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)

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломного проекту (роботи)

магістр
(освітній рівень)

на тему: *«Дослідження методів ідентифікації загроз в середовищі безпровідних мереж»*

Виконав: студент (ка) *VI* курсу, групи *СБм-61*
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Ліщинський В.С.
підпис (прізвище та ініціали)

Керівник *Карпінський М.П..*
підпис (прізвище та ініціали)

Нормоконтроль *Кареліна О.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 20*19*

АНОТАЦІЯ

Дослідження методів ідентифікації загроз в середовищі безпровідних мереж // Дипломна робота ОР «Магістр» // Ліщинський Владислав Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2019 // С. , рис. – 111, табл. – , кресл. – , додат. – .

Ключові слова: БЕЗПРОВІДНІ МЕРЕЖІ, WI-FI, ОС, ЗАГРОЗИ, РИЗИКИ, АНОМАЛІЇ, SSL, TLS, IPSEC, КЛАСИФІКАТОР ЗАГРОЗ.

Дана магістерська кваліфікаційна робота присвячена дослідженню методів ідентифікації загроз в безпровідних мережах. Проведено дослідження засобів і механізмів забезпечення інформаційної безпеки та достовірності інформації в середовищі безпровідних мереж.

Для отримання якісної оцінки кібератак і їх подальшої класифікації, запропоновано застосувати відому просторі ознак класифікацію. Такий підхід дозволив розширити простір ознак для опису невідомих класів кібератак.

В роботі запропоновано класифікатор загроз, що забезпечує можливість формування єдиного підходу щодо визначення загрози та її врахування під час виявлення аномальної роботи, або відхилення від нормальної роботи в середовищі безпровідних мереж на прикладі АБС.

У першій главі наведено основні теоретичні відомості щодо тематики роботи.

У другій главі проведено аналіз протоколів забезпечення конфіденційності, цілісності та автентичності даних.

У третій главі наведено методику моделювання процесів кібербезпеки на основі моделі класів кібератак.

В спеціальній частині описано сучасні програми - аналізатори мережевого трафіку.

В п’ятому розділі обчислено основні показники економічної ефективності від розробки і реалізації запропонованого алгоритму.

У підрозділі "Охорона праці" розглянуто правила охорони праці під час експлуатації електронно-обчислювальних машин У підрозділі "Безпека життєдіяльності" описано окремі питання безпеки у виробничих приміщеннях.

В розділі "Екологія" по радіоекології та роботі з банками екологічної інформації.

ANNOTATION

Research of threats identification methods in a wireless network environment // Thesis of the Master degree // Lishchynskyi Vladyslav // Ternopil Ivan Puluj National Technical University, Department of Computer Information Systems and Software Engineering, Department of Cybersecurity // Ternopil, 2019 // P. 111, Tables – , Fig. – , Diagrams – , Annexes. – , References – .

Keywords: WIRELESS NETWORKS, WI-FI, OS, THREATS, RISKS, Anomalies, SSL, TLS, IPSEC, THREAT CLASSIFIER.

This master's qualification thesis is devoted to the study of methods of threats identification in wireless networks. Research on the means and mechanisms for ensuring information security and reliability of information in the wireless network environment has been made. In order to obtain a qualitative assessment of cyber attacks and their further classification, it is proposed to apply the known space of classification features. This approach made it possible to extend the space of features to describe unknown classes of cyberattacks.The paper proposes a classifier of threats, which provides the possibility of creating a unified approach to detect the threat when detecting abnormal work, or deviating from normal work in a wireless network environment.

The first chapter provides basic theoretical information on the subject of work.

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

The third chapter describes how to model cybersecurity processes based on the model of cyberattack classes.

The special part describes the modern programs - network traffic analyzers.

The fifth section calculates the main cost-effectiveness indicators for developing and implementing the proposed algorithm.

The section "Occupational safety" discusses the rules of occupational safety during the operation of electronic computers In the section "Safety of life" describes some issues of safety in industrial premises.

In the "Ecology" section radioecology and working with environmental information banks are described.

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 телекомунікації забезпечують надійність функціонування великої кількості інформаційних систем різноманітного призначення. Більшість таких систем несуть у собі інформацію конфіденційного характеру. Таким чином, вирішення задачі автоматизації процесів обробки даних спричиняє проблему інформаційної безпеки, при цьому актуальною проблемою є своєчасне виявлення аномальної та/або відхилення від нормальною роботи ПЗ та забезпечення бездротових мереж [1, 2, 10, 11, 13–17, 19–23, 28, 34]. З часу своєї появи банки незмінно викликали злочинний інтерес, який був пов’язаний зі зберіганням в кредитних організаціях не тільки грошових коштів, але і важливої, найчастіше секретної інформації про фінансову і господарську діяльність багатьох людей, компаній, організацій, цілих держав. Комп'ютеризація банківської діяльності дала змогу значно збільшити продуктивність праці співробітників банку, впровадити нові фінансові продукти і технології. Прогрес техніки злочинів йшов не менш швидкими темпами. В даний час понад 90% всіх злочинів пов’язано з використанням автоматизованих систем обробки інформації банку (АСОІБ) [11]. Захист власне банківської системи має використовувати потужні засоби автентифікації і контролю дій як внутрішніх користувачів, так і клієнтів. Загально-прийнято, що найбільш надійний захист можуть забезпечити засоби двофакторній автентифікації, будь то електронні ключі (токени) або генератори одноразових паролів. Безпека даних при зберіганні вимагає використання засобів шифрування, які можуть працювати або на рівні сховищ даних, або на рівні окремих компонентів системи, наприклад, таблиць баз даних. Безпека банкоматів і платіжних терміналів має забезпечуватись з використанням традиційних засобів – засобів антивірусного захисту. У той же час специфіка таких пристроїв потребує застосування додаткових засобів захисту, зокрема створення “замкнутого програмно-апаратного середовища”, що повністю виключає встановлення будь-якого стороннього ПЗ і підключення зовнішніх пристроїв [1, 29, 35]. Для забезпечення

адекватності системи захисту інформації доцільно застосовувати принципи Ризик-менеджменту. Метод дозволить, при розумному підході визначити і класифікувати загрози і, відповідно до ймовірності настання негативних наслідків та їх можливої оцінкою втрат для Банку, створити Систему захисту [3, 21, 24, 28, 29, 35]. На практиці, забезпечення інформаційної безпеки відбувається в умовах випадкового впливу чинників, які в повній мірі складно передбачити заздалегідь при проектуванні системи захисту інформації.

Однією з істотних проблем при проектуванні та експлуатації систем захисту інформації є нехтування методологією системного аналізу щодо засобів і інструментів для їх захисту. Слід визнати складність, часом неможливість, об'єктивного підтвердження ефективності системи захисту інформації, що багато в чому визначається неповнотою нормативно-методичного забезпечення інформаційної безпеки, перш за все в області показників та критеріїв [11, 12]. Міжнародний стандарт для операцій по банківських картках з чіпом (EMV), введений у 2005 році, визначає фізичну, електронну та інформаційну взаємодію між банківською карткою та платіжним терміналом для фінансових операцій на основі стандартів ISO / IEC 7816 для контактних карток, та ISO / IEC 14443 для безконтактних карток. Інтернет-банкінг широко поширився серед банків та клієнтів. Використання Інтернет-ресурсів як альтернативного засобу передачі пін-коду клієнта в банк призводить до зниження витрат на передачу, проте дозволяє поліпшити банківську конкурентоспроможність та збільшити гнучкість роботи банку з клієнтами. Головними перешкодами на шляху інтернет-банкінгу є безпека системи, відсутність довіри та правової підтримки [17, 18]. В роботі [7] відзначається, що безпека інформації може бути забезпечена лише при комплексному використанні всього набору наявних засобів захисту у всіх структурних елементах виробничої системи на всіх етапах технологічного циклу обробки інформації. Найбільший ефект досягається при об’єднанні в єдиний цілісний механізм-систему захисту інформації (СЗІ) всіх використовуваних засобів, методів та заходів. При цьому функціонування системи має контролюватися, оновлюватися та доповнюватися в залежності від зміни зовнішніх та внутрішніх умов.. *Метою* даної роботи є моделювання процесів

ідентифікації кібератак та формалізація принципів побудови класифікатора загроз складових безпеки.

Для досягнення поставленої мети необхідно вирішити наступні *завдання*:

1. Аналіз основних загроз в середовищі безпровідних мереж.
2. Аналіз методів виявлення аномалій і зловживань.
3. Аналіз методик оцінки ризиків.
4. Дослідження засобів і механізмів забезпечення інформаційної безпеки та достовірності інформації в середовищі безпровідних мереж.
5. Моделювання процесів кібербезпеки на основі моделі класів кібератак.
6. Формалізація принципів побудови класифікатора загроз складових безпеки БІн: інформаційної безпеки, кібербезпеки, безпеки інформації.

Об'єктом досліджень є загроз в середовищі безпровідних мереж.

Предметом дослідження є моделі та алгоритми процесів кібератак, методи захисту інформації.

Наукова новизна та практична цінність роботи: розширення простору ознак кібератак дає можливість підвищити точність класифікації. Запропонований класифікатор загроз забезпечує можливість формування єдиного підходу щодо визначення загрози та її врахування під час виявлення аномальної роботи, або відхилення від нормальної роботи в середовищі безпровідних мереж на прикладі АБС

Апробація результатів роботи. Окремі результати роботи доповідались на VII науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 11 – 12 грудня 2019 р.

1 ТЕОРЕТИЧНА ЧАСТИНА

1.1 Аналіз основних загроз в середовище безпровідних мереж

Для аналізу основних видів загроз безпеки інформації в середовищі безпровідних мереж використовуємо відому модель безпеки – тріади CIA (confidentiality, integrity, availability) в трьох сферах (профілях) безпеки: інформаційної безпеки, безпеки інформації та кібернетичної безпеки на прикладі автоматизованої банківської системи з використання м в якості інформаційних ресурсів – банківську інформацію.

У даній моделі під інформаційною безпекою розуміється процес забезпечення конфіденційності, цілісності та доступності інформації клієнтами / клієнтом банку на основі сукупності колективної та індивідуальної свідомості. Під конфіденційністю розуміється забезпечення доступу до інформації тільки авторизованим користувачам, під цілісністю – забезпечення достовірності та повноти інформації, і методів її обробки для авторизованих користувачів, під доступністю – забезпечення доступу до інформації та пов'язаних з нею активів авторизованих користувачів в міру необхідності.

Безпека інформації – стан захищеності даних, при якому забезпечуються їх конфіденційність, доступність і цілісність; визначається відсутністю неприпустимого ризику, пов’язаного з витоком інформації технічними каналами, несанкціонованими і ненавмисними діями на дані або на інші ресурси автоматизованої інформаційної системи, що використовуються в автоматизованій системі.

Кібербезпека – набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до управління ризиками, дій, професійної підготовки, страхування і технологій, які використовуються для захисту кіберсереди, ресурсів організацій і користувачів. Кібербезпека передбачає досягнення і збереження властивостей безпеки у ресурсів організації або користувачів, спрямованих проти відповідних кіберзагроз та охоплює такі поняття, як захист

персональної інформації (виявлення, запобігання або реакція на атаки). Стандарт ISO / IEC 27032 до: 2012 Information technology – Security techniques – Guidelines for cybersecurity – дає чітке розуміння зв'язку терміна cybersecurity (кібербезпека) з мережевою безпекою, прикладною безпекою, Інтернет-безпекою та безпекою критичних інформаційних інфраструктури (див. рис. 1.1.) [26].

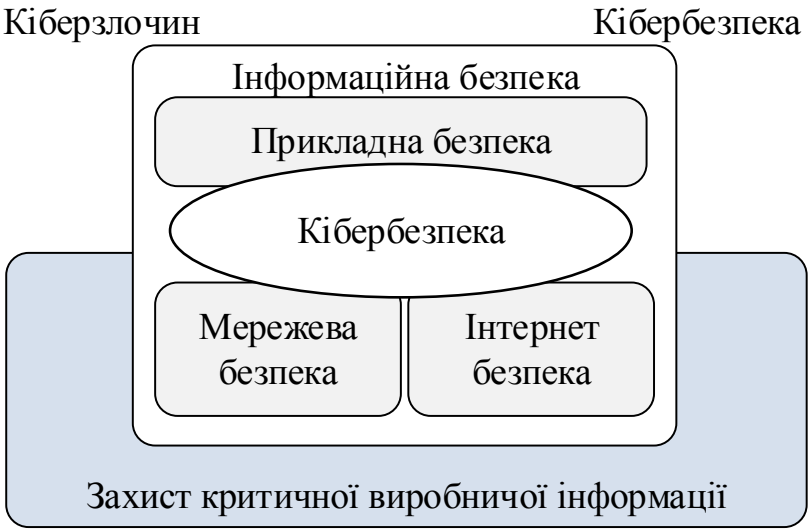


Рисунок 1.1 – Взаємозв'язок між кібербезпекою та іншими доменами безпеки

Отже, відома модель тріади CIA для комплексних АБС може бути представлена у вигляді, представленому на рис. 1.2.

