресурсів, включаючи засоби безпеки, управління ризиками, професійну підготовку, страхування і технологічні рішення.

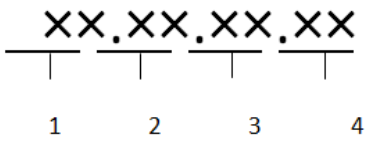
Класифікація загроз враховує такі напрямки:

1. Нормативно-правовий напрям: забезпечує виконання вимог нормативно-правових актів та стандартів.
2. Організаційний напрям: визначає структури, процеси і процедури управління безпекою.
3. Інженерно-технічний напрям: орієнтований на застосування технічних засобів та механізмів для забезпечення безпеки.

За характеристиками інформації (конфіденційність, цілісність, доступність, аутентичність) визначається рівень захищеності інформації на різних рівнях ієрархії інфраструктури автоматизованих банківських систем:

1. Фізичний рівень.
2. Рівень систем управління базами даних.
3. Мережевий рівень.
4. Системно-операційний рівень.
5. Рівень технологічних застосунків і сервісів банків.

Ці частини класифікатора розділені за допомогою крапки і представлені на рисунку 3.2.



(*1* – складова безпеки БІР, *2* – напрямовий характер;
3 – інформаційна особливість; *4* – ієрархічний рівень інфраструктури АБС).

Рисунок 3.2 – Складові узагальненого класифікатора

На рисунку 3.3 показано взаємозв'язок структурної схеми класифікатора загроз з автоматизованими банківськими системами (АБС) і оперативними банківськими системами (ОБС) [24].