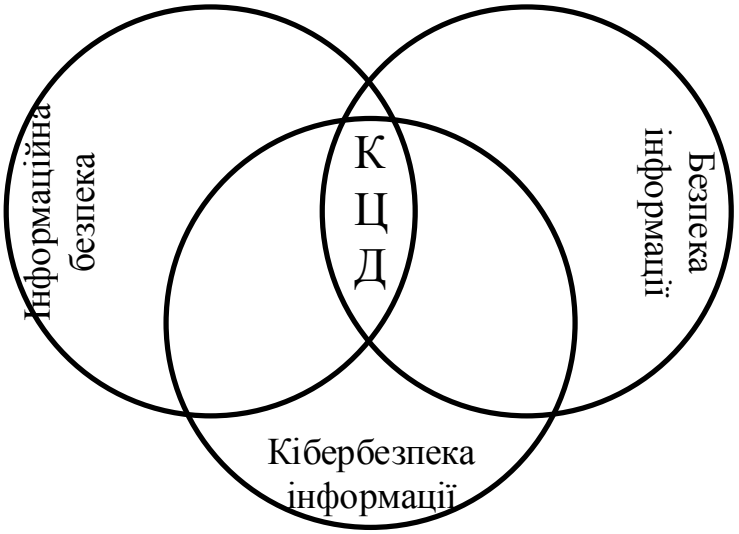


Рисунок 1.2 – Модель тріади CIA для комплексних АБС

Незважаючи на широке застосування різних криптографічних алгоритмів на різних рівнях захисту АБС схильна до різних загроз, загальна класифікація яких приведена у трьох сферах безпеки на рис. 1.3.

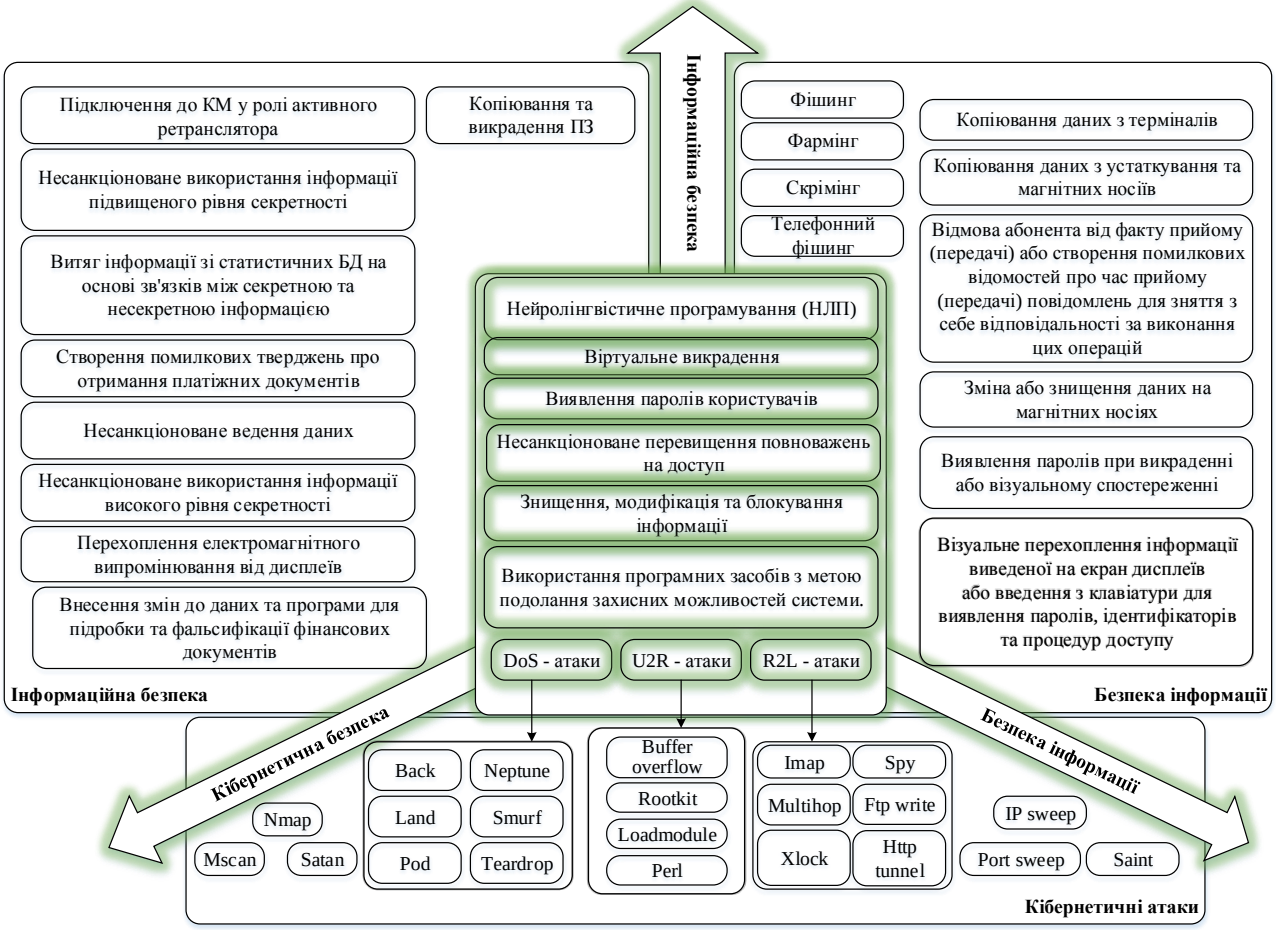


Рисунок 1.3 – Загальна класифікація загроз АБС

Загрози банку – потенційно можливі або реальні дії зловмисників або конкурентів, здатні завдати банку матеріальної чи моральної шкоди [6, 10, 24].

За походженням джерел загрози: внутрішні та зовнішні. Як перші, так і другі за спрямованістю та характером впливу на діяльність банків можуть бути економічними, фізичними, інтелектуальними.

Економічні загрози: корупція, шахрайство, несумлінна конкуренція, використання банками неефективних технологій банківського виробництва. Реалізація таких загроз веде до заподіяння збитків банкам або упущення ними вигоди.

Фізичні загрози: крадіжки, грабежі майна і коштів банків, поломки, виведення з ладу обладнання банків, неефективна його експлуатація. При реалізації таких загроз завдаються збитки банкам, пов'язані з втратою своєї власності і необхідністю нести додаткові витрати на відновлення засобів виробництва та інших матеріальних засобів.

Інтелектуальні загрози: розголошення або неправомірне використання банківської інформації, дискредитація банку на ринку банківських послуг, різного роду соціальні конфлікти навколо банківських установ або в них самих. Наслідки реалізації: збитки банків, погіршення їх іміджу, соціальна чи психологічна напруженість навколо установи банків або в їх колективах.

Проведений аналіз показав, що одним з найбільш вразливих місць в комплексній АБС є пересилання платіжних та інших повідомлень між банками, між банком і банкоматом, між банком і клієнтом, пов'язане з наступними особливостями:

внутрішні системи організацій відправника і одержувача повинні бути пристосовані для відправки та отримання електронних документів і забезпечувати необхідний захист при їх обробці в межах організації (захист кінцевих систем);

взаємодія відправника і одержувача електронного документа здійснюється опосередковано через канал зв’язку.

Ці особливості породжують наступні проблеми:

взаємне розпізнавання абонентів (проблема встановлення взаємної автентичності при встановленні з’єднання);

захист електронних документів, переданих по каналах зв’язку (проблеми забезпечення конфіденційності і цілісності документів);

захист процесу обміну електронними документами (проблема доказу відправлення і доставки документа);

забезпечення виконання документа (проблема взаємної недовіри між відправником і отримувачем через їх приналежність до різних організацій і взаємної незалежності) [3, 29].

Результати досліджень компанії “Arbor Networks” (червень 2015) атак на комп'ютерні мережі наведені на рис. 1.4.

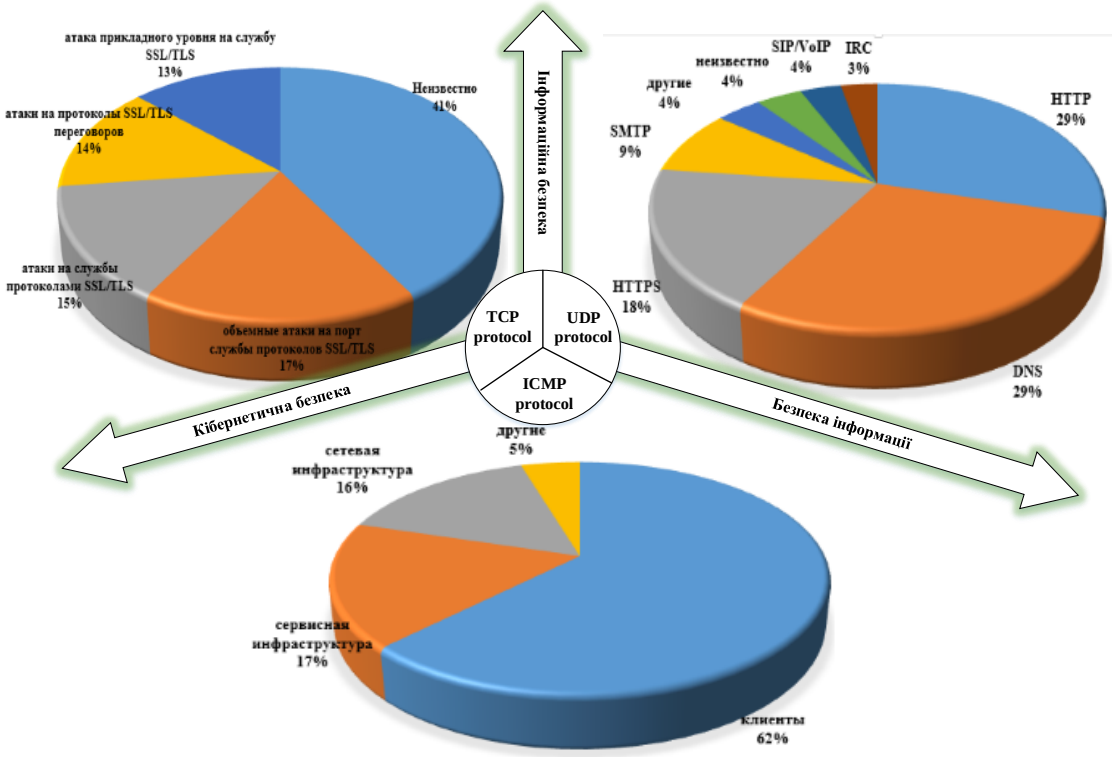


Рисунок 1.4 – Дослідження загроз на протоколи IP-мереж

З ростом кіберзлочинності і обчислювальних можливостей зловмисників спостерігається подальше вдосконалення відомих кібератак і поява нових. Основна класифікація кібератак представлена у вигляді схеми на рис. 1.5.

Перелік атак, які застосовуються для проведення вторгнень поділяються на 4 категорії, кожна з яких містить множину типів атак, що реалізують мету вторгнення. В свою чергу, кожен тип атаки несе загрозу мережі на відповідних рівнях мережевої моделі OSI та виконує свою функцію, щодо здійснення деструктивного впливу на мережу [4, 10, 13, 21, 24, 29]. До вказаних категорій атак відносять:

DoS атаки – це мережеві атаки на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, спрямовані на виникнення ситуацій, коли відбувається відмова в обслуговуванні. Атаки характеризуються заповненням системи великою кількістю з’єднань, зловживанням ресурсами системи, появою помилок, пов’язаних зі зміною параметрів конфігурації

системи, що призводить до перенавантаження та блокування сервера комп'ютерної системи.

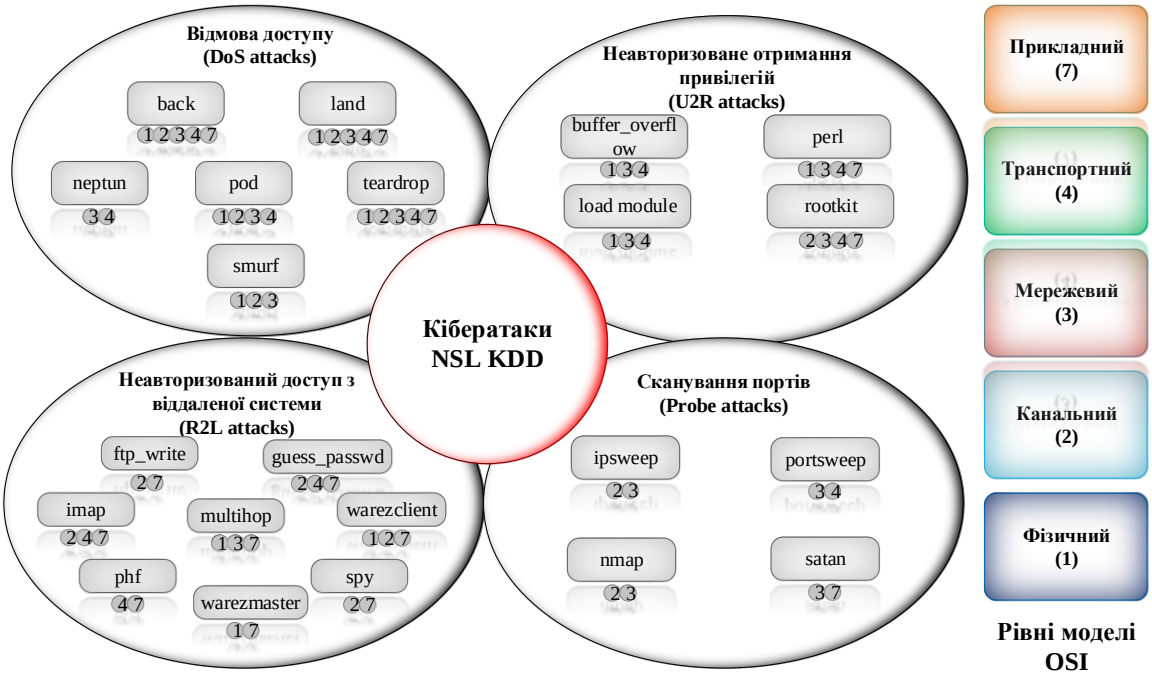


Рисунок 1.5 – Класифікація кібератак

Якщо атака відбувається одночасно з великої кількості IP-адрес, то її називають розподіленою (англ. Distributed Denial-of-Service —DDoS).

U2R атаки – зловмисник здійснює доступ до облікового запису звичайного користувача і, використовуючи уразливість системи, отримує несанкціонований доступ до кореневого каталогу.

R2L атаки, що характеризуються отриманням доступу незареєстрованого користувача до мережі з боку віддаленої станції.

Probe-атаки – полягають в скануванні мережевих портів з метою отримання конфіденційної інформації.

Вказані типи атак за своєю функцією можуть впливати на: управління передачею даних, обмін пакетами, організацію з'єднань, міжмережевий обмін, енергетичні характеристики засобів зв'язку, доступ до кодування, управління інформацією та інше. Виходячи з цього, вплив атак можна розподілити за рівнями мережевої моделі OSI (табл. 1.1.)

Таблиця 1.1 – Вплив атак на рівнях мережевої моделі OSI

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 рівень моделі OSI обслуговує певний набір мережевих протоколів (табл. 1.2):

Таблиця 1.2 – Мережеві протоколи різних рівнів моделі 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 і надійне з'єднання "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,perl load_module, rootkit, neptun, port_sweep	Атака SYN-пакетами (SYN Flood), атака ICMP-запитами зі зміненими адресами (Smurf Attack)

Продовження таблиці 1.2

Рівень	Протоколи	Атаки	Приклад
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 ICMP-запитами (ICMP Flooding)
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 (Dummy Packet Attack)

Таким чином, проведений аналіз підтверджує пропорційне зростання кібератак з еволюційним зростанням обчислювальної техніки і комп'ютерною грамотністю зловмисників в останні десятиліття.

1.2 Аналіз методів виявлення аномалій і зловживань

У процесі аналізу ризиків інформаційної безпеки можуть використовуватися спеціалізовані програмні комплекси, що дозволяють автоматизувати процес аналізу вихідних даних і розрахунку значень ризиків. Прикладами таких комплексів є “Гриф” і “Кондор” (компанії "Digital Security"), британський CRAMM (компанія Insight Consulting, підрозділ Siemens), американський RiskWatch (компанія RiskWatch), а також “Авангард” (Інституту Системного Аналізу РАН). Основою безпечної IT-інфраструктури АБС є тріада сервісів – конфіденційність, цілісність, доступність – Confidentiality, Integrity, Availability (CIA). Метою інформаційної безпеки є забезпечення трьох найбільш важливих сервісів безпеки, відповідно моделі безпеки інформації включають: конфіденційність, цілісність і доступність.

На рис. 1.6. наведені відомі моделі аналізу ризиків інформаційної безпеки.

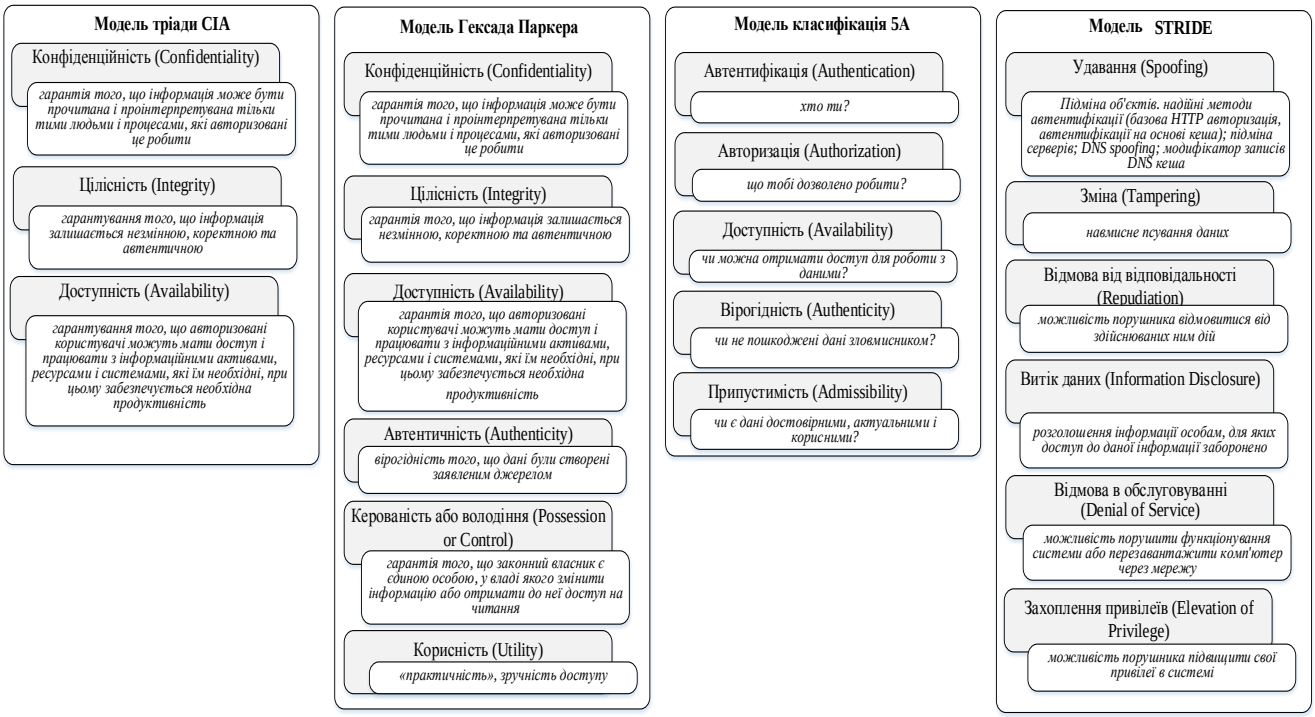


Рисунок 1.6 – Відомі моделі аналізу ризиків інформаційної безпеки

Проведений аналіз відомих моделей аналізу ризиків інформаційної безпеки показав, що основу їх складає модель тріади CIA, однак розгляд послуг безпеки забезпечує сферу інформаційної безпеки і не дозволяє комплексно оцінити сфери безпеки інформації та кібербезпеки АБС в режимі реального часу.

Основою управління інформаційною безпекою АБС є аналіз ризиків. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно існуючі засоби захисту здатні протистояти інформаційним атакам.

Зазвичай виділяють дві основні групи методів розрахунку ризиків безпеки. Перша група дозволяє встановити рівень ризику шляхом оцінки ступеня відповідності визначеному набору вимог щодо забезпечення інформаційної безпеки. Друга група методик оцінки ризиків інформаційної безпеки базується на визначенні ймовірності реалізації атак, а також рівнів їх шкоди. Значення шкоди визначається власником інформаційного ресурсу, а ймовірність атаки обчислюється групою експертів, які проводять процедуру аудиту.

Метод виявлення атак є одним із головних критеріїв оцінки СЗІ. Основна класифікація методів представлена у вигляді схеми на рис. 1.7.

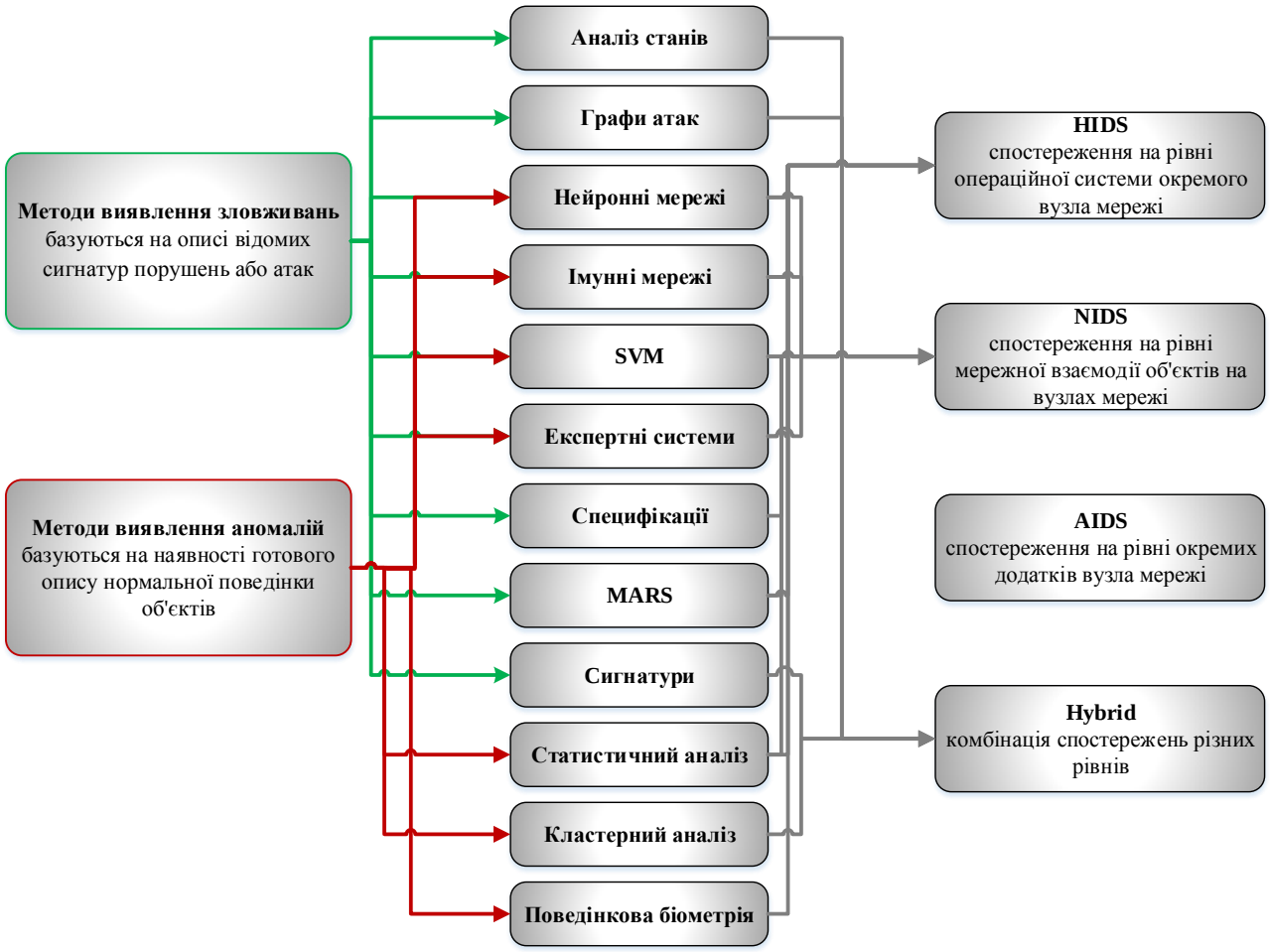


Рисунок 1.7 – Класифікація методів виявлення аномалій та зловживань

Основні характеристики методів представлені в табл. 1.3.