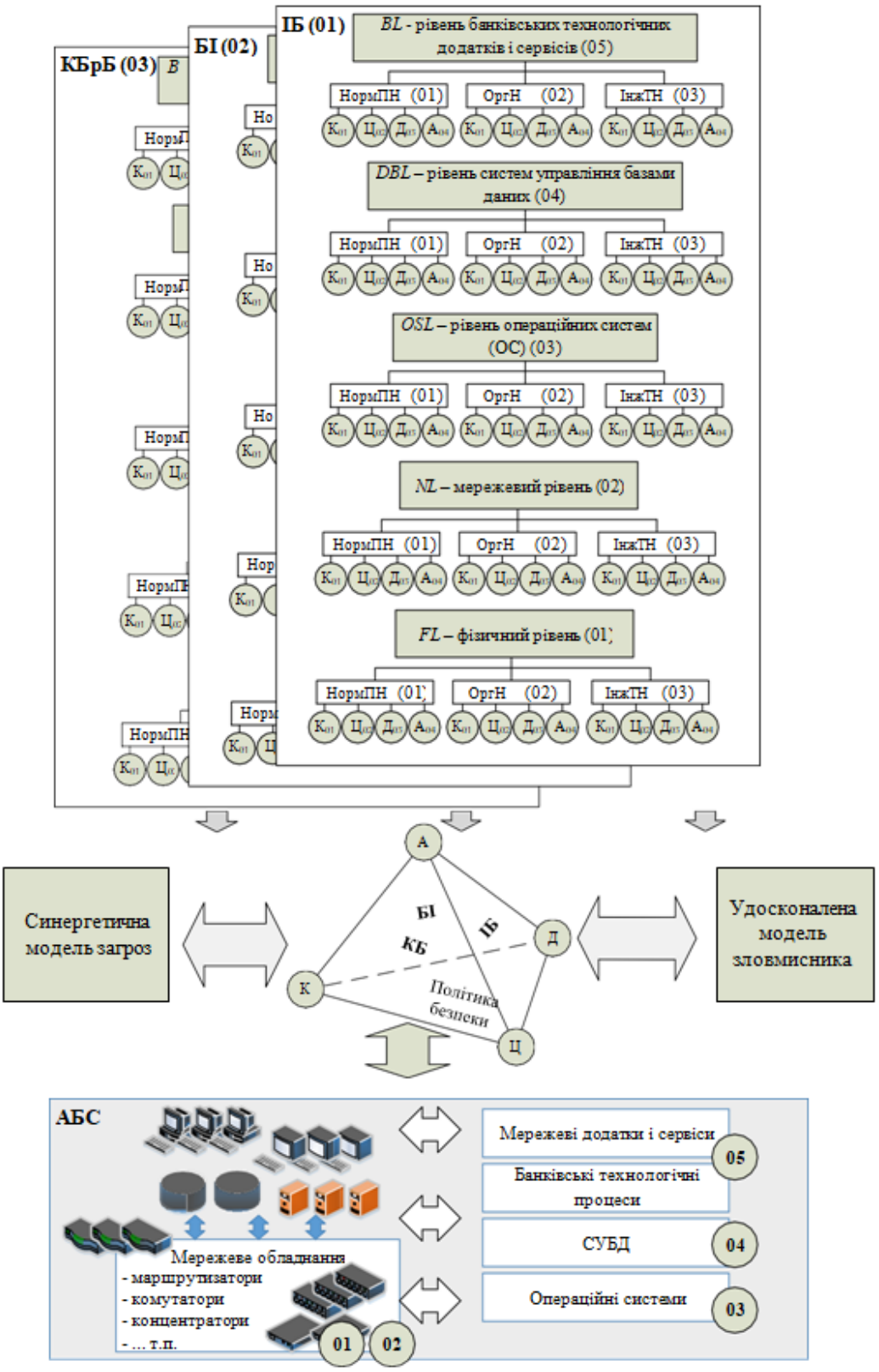


Рисунок 3.3 – Взаємозв’язок структурної схеми класифікатора загроз

3.1 Висновки до третього розділу

Класифікація КБА І-го та ІІ-го класів включає найбільш небезпечні та поширені види кібератак. Цей формалізований підхід сприяє розвитку систем опису ознак КБА і створенню чітких вимог до високоефективних систем захисту інформації (СЗІ). Різноманітність ознак і особливостей кібератак робить кожен випадок унікальним. Класифікація кібератак за ознаками надає базу для розробки концептуальних моделей для їхнього передбачення і формулювання вимог до превентивних систем. З урахуванням появи нових методів кібератак, класифікація може розширюватися, адаптуючись до сучасних викликів. Запропонований класифікатор дозволяє створити єдиний підхід до визначення загрози й впровадження алгоритмів виявлення аномальної або відхилень у роботі бездротових мереж, які використовуються в автоматизованих банківських системах.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

4.1.1 Правила охорони праці під час експлуатації електронно-обчислювальних машин

В Україні діють закони, які визначають права і обов'язки її працівників, а також організаційну структуру органів влади і виробництва. Конституція України – основний закон держави, який декларує рівні права і свободи всім жителям держави на вільний вибір праці, що відповідає безпечним і здоровим умовам, на відпочинок, на соціальний захист у разі втрати працездатності та у старості. Всі закони і нормативні документи узгоджуються, базуються і відповідають статтям Конституції.

Згідно закону України "Про охорону праці", в останній редакції 2018 року, охорона праці – це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних, лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людинив процесі трудової діяльності. Дія цього Закону поширюється на всіх юридичнихта фізичних осіб, які відповідно до законодавства використовують найману працю, та на всіх працюючих.

Для управління охороною праці створюються відповідні служби і призначаються компетентними органами посадові особи, які забезпечують вирішення конкретних питань охорони праці. На підприємстві з кількістю працюючих 50 і більше осіб роботодавець створює службу охорони праці відповідно до типового положення, що затверджується спеціально уповноваженим центральним органом виконавчої влади з питань нагляду за охороною праці (стаття 15). На підприємстві з кількістю працюючих менше 50 осіб функції служби охорони праці можуть виконувати в порядку сумісництва особи, які мають відповідну підготовку. На підприємстві з

кількістюпрацюючих менше 20 осіб для виконання функцій служби охорони праці можуть залучатися сторонні спеціалісти на договірних засадах, які мають відповідну підготовку.

За порушення законодавства про охорону праці, невиконання розпоряджень посадових осіб органів державного нагляду за охороною праці юридичні та фізичні особи, які відповідно до законодавства використовують найману працю, притягаються органами державного нагляду за охороною праці до сплати штрафу у порядку, встановленому законом.

Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями (затверджені наказом Міністерства соціальної політики України №207 від 14.02.2018) поширюються на всіх суб'єктів господарювання незалежно від форм власності, організаційно-правової форми і видів діяльності та встановлюють мінімальні вимоги безпеки та захисту здоров'я під час здійснення роботи, пов'язаної з використанням екранних пристроїв незалежно від їхнього типу та моделі. Під екранними пристроями розуміють електронні засоби для відтворення будь-якої графічної або алфавітно-цифрової інформації (на основі електронно-променевої трубки, рідкокристалічні, плазмові, проекційні, органічні світлодіодні монітори та інші новітні розробки у сфері інформаційних технологій)

Вимоги безпеки до робочих місць працівників з екранними пристроями передбачають:

Робочі місця працівників з екранними пристроями мають бути спроектовані так і мати такі розміри, щоб працівники мали простір для зміни робочого положення та рухів.

Для забезпечення безпеки та захисту здоров'я працівників усе випромінювання від екранних пристроїв має бути зведене до гранично допустимого рівня з погляду безпеки та охорони здоров'я працівників.

Організація робочого місця працівника з екранними пристроями має забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним, антропологічним, психофізіологічним вимогам, а також

характеру виконуваних робіт.

Робочий стіл або робоча поверхня повинні бути достатнього розміру та мати поверхню з низькою відбивною здатністю, допускати гнучкість під час розміщення екрана, клавіатури, документів і відповідного устаткування.

Робоче крісло має бути стійким і дозволяти працівнику з екранними пристроями легко рухатися та займати зручне положення. Сидіння має регулюватися по висоті, спинка сидіння - як по висоті, так і по нахилу.

4.1.2 Вимоги до споруд та приміщень під час експлуатації приміщень для експлуатації ЕОМ, ПЕОМ

Для всіх споруд і приміщень, в яких експлуатуються ЕОМ та ПЕОМ, визначається категорія з вибухопожежної і пожежної безпеки відповідно до ДСТУ Б В.1.1-36:2016 “Визначення категорій приміщень, будинків та зовнішніхустановок за вибухопожежною та пожежною небезпекою”.

Виробничі приміщення, в яких розташовані ЕОМ, не повинні межувати з приміщеннями, де рівні шуму та вібрації перевищують норму. Робочі місця з відеотерміналами або персональними ЕОМ у приміщеннях з джерелами шкідливих виробничих факторів розміщуються в ізольованих кабінах з обладнаним повітрообміном. Площу приміщень, в яких розташовують відеотермінали, визначають згідно з чинними нормативними документами з розрахунку на одне робоче місце, обладнане відеотерміналом: площа – не менше6,0 м^2, обсяг – не менше 20,0 м^3, з урахуванням максимальної кількості осіб, які одночасно працюють у зміні.

Стіни, стеля, підлога приміщень, де розміщені ЕОМ, виготовляються з матеріалів, дозволених для оздоблення приміщень органами державного санітарно-епідеміологічного нагляду.

Обслуговування, ремонт та налагодження ЕОМ, вузлів та блоків ЕОМ виконують в окремому приміщенні (майстерні), які можуть передбачити можливість вологого очищення поверхонь комунікацій та опалювальних приладів.

Підлогу всієї зони обслуговування, ремонту та налагодження ЕОМ, вузлів та блоків ЕОМ вкривають діелектричними килимками, термін використання яких після їх випробування на електричну міцність не закінчився, або викладена ізолювальними підстилками (шириною не менше ніж 0,75-0,8 м) для ніг.

Раціональне освітлення виробничих ділянок є одним з найважливіших факторів попередження травматизму і професійних захворювань. Правильно організоване освітлення створює сприятливі умови праці, підвищує працездатність і продуктивність праці. Освітленість на робочому місці повинна бути такою, щоб працюючий міг без напруги зору виконувати свою роботу при припустимому з народногосподарської точки зору витратою засобів, матеріалів і електроенергії.