Таблиця 1.3 – Методи виявлення аномалій і зловживань

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

Продовження таблиці 1.3

1	2	3	4	5	6	7
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
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

Закінчення таблиці 1.3

1	2	3	4	5	6	7
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	Р
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	Р
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	Р
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	Р

Проведений аналіз систем виявлення аномалій (СВА) показав, що основним недоліком переважної більшості сучасних комерційних СВА є відносно низька ефективність виявлення невідомих класів кібератак [10 – 12, 21, 26–35]. При цьому більшість сучасних СВА використовують сигнатурні методи виявлення кібератак, що само по собі передбачає організацію процесу захисту з

запізненням. В обох класах виявлення кібератак вхідними даними для роботи системи виступають сформовані на основі множини вхідних параметрів шаблони поведінки – патерни подій. Завдання виявлення кібератаки при такій постановці зводиться до розпізнавання шаблона поведінки системи і фіксації факту її початку. Але, як і в першому, так і в другому випадках безліч вхідних параметрів підлягає оцінюванню на предмет їх інформативності. Відомо, що нині основним способом формування множин інформативних параметрів для СЗІ є евристичний підхід, але одними з головних його недоліків при цьому залишаються неформалізовані і суб'єктивні процедури відбору інформативних параметрів.

1.3 Аналіз методик оцінки ризиків

Систематизувавши відомі підходи до оцінювання інформативності параметрів, наведемо їх у вигляді схеми (рис. 1.8).

Рисунок 1.8 – Оцінювання інформативності параметрів

Процедура вибору одного з наведених вище підходів та адаптація його до формування множини інформативних параметрів для СЗІ повинна спиратися на один або кілька критеріїв якості [19, 28]. Для порівняння відомих підходів між собою оберемо такі критерії якості: ступінь математичного обґрунтування підходу (Крит. 1); відносна складність реалізації підходу (Крит. 2); відносна швидкість процедур оцінювання інформативності параметрів (Крит. 3); якість параметрів, інформативність яких підлягає оцінюванню (Крит. 4). Спираючись на лінгвістичні оцінки приведені в [7] за визначеними вище критеріями, подано їх у вигляді стовпчастої діаграми (рис. 1.9).

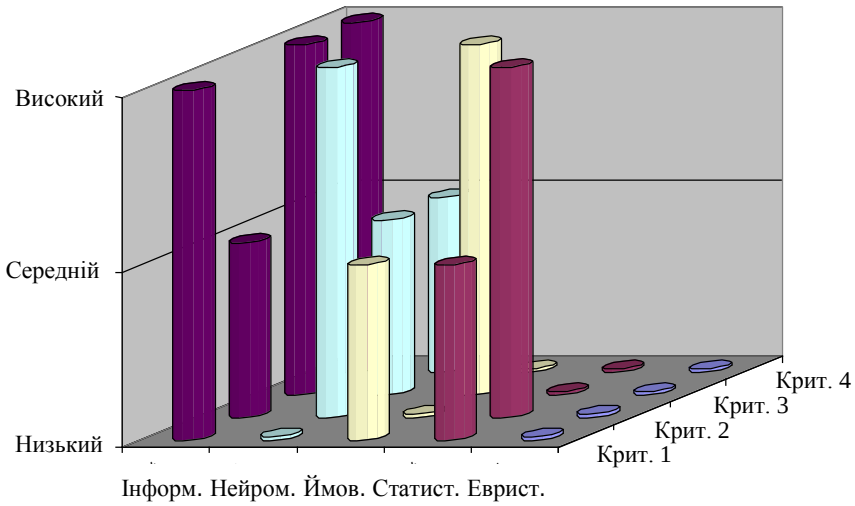


Рисунок 1.9 – Діаграма розподілу критеріїв якості залежно від обраного підходу до оцінювання інформативності параметрів

Спираючись на проведений аналіз [8, 9, 12–15, 17,18] в табл. 1.4 подано результати порівняння ефективності досліджуваних підходів у вигляді узагальненої таблиці.

Таблиця 1.4 – Узагальнені дані за результатами оцінювання ефективності досліджуваних підходів

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

Аналіз одержаних результатів (див. табл. 1.4) дозволяє зробити висновок: інформаційний підхід за усіх рівних початкових умов є найефективнішим серед досліджених підходів й може бути застосований для формування множини інформативних параметрів для систем захисту інформації.

Оцінка рівня ризиків інформаційної безпеки є найбільш складним і відповідальним моментом, оскільки саме від її результатів залежать подальші дії організації.

Метод оцінки ризиків – систематизована сукупність кроків, дій, що дає змогу провести оцінку ризиків. Всі методи оцінки ризику можна розділити на кількісні, якісні або комбінацію кількісних методів з якісними (змішаний).

Кількісні методи використовують вимірні, об'єктивні дані для визначення вартості активів, імовірність втрати і пов'язаних з ними ризиків.

Якісні методи використовують відносний показник ризику або вартості активу на основі рейтингу або поділ на категорії, такі як низький, середній, високий, не важливо, важливо, дуже важливо, чи за шкалою від 1 до 10.

Комбінація кількісного і якісного методу являє собою змішану сукупність переваг і недоліків вище згаданих методів.

З огляду різної природи загроз до профілів забезпечення банківської системи, розглянемо деякі методики оцінки ризиків (табл. 1.5).

Таблиця 1.5 – Методики 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

Закінчення таблиці 1.5

1	2	3	4
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
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

У табл. 1.6 наведені результати досліджень деяких методик оцінки ризиків.

В інтересах отримання в подальшому оцінок величини ризику еквівалентного грошового капіталу, та безпосереднього відображення її захищеності пропонується використовувати методики, засновані на комплексному підході до оцінки ризиків, що поєднує кількісні та якісні методи аналізу, до таких відносяться методики CRAMM і FAIR, структурні схеми представлені на рис. 1.10., рис. 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			+/-	+

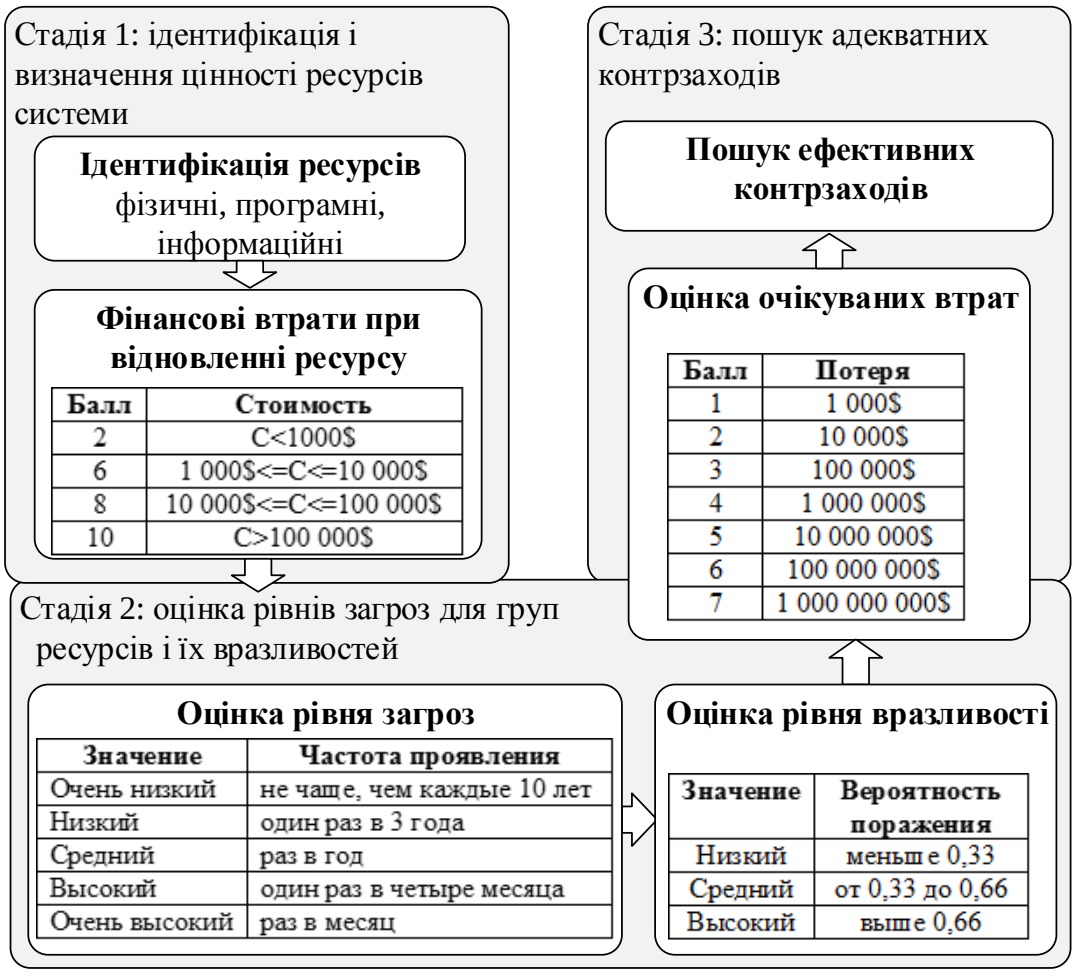


Рисунок 1.10 – Методика CRAMM – комплексний підхід до оцінки ризиків

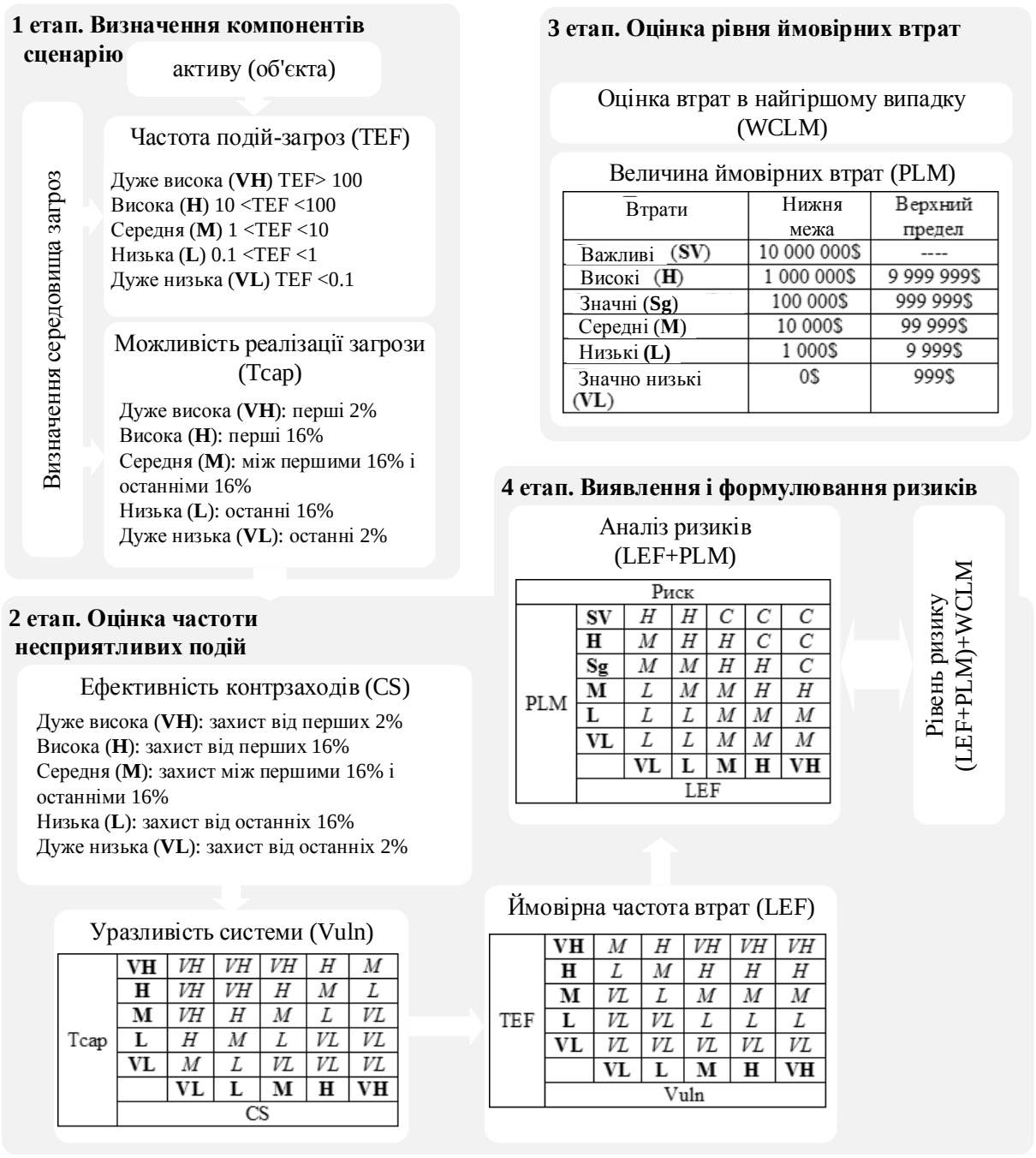


Рисунок 1.11 – Методика FAIR

Методики комплексного підходу оцінки ризиків, як правило, використовують такі стадії (етапи) [20, 21]:

- на першій стадії аналізується все, що стосується ідентифікації та визначення цінності ресурсів системи: визначення меж досліджуваної системи: відомості про конфігурацію системи, відомості про відповідальних особах за фізичні і програмні ресурси, визначення кількості користувачів системи, їх привілеїв. Проводиться ідентифікація ресурсів: фізичних, програмних і

інформаційних, що містяться всередині кордонів системи. Будується модель інформаційної системи з позиції ІБ;

- на другій стадії ідентифікуються загрози і оцінюються рівні загроз для груп ресурсів і їх вразливостей, оцінюються залежність призначених для користувача сервісів від певних груп ресурсів і існуючий рівень загроз і вразливостей, обчислюються рівні ризиків і аналізуються результати. Наприкінці стадії замовник отримує ідентифіковані і оцінені рівні ризиків для своєї системи;

- третя стадія дослідження полягає в пошуку адекватних контрзаходів – пошук варіанту системи безпеки, найкращим чином задовольняє вимогам замовника. На цій стадії генерує кілька варіантів заходів протидії, адекватних виявленим ризикам і їх рівнями.