Працівникам забороняється:

1. Працювати поблизу відкритих струмовідних частин, крім випадків, обумовлених «Вимогами охорони праці під час експлуатації електронно-обчислювальних машин».
2. Залишати без догляду увімкнуте в мережу живлення устаткування, прилади, що використовуються при проведенні робіт.
3. Залишати на устаткуванні, приладах запобіжники, з'єднувачі, провід, залишки флюсу, припою тощо.
4. Розміщувати на одному робочому столі (місці) два або більше увімкнутих в мережу живлення відеотермінали з знятими футлярами.
5. Проводити всередині відеотермінала операції, що виконуються тільки двома руками, без попереднього вимкнення відеотермінала з мережі живлення і зняття залишкових зарядів з конденсаторів фільтрів випрямлячів та другого анода кінескопа.
6. Проводити всередині відеотерміналу операції, що виконуються однією рукою.

4.2 Безпека в надзвичайних ситуаціях

4.2.1 Освітлення виробничих приміщень для роботи ВДТ

Приміщення для роботи з ВДТ повинні мати природне та штучне освітлення відповідно до ДБН В.2.5-28-2018.

За виробничої потреби дозволяється експлуатувати ЕОМ у приміщеннях без природного освітлення за узгодженням з органами державного нагляду за охороною праці та органами і установами санітарно-епідеміологічної служби.

Вікна приміщень з ВДТ повинні мати регулювальні пристрої для відкривання, а також жалюзі, штори, зовнішні козирки тощо.

Штучне освітлення приміщення з робочими місцями, обладнаними ВДТ ЕОМ загального та персонального користування, має бути обладнане системою загального рівномірного освітлення. У виробничих та адміністративно- громадських приміщеннях, де переважають роботи з документами, допускається вживати систему комбінованого освітлення (додатково до загального освітлення встановлюються світильники місцевого освітлення).

Загальне освітлення має бути виконане у вигляді суцільних або переривчатих ліній світильників, що розміщуються збоку від робочих місць (переважно зліва) паралельно лінії зору працівників. Допускається застосовуватисвітильники таких класів світлорозподілу:

1. Світильники прямого світла – П;
2. Переважно прямого світла – Н;
3. Переважно відбитого світла – В.

При розташуванні відеотерміналів ЕОМ за периметром приміщення лінії світильників штучного освітлення повинні розміщуватися локально над робочими місцями.

Для загального освітлення необхідно застосовувати світильники із розсіювачами та дзеркальними екранними сітками або віддзеркалювачами,

укомплектовані високочастотними пускорегулювальними аппаратами. Застосування світильників без розсіювачів та екранних сіток забороняється.

Як джерело світла при штучному освітленні повинні застосовуватися, як правило, люмінесцентні лампи типу ЛБ. При обладнанні відбивного освітлення у виробничих та адміністративно-громадських приміщеннях можуть застосовуватися металогалогенні лампи потужністю до 250 Вт. Допускається у світильниках місцевого освітлення застосовувати лампи розжарювання.

Яскравість світильників загального освітлення в зоні кутів випромінювання від 50º до 90º відносно вертикалі в подовжній і поперечній площинах повинна складати не більше 200 кд/м2, а захисний кут світильників повинен бути не більшим за 40º.

Коефіцієнт пульсації повинен не перевищувати 5 % і забезпечуватися застосуванням газорозрядних ламп у світильниках загального і місцевого освітлення.

За відсутності світильників без розсіювачів та екранних сіток лампи багатолампових світильників або розташовані поруч світильники загального освітлення необхідно підключати до різних фаз трифазної мережі.

Рівень освітленості на робочому столі в зоні розташування документів має бути в межах 300…500 лк. У разі неможливості забезпечити даний рівень освітленості системою загального освітлення допускається застосування світильників місцевого освітлення, але при цьому не повинно бути відблисків на поверхні екрану та збільшення освітленості екрану більше ніж до 300 лк.

Світильники місцевого освітлення повинні мати напівпрозорий відбивач світла з захисним кутом не меншим за 40º.

Необхідно передбачити обмеження прямої блискості від джерела природного та штучного освітлення, при цьому яскравість поверхонь, що світяться (вікна, джерела штучного світла) і перебувають у полі зору, повинна бути не більшою за 200 кд/м2.

Необхідно обмежувати відбиту блискість шляхом правильного вибору

типів світильників та розміщенням робочих місць відносно джерел природногота штучного освітлення. При цьому яскравість відблисків на екрані відеотерміналу не повинна перевищувати 40 кд/м2, яскравість стелі при застосуванні системи відбивного освітлення не повинна перевищувати 200 кд/м2.

Необхідно обмежувати нерівномірність розподілу яскравості в полі зору осіб, що працюють з відеотерміналом, при цьому відношення значень яскравості робочих поверхонь не повинно перевищувати 3:1, а робочих поверхонь і навколишніх предметів (стіни, обладнання) – 5:1.

Необхідно використовувати систему вимикачів, що дозволяє регулювати інтенсивність штучного освітлення залежно від інтенсивності природного, а також дозволяє освітлювати тільки потрібні для роботи зони приміщення.

Для забезпечення нормованих значень освітлення в приміщеннях з відеотерміналами ЕОМ загального та персонального користування необхідно очищати віконне скло та світильники не рідше ніж 2 рази на рік, та своєчасно проводити заміну ламп, що перегоріли.

4.2.2 Попередження наслідків аварій на виробництвах із застосуванням хлору. Вплив хлору на людей, перша допомога, профілактика уражень

Великі аварії на хімічно небезпечних об’єктах є одними з найбільш небезпечних технологічних катастроф, які можуть призвести до масового отруєння і загибелі людей і тварин, значного економічного збитку і важких екологічних наслідків. Причини аварій, в більшості випадків, пов’язані з порушеннями встановлених норм і правил при проектуванні, будівництві і реконструкції хімічно небезпечних об’єктів, порушенням технології виробництва, правил експлуатації обладнання, машин і механізмів, апаратів, низької трудової і технологічної дисципліни виробничого процесу.

Хлор за обсягом виробництва і галузі застосування є одним з найважливіших продуктів хімічної промисловості. Широке використання і

великі обсяги виробництва хлору визначають високу потенційну небезпеку виникнення надзвичайних ситуацій, обумовлених його аварійними викидами в навколишнє середовище. Ці обставини поглиблюються фізико-хімічними та токсикологічними властивостями хлору, що є сильнодіючою отруйною речовиною задушливого характеру. Токсикологічні та фізико-хімічні властивостіхлору є основними вражаючими чинниками при його аварійних викидах.

Комплекс заходів щодо зберігання і використання хлору включає:

1. Використання безпечних технологій;
2. Здійснення організаційних, технічних та інших заходів, що забезпечують високу експлуатаційну надійність об'єктів, а також обмеження розповсюдження хлору за межі санітарно-захисної зони при аваріях і руйнуваннях;
3. Раціональне розміщення хлору з урахуванням можливих наслідків
4. Підготовка і проведення спеціальних заходів щодо захисту населення, що дозволяють знизити масштаби шкідливого впливу.

Велике значення в профілактиці аварій з викидом хлору має оснащеність цих підприємств швидкодіючими технічними засобами захисту, в тому числі автоматичним відсічними пристроями, системами вибухопопередження і локалізації розвитку аварій, а так само відповідною підготовкою персоналу.

Ефективним способом зменшення наслідків аварій є зниження запасів хлору до мінімальної, необхідної за технологією, кількості. Особливо це важливо на етапах вантажно-розвантажувальних робіт, в сховищах хлору і готової продукції. Доцільно проводити роботи, спрямовані на створення таких умовзберігання хлору, які дозволяють виключити можливість його залпових викидів у великих обсягах.

Стабільність експлуатації об'єктів з хлором і його похідними повинна забезпечуватися високою надійністю електропостачання, та використанням систем безаварійної зупинки при припиненні подачі електроенергії. Для підвищення міцності обладнання може проводитися обвалювання,

заглиблення вгрунт або розміщення під землею. Навколо великих сховищ доцільно споруджувати захисні оболонки.