Взаємозв'язок між методами виявлення атак і методиками оцінки ризиків представлено на рис. 1.12.

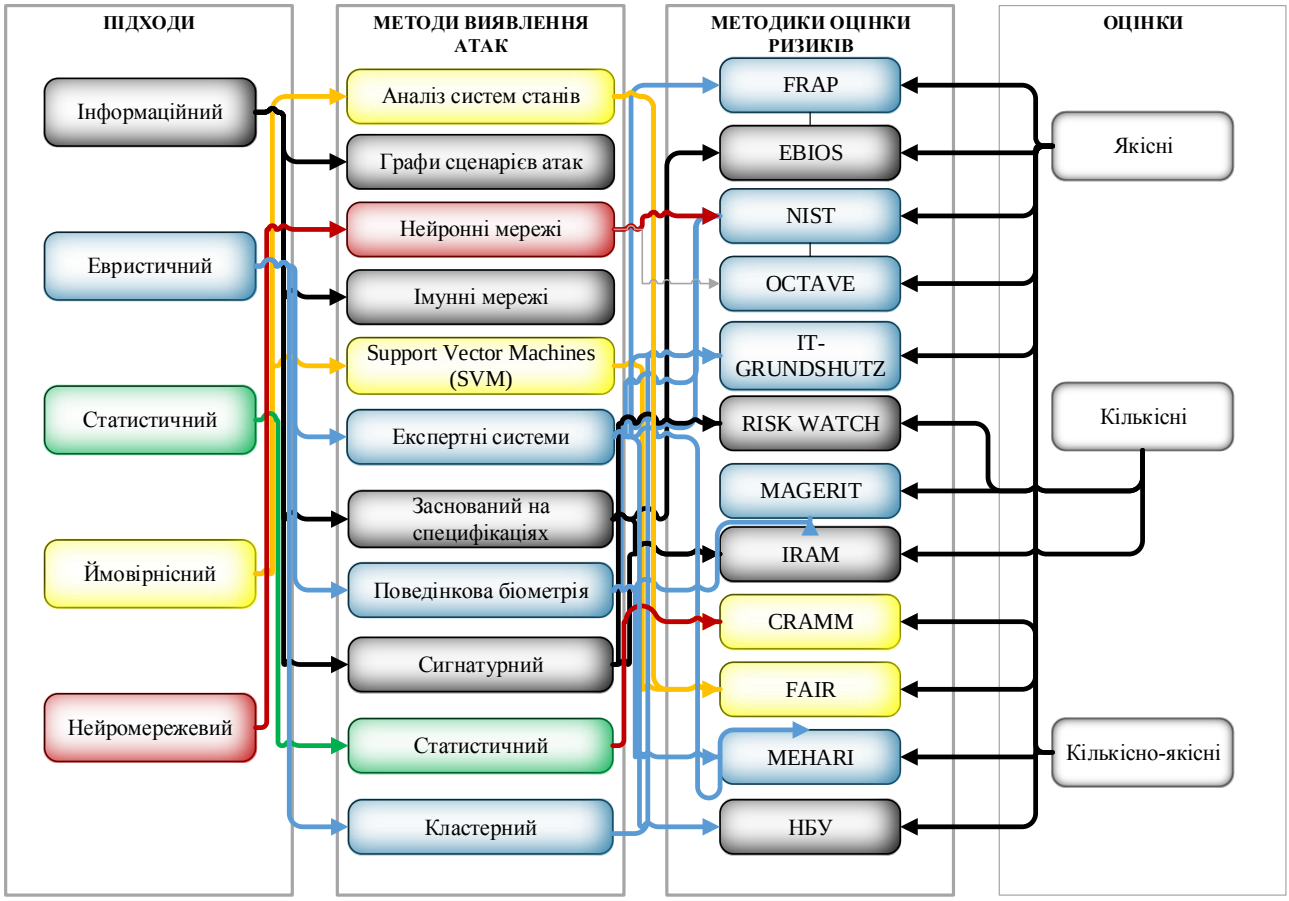


Рисунок 1.12 – Взаємозв'язок між методами виявлення атак та методиками оцінки ризиків

У контексті підвищення ефективності функціонування СВА, незважаючи на переваги та недоліки кожного із напрямків, вони обидва залишаються актуальними, тому інтенсивно розвиваються. Альтернативою є подальший розвиток класифікаторів кібератак у основу яких покладені дерева прийняття рішень, які, за умови правильності їх побудови, дають можливість отримати досить достовірні результати класифікації та мають відносно низьку обчислювальну складність.

Важливу роль в процесі класифікації кібератак грають вхідні дані, які виступають основою для побудови класифікаторів СВА комунікаційних систем та дозволяють отримувати кількісну характеристику кібератак. В якості навчальних і тестових даних доцільним вбачається застосування загальнодоступної і широковідомої бази даних KDD99, що містить приблизно 5 мільйонів, класифікованих за 22 типами, екземплярів атак (класів), визначених 41 ознакою (табл. 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

Закінчення таблиці 1.7

1	2	3
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
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

Усі ознаки інформативно нерівнозначні. Розподіл інформативності про мережеве з'єднання в залежності від ознаки представлено у відсотковому вигляді у табл. 1.8.

Не важко помітити, ознаки, що характеризують мережевий трафік, за своєю структурою є надлишковими.

Таблиця 1.8 – Відсотковий розподіл інформації про мережеве з’єднання згідно ознак

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	

Не важко помітити, ознаки, що характеризують мережевий трафік, за своєю структурою є надлишковими.

Виходячи з цього, сьогодні пропонується використовувати набір даних NSL-KDD, що представляє собою удосконалену версію набору даних KDD99, не містить надлишкових записів, 78 % яких було зафіксовано у KDD99, та пропонує виявляти атаки, використовуючи найбільш впливові 22 ознаки мережевого з’єднання (табл. 1.9).

Таблиця 1.9 – Вирішальні ознаки вектору мережевого з’єднання

№	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

Закінчення 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

Щоб довести доцільність використання набору даних NSL-KDD було експериментально досліджено процент виявлення атак різних категорій, результати представлено у табл. 1.10. – 1.12.

Таблиця 1.10 – Результати виявлення 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 виявлення 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 виявлення Probe-атак

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

1.4 Висновки до розділу 1

Важливу роль в процесі класифікації кібератак грають вхідні дані. За основу вхідних тестових даних доцільним вбачається застосування загальнодоступної бази даних NSL-KDD, що не містить надлишкових записів і дає більший відсоток виявлення атак порівняно до KDD – 99. Якість виявлення атак було значно підвищено, за рахунок скорочення ознак мережевого трафіку з 41 до 22, була збільшена швидкодія системи, що є одним із головних факторів успішного функціонування систем захисту інформації.

Для отримання якісної оцінки кібератак та їх подальшої класифікації, пропонується застосувати відому ознакову класифікацію. Такий підхід дозволить розширити простір ознак для опису невідомих класів кібератак.

Комплексування двох якісного та кількісного підходів дозволить об'єднати переваги кожного із них, що надаються ними окремо, та при цьому відкриє можливості отримання необхідних характеристик для ефективної організації систем захисту.

2 ДОСЛІДЖЕННЯ ЗАСОБІВ І МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ДОСТОВІРНОСТІ ІНФОРМАЦІЇ В СЕРЕДОВИЩІ БЕЗПРОВІДНИХ МЕРЕЖ

Для забезпечення інформаційної скритності та достовірності інформації в комп'ютерних мережах та середовище безпровідних мереж, на сьогоднішній день використовуються протоколи SSL, TLS та IPSec.

2.1 Аналіз протоколів забезпечення конфіденційності та цілісності даних

2.1.1. Аналіз протоколу SSL.

Протокол SSL (secure socket layer) забезпечує захист даних між сервісними протоколами (такими як HTTP, NNTP, FTP і т.д.) і транспортними протоколами (TCP/IP) [1, 3]. SSL становить не один протокол, а два рівні протоколів, як показано на рис. 2.1.

<table>
<tr><td>Протокол квантування SSL</td><td>Протокол зміни параметрів шифрування SSL</td><td>Протокол сповіщанняSSL</td><td>HTTP</td></tr>
<tr><td colspan="4">Протокол запису SSL</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

Рисунок 2.1 – Стек протоколів SSL

Протокол SSL пропонує базовий набір засобів захисту, які застосовуються протоколами більш високих рівнів, і забезпечує конфіденційність каналу комунікацій і автентифікацію користувача.

Протокол діалогу SSL має дві основні фази. Перша фаза використовується для встановлення конфіденційного каналу комунікацій. Друга – служить для автентифікації користувача. В дані сесії входять:

- ідентифікаційний номер сесії;

- сертифікати обох сторін;
- параметри алгоритму шифрування, який буде використаний;
- алгоритм стиснення інформації, який буде використовуватися;
- “загальний секрет”, застосований для створення ключів;
- відкритий ключ.

Загальна схема використання протоколу SSL зображена на рис. 2.2.

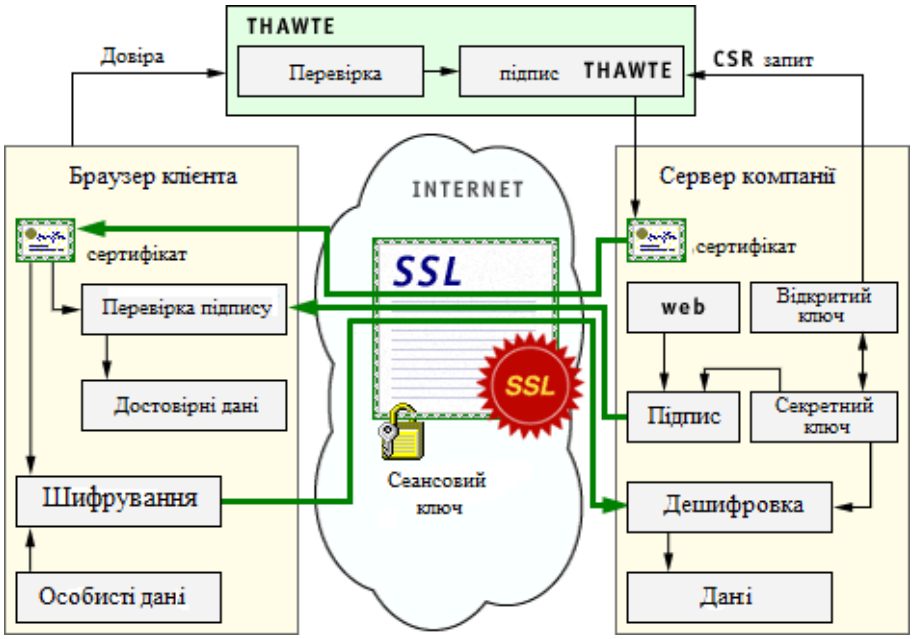


Рисунок 2.2 – Схема використання протоколу SSL

Для забезпечення конфіденційності в протоколі використовуються симетричні протоколи шифрування: 3DES, AES-256 та інш., для забезпечення обміну (розповсюдження) ключовими даними використовуються несиметричні криптосистеми Діффі-Геллмана або RSA.

Для забезпечення цілісності даних в протоколі SSL використовуються алгоритмі гешування за допомогою MAC-алгоритмів або HMAC.

2.1.2. Аналіз протоколу TLS.

Протокол TLS призначений для забезпечення конфіденційності й цілісності даних. Він має два рівні: протокол записів TLS і протокол діалогу TLS. Протокол записів TLS забезпечує конфіденційність даних з використанням симетричних

алгоритмів шифрування DES, RC4 і цілісність даних з використанням геш-функцій SHA-1 або MD5. Протокол діалогу TLS забезпечує цифровий підпис, заснований на підході RSA або DSS. Цей протокол забезпечує безпеку з'єднань, які мають дві основні властивості.

• З'єднання є конфіденційним. Для шифрування даних використовується симетрична криптографія (напр., DES, RC4, і т.д.). Ключі для шифрування генеруються незалежно для кожного з'єднання і базуються на секретному коді, що отримується за допомогою іншого протоколу (такого, як протокол діалогу TLS). Протокол записів може використовуватися і без шифрування.

• З'єднання є надійним. Процедура передачі повідомлення включає в себе перевірку цілісності за допомогою обчислення MAC. Для розрахунку MAC використовуються хеш-функції (напр., SHA, MD5 і т.д.). Протокол записів може працювати і без MAC, але в цьому режимі он застосовується тільки в разі, коли інший протокол використовує протокол записів в якості транспортного при з'ясуванні параметрів безпеки [35]. Але проведений аналіз алгоритмів гешування в [11, 20, 28] показав, що використані в цьому протоколі функції гешування зламані і не в повному обсязі забезпечують криптостійкість.

Структурна схема роботи протоколу TLS зображена на рис. 2.3. Спочатку клієнт ініціалізує обмін повідомленнями. Сервер відсилає свій сертифікат

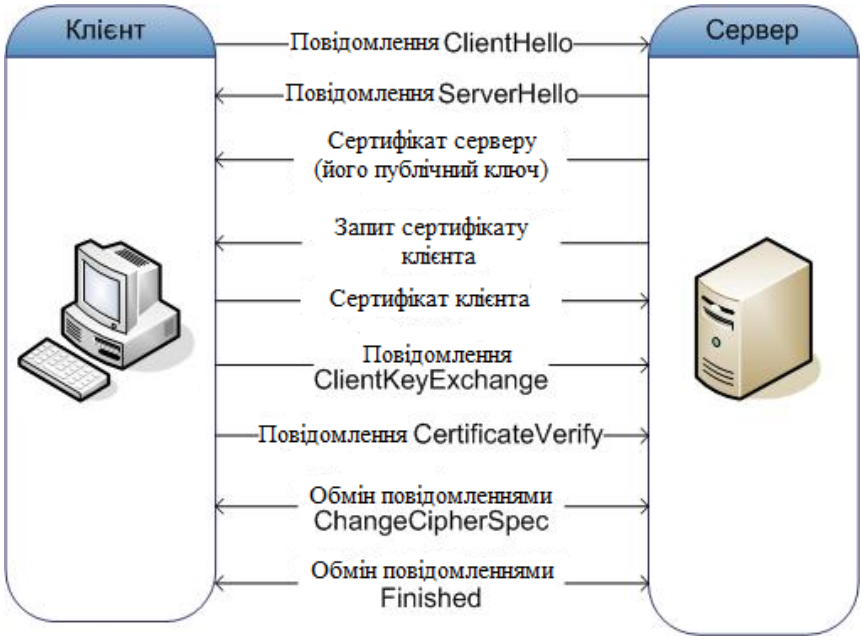


Рисунок 2.3 – Схема роботи протоколу TLS у режимі логічного з’єднання

Основні принципи протоколу TLS є:

1. Криптографічна безпека. TLS повинен застосовуватися для встановлення безпечного з’єднання між двома користувачами мережі.

2. Сумісність. Незалежні програмісти повинні бути здатні розробляти програму для використання TLS, які зможуть успішно обмінюватися криптографічними параметрами без знання особливостей програм один одного.

3. Можливість розширення. TLS забезпечує при необхідності можливість вбудувати в систему нові алгоритмі шифрування..

4. Відносна ефективність. Протокол TLS має опціонну схему кешування сесії, що дозволяє зменшити кількість з’єднань з новими тимчасовими буферами.

В поточній версії протоколу доступні такі алгоритми:

для обміну ключами симетричних алгоритмів використовуються, як і в протоколі SSL алгоритми несиметричної криптографії: RSA, Diffie-Hellman;

для забезпечення конфіденційності використовуються алгоритми традиційної криптографії: RC2, RC4, IDEA, DES, 3DES або AES-256;

для забезпечення цілісності алгоритми гешування: MD5 або SHA-256.

Основними недоліками протоколу є основі зауваження, як і до попереднього протоколу SSL – низький рівень криптостійкості MAC-кодів, які формують відповідні функції гешування в умовах постквантової криптографії.

2.1.3. Аналіз протоколу IPSec

IPsec становить набір протоколів для забезпечення безпеки мережного з’єднання. Протоколи IPsec розроблені IETF (Internet Engineering Task Force). IPsec як служба прозора для користувачів і, як правило, немає необхідності адаптувати для роботи з IPsec уже існуючі програмні застосунки. Протокол IPsec надає три види послуг: автентифікацію (AH), конфіденційність (ESP) і обмін (розподілення) ключів між користувачами системи двох протоколів AH та ESP. Для забезпечення послуг автентичності і конфіденційності як правило формується захищений приватний канал – VPN (Virtual Private Network), який дозволяє забезпечити шифрування інформаційного потоку даних між користувачами.

Загальна схема перетворення даних в IPsec в тунельному режимі наведена на рис. 2.4.

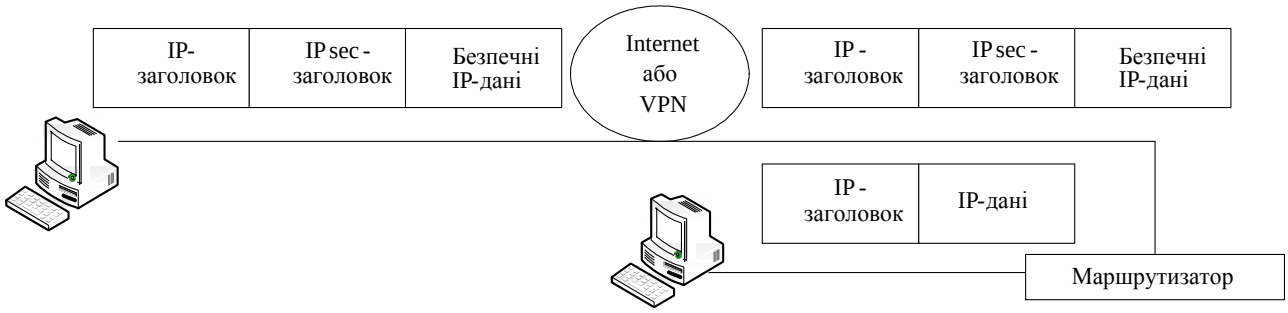


Рисунок 2.4 – Загальна схема перетворення даних в IPsec

Заголовок автентифікації (AH) і Encapsulating Security Payload (ESP) є двома протоколами нижнього рівня, які застосовуються IPsec, саме вони здійснюють автентифікацію й шифрування + автентифікацію даних, переданих через з'єднання. Ці механізми зазвичай використовуються незалежно, хоча можливо (але не типове) їх спільне застосування. IPSec може функціонувати в двох режимах: транспортному і тунельному.

Транспортний режим забезпечує безпечне з'єднання двох терміналів шляхом інкапсуляції вмісту IP-даних, у той час як тунельний режим інкапсулює увесь IP-пакет на ділянці між шлюзами. Останній варіант використовується для формування традиційної VPN, де тунель створює безпечний шлях через повний небезпек Інтернет. Встановлення IPsec-з'єднання має на увазі будь-які варіанти криптоалгоритмів, але ситуація суттєво спрощується завдяки тому, що звичайно припустиме застосування двох, максимум трьох варіантів.

На фазі автентифікації обчислюється контрольна сума ICV (Integrity Check Value) пакета із залученням алгоритмів MD5 або SHA-1. При цьому передбачається, що обидва партнери знають секретний ключ, який

дозволяє одержувачу обчислити ICV і зрівняти з результатом, присланим відправником. Якщо порівняння ICV пройшло успішно, вважається, що відправник пакета автентифікований. Протокол AH завжди здійснює автентифікацію, а ESP виконує її опційно.

Шифрування використовує секретний ключ для кодування даних перед їх транспортуванням, що виключає доступ до вмісту з боку противників. В системі IPsec можуть застосовуватися наступні алгоритми: DES, 3DES, Blowfish, CAST, IDEA, RC5 і AES. Але дозволені й інші алгоритми. Місця розміщення додаткової інформації, що вставляється протоколами в пакет, представлені на рис. 2.5.

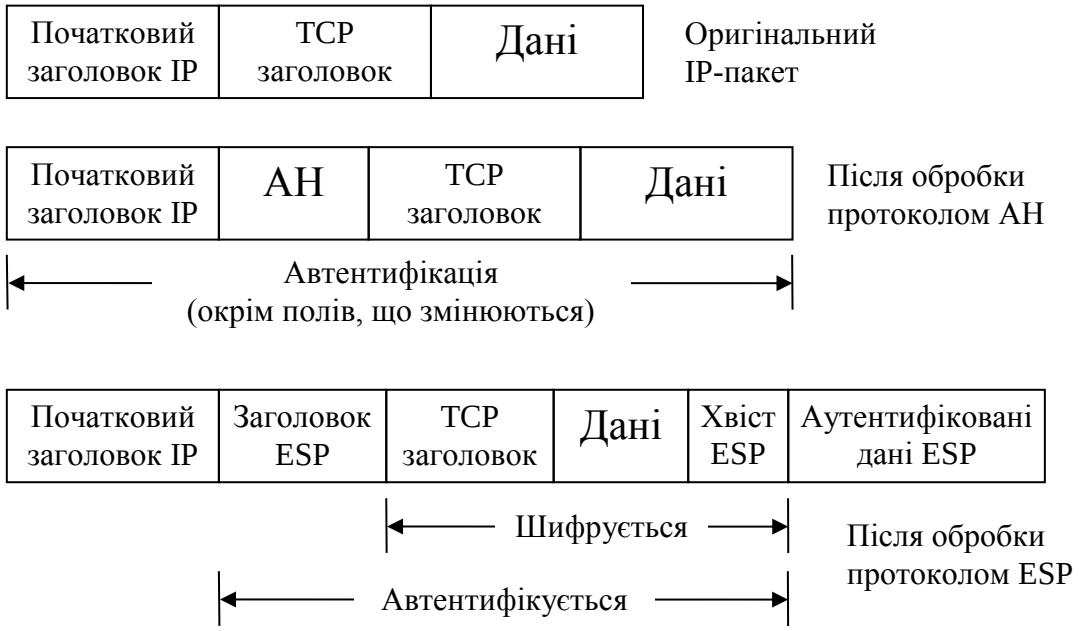


Рисунок 2.5 – Транспортний режим протоколу IPSec

Тунельний режим може використовуватися для підключення віддалених комп’ютерів до VPN-мережі або для організації безпечної передачі даних через відкриті канали зв’язку (наприклад, Інтернет) між шлюзами для об’єднання різних частин віртуальної приватної мережі.

Згідно з рис. 2.6 видно переваги і недоліки обох протоколів. ESP забезпечує приховування даних, але не повну автентифікацію всього пакета. AH повністю автентифікує, але не приховує дані. У цьому причина того, що для забезпечення високого рівня безпеки, застосування протоколів поєднується.

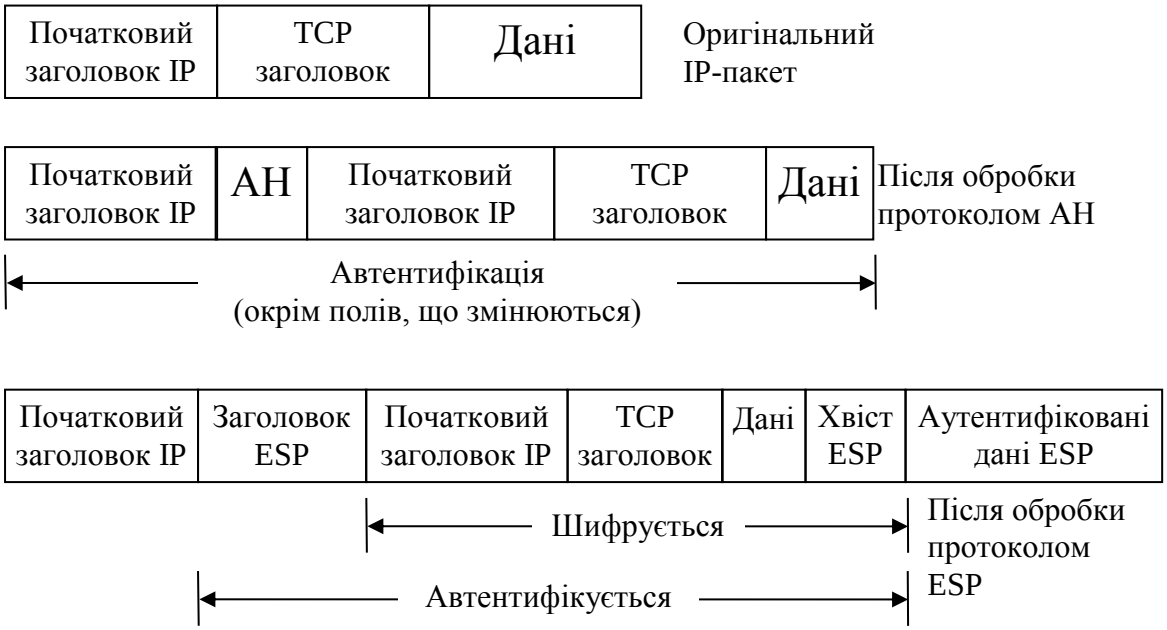


Рисунок 2.6 – Тунельний режим протоколу IPSec

Відповідно, є три схеми застосування IPSec: “хост-хост”, “шлюз-шлюз” і “хост-шлюз” [1, 21, 27, 28, 34, 35]. Розглянемо схеми використання захищеного каналу на основі протоколу IPSec.