При гострому отруєнні хлором виникає токсичний ларингіт, бронхіт, в більш важких випадках – набряк легень, пневмонія. Вдихання концентрованих парів хлору викликає хімічний опік верхніх дихальних шляхів і може привестидо рефлекторної зупинки дихання.

У клінічній картині, що розвивається при отруєнні хлором, виділяють період роздратування (рефлекторний період), обумовлений дратівливою дією хлору на слизову дихальних шляхів, очі. При цьому виникає відчуття печіння і дряпання в дихальних шляхах, відчуття утруднення дихання, різь в очах, слинотеча.

Одним з грізних проявів ураження хлором є розвиток токсичного набряку легень. Причиною його є підвищення проникності капілярної і альвеолярної стінки. Токсичний набряк легень виникає як в результаті безпосереднього впливу хлору на легеневу тканину, так і в результаті загальних розладів в організмі.

Перша допомога ураженому хлором полягає в наступному:

1. Одягання на потерпілого промисловогопротигаза типуВ або громадянського ДП-5, ГП-7;
2. Винесення потерпілого на незаражену територію і зняття протигаза;
3. Звільнення від тісного одягу;
4. При відсутності дихання – штучне дихання, переважно методом “рот в рот”;
5. Вдихання, для пом’якшення подразнення, аерозолю 0,5% розчину соди, а також кисню;
6. Промивання шкіри і слизових оболонок 2% содовим розчином;
7. Максимальне обмеження самостійного пересування потерпілого, подальше транспортування тільки в лежачому положенні;
8. У холодну пору – відігрівання і забезпечення повного спокою;
9. Накласти асептичні пов’язки на рани і іммобілізувати пошкоджені

кінцівки;

4.3 Висновки до четвертого розділу

У підрозділі Охорона праці розглянуто правила охорони праці під час експлуатації електронно-обчислювальних машин та вимоги до споруд та приміщень. В підрозділі Безпека в надзвичайних ситуаціях описано попередження наслідків аварій на виробництвах із застосуванням хлору. Наведено інформацію про освітлення виробничих приміщень для роботи ВДТ.

ВИСНОВКИ

Швидкий розвиток та впровадження обчислювальної техніки та мереж збільшують обсяг послуг в Інтернеті, але також зростає ризик кіберзлочинів, які стосуються порушення безпеки інформації. Хоча використання комплексних систем захисту інформації (КСЗІ) широко поширене, важливо ефективно оцінювати легітимність операцій, особливо в системах, які важливі для національної безпеки. Системи виявлення атак (СВА) грають ключову роль у виявленні надзвичайної діяльності та відхилень від нормального в комунікаційних системах. Застосування загальнодоступних баз даних, таких як NSL-KDD, сприяє високій точності виявлення кібератак, що дозволяє кількісно оцінювати загрози. Ознакова класифікація кібератак покращує способи виявлення та реагування на нові типи загроз, забезпечуючи ефективніший захист інформації в сучасних комунікаційних системах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В. Л. Політика інформаційної безпеки: підручник / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко ; під заг. ред. проф. В. О. Хорошка. – К.: ПВП «Задруга», 2014

2. Report on Post-Quantum Cryptography. URL: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (Дата обращения 255.12.2019).

3. Тимощук, В., & Стебельський, М. (2023). Шифрування даних в операційних системах. Матеріали VI Міжнародної студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання “, 183-184.

4. Букатка, С., & Тимощук, В. (2023). ХЕШ-алгоритм шифрування паролів користувачів ос Linux. Матеріали VI Міжнародної студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання “, 112-113.

5. ГОСТ Р34.10-94. Інформаційна технологія. Криптографічний захист інформації. Процедури розробки і перевірки електронного цифрового підпису на базі асиметричного криптографічного алгоритму. – Національний стандарт.

6. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД, (14.06. 2024; Суми, Україна), 191-193. https://doi.org/10.62731/mcnd-14.06.2024.004

7. СТУ 4145–2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К.: Держстандарт України, 2002. – 40 с.

8. Бекер, І., Тимощук, В., Маслянка, Т., & Тимощук, Д. (2023). МЕТОДИКА ЗАХИСТУ ВІД ПОВІЛЬНИХ ТА ШВИДКИХ BRUTE-FORCE АТАК НА IMAP СЕРВЕР. Матеріали конференцій МНЛ, (17 листопада 2023 р., м. Львів), 275-276.

9. ДСТУ 7624–2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – К.: Держстандарт України, 2014. – 235 с.

10. Ванца, В., Тимощук, В., Стебельський, М., & Тимощук, Д. (2023). МЕТОДИ МІНІМІЗАЦІЇ ВПЛИВУ SLOWLORIS АТАК НА ВЕБСЕРВЕР. Матеріали конференцій МЦНД, (03.11. 2023; Суми, Україна), 119-120.

11. Іваночко, Н., Тимощук, В., Букатка, С., & Тимощук, Д. (2023). РОЗРОБКА ТА ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ ВІД UDP FLOOD АТАК НА DNS СЕРВЕР. Матеріали конференцій МНЛ, (3 листопада 2023 р., м. Вінниця), 177-178.

12. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD): СОУ Н НБУ 65.1 СУІБ 1.0:2010. – К.: НБУ, 2010. – 209с.

13. Демчук, В., Тимощук, В., & Тимощук, Д. (2023). ЗАСОБИ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАК. Collection of scientific papers «SCIENTIA», (November 24, 2023; Kraków, Poland), 130-130.

14. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD). – К.: НБУ., 2010. – 67 с.

15. Тимощук, В., & Тимощук, Д. (2022). Віртуалізація в центрах обробки даних-аспекти відмовостійкості. Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології “Тернопільського національного технічного університету імені Івана Пулюя, 95-95.

16. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів національного банку України. – Режим доступу: zakon.rada.gov.ua/laws/show/v0365500-11

17. Міжбанківські розрахунки в Україні. – Режим доступу: http://www.bank.gov.ua/control/uk/publish/. Accessed on: Des. 09, 2019.

18. Основи створення комплексної системи економічної безпеки підприємства: теоретичний аспект / Коваленко К.В. – Режим доступу до статті http://www.nbuv.gov.ua. Accessed on: Des. 09, 2019.

19. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). СИСТЕМА ЗМЕНШЕННЯ ВПЛИВУ DOS-АТАК НА ОСНОВІ MIKROTIK. Матеріали конференцій МЦНД, (17.05. 2024; Ужгород, Україна), 198-200. https://doi.org/10.62731/mcnd-17.05.2024.008

20. Mathy Vanhoef, Key Reinstallion Attacks. Breaking WPA2 by forcing nonce reuse. URL: http://www.krackattacks.com.

21. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170. https://doi.org/10.36074/logos-21.06.2024.034

22. Stewart S. Miller, Wi-Fi Security –McGraw-Hill Networking Professional Publishing, 2003, 309 p.

23. Karpinski, M., Korchenko, A., Vikulov, P., Kochan, R., Balyk, A., & Kozak, R. (2017, September). The etalon models of linguistic variables for sniffing-attack detection. In 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems : Technology and Applications (IDAACS) (Vol. 1, pp. 258-264). IEEE.

24. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, 2022(1), 55-61.

25. Skarga-Bandurova, I., Biloborodova, T., Skarha-Bandurov, I., Boltov, Y., & Derkach, M. (2021). A Multilayer LSTM Auto-Encoder for Fetal ECG Anomaly Detection. Studies in health technology and informatics, 285, 147-152.

26. Kulchytskyi, T., Rezvorovych, K., Povalena, M., Dutchak, S., & Kramar, R. (2024). LEGAL REGULATION OF CYBERSECURITY IN THE CONTEXT OF THE DIGITAL TRANSFORMATION OF UKRAINIAN SOCIETY. Lex

Humana (ISSN 2175-0947), 16(1), 443-460.