Схема “хост-хост” як правило використовує транспортний режим між двома кінцевими вузлами телекомунікаційної мережі (рис. 2.7).

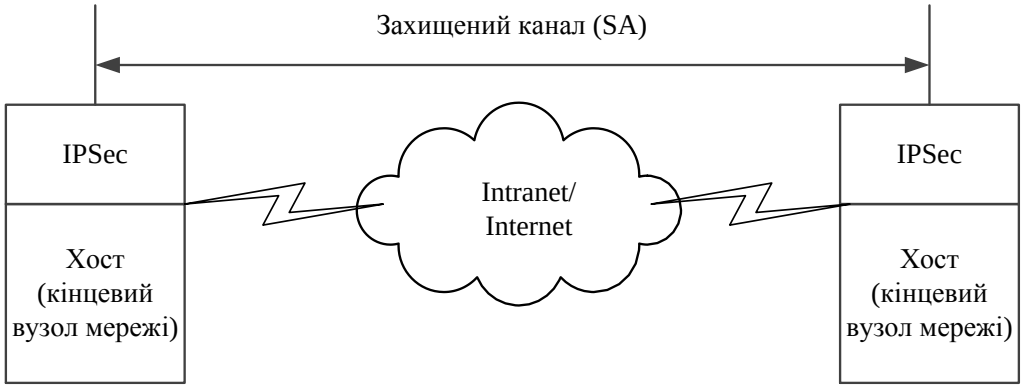


Рисунок 2.7 – Схема організації захищеного каналу “хост-хост”

Схема “шлюз – шлюз” (рис. 2.8) забезпечує в тунельному режимі захищений шлюз (Security Gateway, SG), який дозволяє захищену передачу даних відкритими каналами зв’язку. На відміну від першої схеми в цьому випадку суттєвим недоліком є неможливість корегування маршруту руху інформаційного потоку, т.к. весь пакет шифрується.

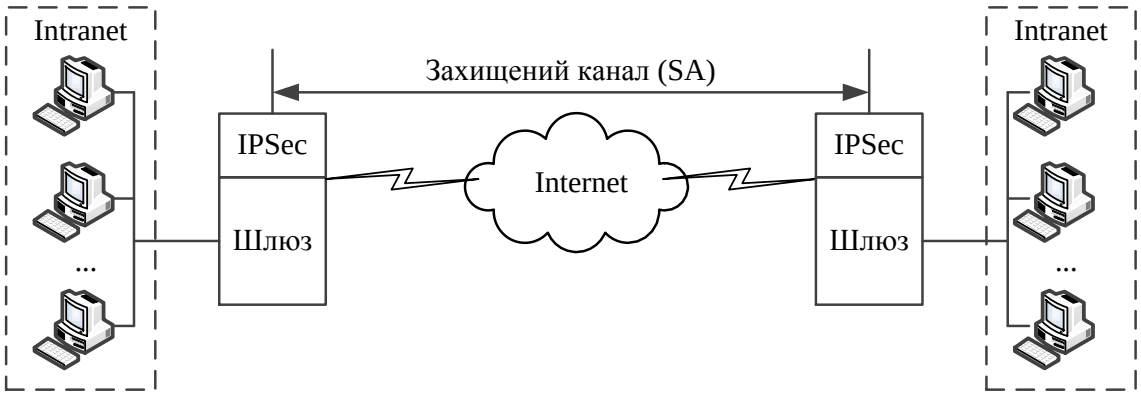


Рисунок 2.8 – Схема організації захищеного каналу “шлюз-шлюз”

Схема “хост-шлюз” (рис. 2.9) часто застосовується при дистанційному доступі.

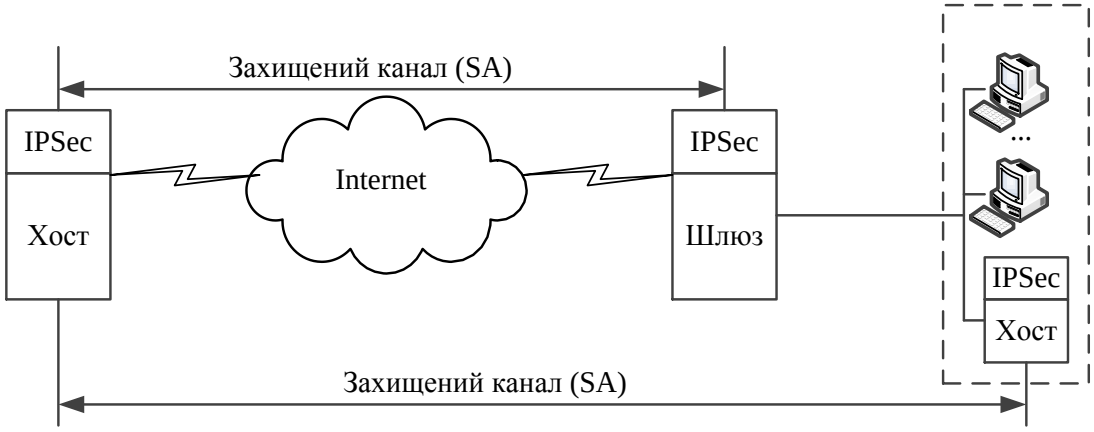


Рисунок 2.9 – Схема організації захищеного каналу “хост-шлюз” з додатковим каналом “хост-хост”

У даному випадку захищений канал формується між віддаленими хостом, на якому працює IPSec, і шлюзом, що захищає трафік для всіх хостів, які входять у мережу Internet організації. Віддалений хост може використовувати при відправленні пакетів шлюзу як у транспортному, так і тунельному режими, шлюз же відправляє пакет хосту тільки в тунельному режимі. Цю схему можна ускладнити, створивши паралельно ще один захищений канал – між віддаленим хостом і яким-небудь хостом, що належать внутрішній мережі, яка захищається шлюзом. Таким чином, комбіноване використання двох SA дозволяє надійно захистити трафік і у внутрішній мережі. Але в умовах постквантової

криптографії використання , і головне забезпечення необхідного рівня безпеки за допомогою IPSec стає неможливим.

2.2 Аналіз забезпечення автентичності на основі протоколу IPSec

2.2.1. Забезпечення цілісності й автентичності даних з використанням протоколу AH (IPSec).

Протокол AH використовується для автентифікації, але не для шифрування IP-трафіка, і служить для підтвердження, що ми зв’язані саме з тим, з ким припускаємо, і що отримані дані не перекручені й не

підмінені при транспортуванні.

Автентифікація виконується шляхом обчислення зашифрованого автентифікаційного геш-коду повідомлення. Гешування охоплює практично всі поля IP-пакета (окрім тільки тих, які можуть модифікуватися при транспортуванні, наприклад, TTL або контрольна сума заголовка). Цей код записується в AH-заголовку й пересилається одержувачу. Формат AH-заголовка поданий на рис. 2.10.

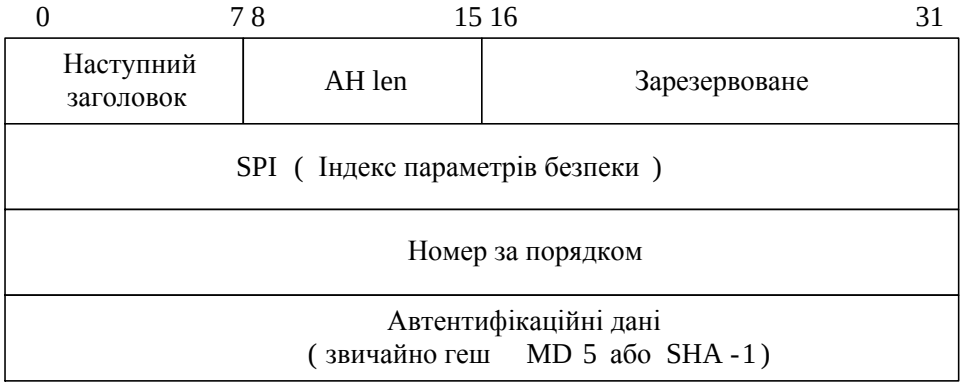


Рисунок 2.10 – Формат заголовка AH

Цей AH-заголовок містить п’ять важливих полів:

Наступний заголовок – ідентифікує тип протоколу, який використовується для наступного поля даних. Фактично це тип пакета, інкапсульованого в AH IPsec.

AH len – визначає довжину заголовка пакета, обмірювану в 32-бітових словах, за винятком двох слів (це диктується RFC 1883 для Ipv6).

Зарезервоване – поле зарезервоване на майбутнє й повинне містити нулі.

Індекс параметрів безпеки (SPI) – 32-бітовий ідентифікатор, який допомагає одержувачу вибрати, до якого із вхідних обмінів відноситься цей пакет. Кожний обмін, захищений AH, використовує геш-алгоритм (MD5, SHA-1 та ін.), якісь секретні та, можливо, деякі інші дані. SPI може розглядатися як індекс таблиці наборів таких параметрів, щоб полегшити вибір потрібного набору.

Номер за порядком – ідентифікатор, що монотонно збільшується, який дозволяє встановити відповідність між посланим пакетом і відгуком підтвердження його одержання. Цей код включається в автентифіковані дані, що дозволяє детектувати будь-які модифікації, а також атаки відтворення.

Автентифікаційні дані – це контрольна сума ICV (Integrity Check Value), обчислена для всього пакета, включаючи більшість полів заголовка.

Протокол AH може використовуватися як у тунельному, так і в транспортному режимах, самостійно й у комбінації із протоколом ESP.

2.2.2. Забезпечення конфіденційності, цілісності й автентичності даних з використанням протоколу ESP (IPSec).

У випадку використання інкапсуляції зашифрованих даних заголовок ESP є останнім у низці опціональних заголовків, “видимих” у пакеті. Формат ESP (рис. 2.11) так само, як і формат AH, може зазнавати значних змін залежно від використовуваних криптографічних алгоритмів.

Проте у форматі ESP можна виділити такі обов’язкові поля: SPI, що вказує на контекст безпеки й Sequence Number Field, що містить послідовний номер пакета. Поле “ESP Authentification Data” (контрольна сума) не є обов’язковим у заголовку ESP. Одержувач пакета ESP розшифровує ESP-заголовок і використовує параметри й дані застосовуваного алгоритму шифрування для декодування інформації транспортного рівня.

Протокол ESP реалізує: шифрування даних IP-пакетів для забезпечення конфіденційності інформації, додатково (аналогічно протоколу AH) автентифікацію джерела кожного пакета, цілісність даних кожного пакета, захист від повторної передачі пакетів.

Заголовок ESP, також як і заголовок AH, збільшує довжину оригінального IP-пакета приблизно на 24 байта (196 біт), основну частину цих додатково внесених надлишкових даних займає код контролю цілісності й автентичності ESP. Для його формування в протоколі ESP передбачене використання спеціальних механізмів контролю цілісності й автентичності даних (аналогічних тем, які використовуються протоколом AH): HMAC-MD5-96, HMAC-SHA-1-96, DES-MAC, HMAC – ГОСТ Р 34.11-94, HMAC – ГОСТ Р 34.11-2001, з можливістю заміни їх на більш ефективні.

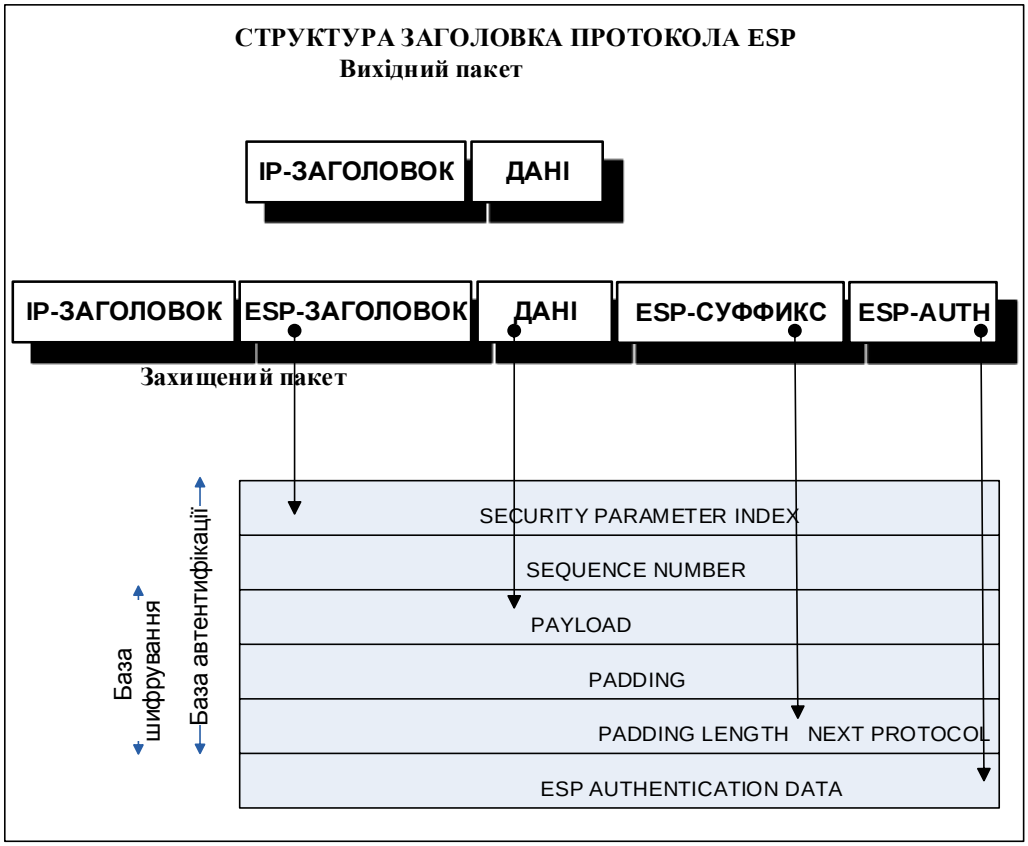


Рисунок 2.11 – Формат заголовка ESP

Для забезпечення конфіденційності даних IP-пакетів дозволяється використання криптографічних алгоритмів шифрування, серед яких передбачені

обов’язкові алгоритми (для забезпечення сумісності програмних продуктів різних виробників), такі, наприклад, як DES-CBC (описаний у стандарті RFC 2405), NULL (описаний у стандарті RFC 2410). Крім того, припускаються і деякі інші (додаткові) алгоритми шифрування, наприклад, CAST-128, IDEA, 3DES (описані у стандарті RFC 2451), а також національний стандарт шифрування США AES-128, 192, 256 (FIPS-197) і вітчизняний стандарт ГОСТ-28147-89. Протокол ESP може застосовуватися як у тунельному, так і в транспортному режимах, самостійно й у комбінації із протоколом AH.

2.2.3. Застосування протоколів AH і ESP у транспортному та тунельному режимах.

Транспортний режим застосовується для захисту віртуальних з’єднань точка-точка. Цей захист здійснюється з використанням автентифікації, шифрування або обох методів.

При транспортному режимі AH IP-пакет модифікується лише злегка шляхом включення AH-заголовка між IP-заголовком і полем даних (TCP, UDP та ін.) і перестановки кодів протоколу.

Перестановка кодів протоколу необхідна для відновлення вихідного виду IP-пакетів кінцевим одержувачем: після виконання перевірки одержувачем коректності IPSec-заголовка цей заголовок віддаляється, а в поле код протоколу IP заноситься колишнє значення (TCP, UDP та ін.).

Коли до адресата приходить пакет, що успішно пройшов процедуру автентифікації, заголовок AH віддаляється, а вміст поля (AH) в IP-заголовку заміняється запам’ятованим значенням поля наступного заголовка. Таким чином, відновлюється первісний вигляд IP-дейтограми і па-кет може бути переданий процесу, що очікує.. Схема проходження IP-пакета даних із застосуванням протоколів безпеки AH і ESP у транспортному режимі наведена на рис. 2.12.

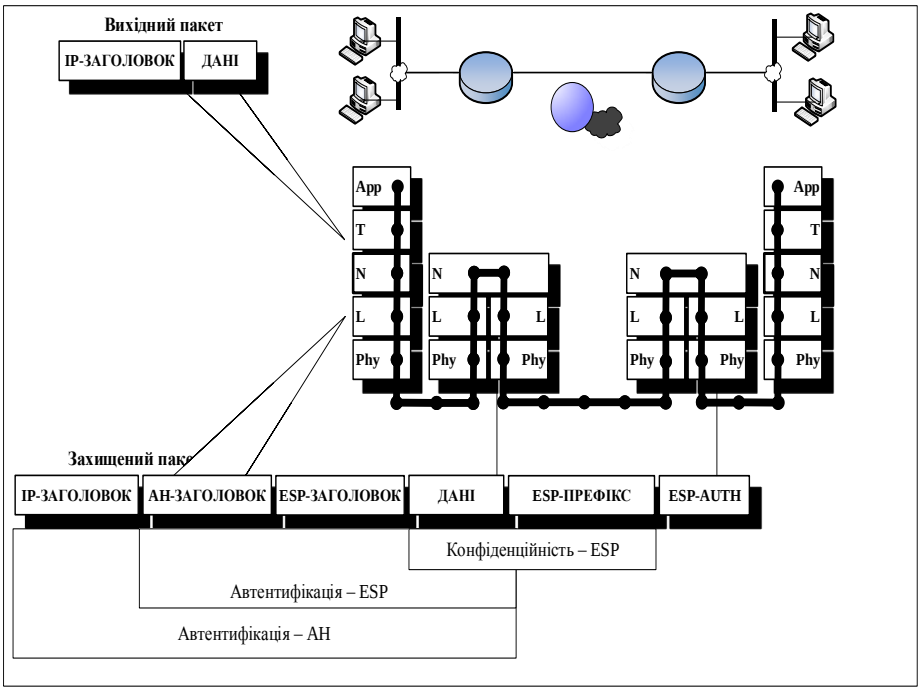


Рисунок 2.12 – Схема проходження IP-пакета даних із використанням протоколів безпеки AH і ESP у транспортному режимі

Прикладом використання транспортного режиму є передача електронної пошти. Усі проміжні вузли на маршруті пакета від відправника до одержувача використовують тільки відкриту інформацію мережного рівня й, можливо, деякі опціональні заголовки пакета (в IPv6). Суттєвим недоліком є можливість моніторингу зловмисником інформаційного потоку.

Тунельний режим (рис. 2.13) реалізує функціональність VPN, де IP-пакет цілком інкапсулює в інший пакет і в такому вигляді доставляється адресату.

Так само, як і в транспортному режимі, пакет захищається контрольною сумою ICV, щоб автентифікувати відправника та запобігти модифікації пакета при транспортуванні. Але, на відміну від транспортного режиму, інкапсулюється весь IP-пакет, що дозволяє адресам відправника й одержувача відрізнятися від адрес, що втримуються в пакеті, це дає можливість формувати тунель.

Але незважаючи на переваги тунельного режиму суттєвим недоліком є можливість отримання зловмисником конфіденційної інформації в проміжних комутаційних засобах підчас формування маршруту.

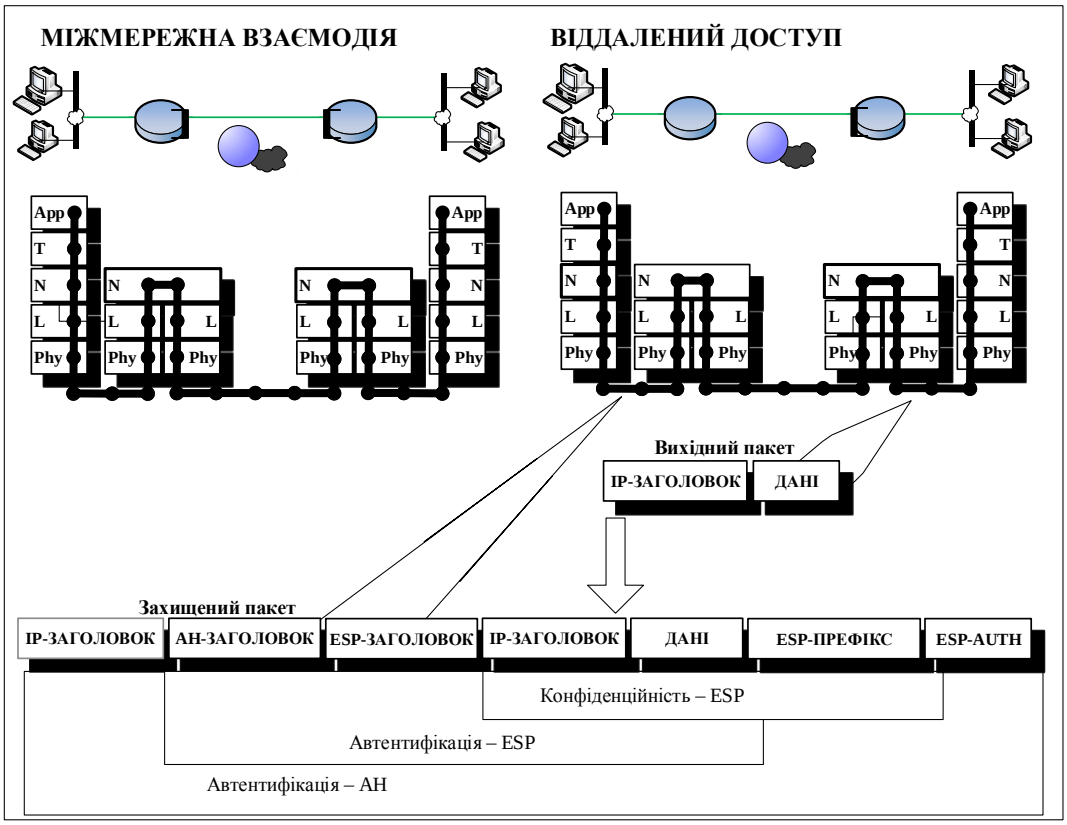


Рисунок 2.13 – Схема проходження IP-пакета даних із використанням протоколів безпеки АН і ESP у тунельному режимі

Коли пакет тунельного режиму приходить адресату, він проходить ту ж автентифікаційну перевірку, що і пакет АН-типу, після чого віддаляються заголовки IP і АН та відновлюється первісний формат пакета.

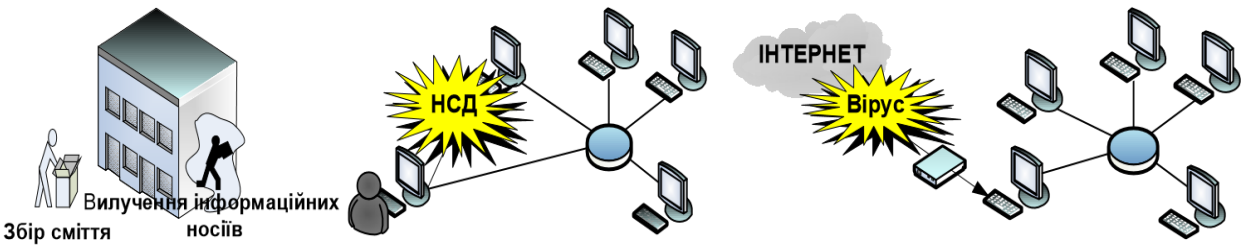
Більшість реалізацій розглядає завершену точку тунелю як мереж-ного інтерфейсу. Реконструйований пакет може бути доставлений локальній машині або маршрутизований ще будь-куди (згідно з місцем призначення IP-адреси в інкапсульованому пакеті). Подальше його транспортування вже не забезпечується засобами безпеки IPSec.

У той час як транспортний режим використовується винятково для забезпечення безпечного зв’язку між двома комп’ютерами, тунельний режим звичайно застосовується між шлюзами (маршрутизаторами, мережними екранами, або окремими VPN-обладнаннями) для побудови VPN (Virtual Private Network). Слід зазначити, що в пакеті IPSec немає спеціального поля “режим”: яке б дозволяло розділити транспортний режим від тунельного, цю функцію виконує поле наступного заголовка пакета АН.

2.3 Ознаковий принцип формування класифікацій кібератак

Спектр кібератак є достатньо різнорідним, тому основним принципом, за яким найбільш ефективно їх класифікувати, буде ознаковий, базовими ознаками з яких є: автоматизація; взаємодія з політикою безпеки ІС; дистанційність; зовнішні прояви; ініціалізаційна умова; інструментальні засоби; наявність зворотного зв'язку; порушення характеристик безпеки; природа взаємодії; реляційні ознаки; дії, породжені НСД; специфіка реалізації; спрямованість результату; ступінь складності; тип базового ресурсу; семирівнева еталонна модель.

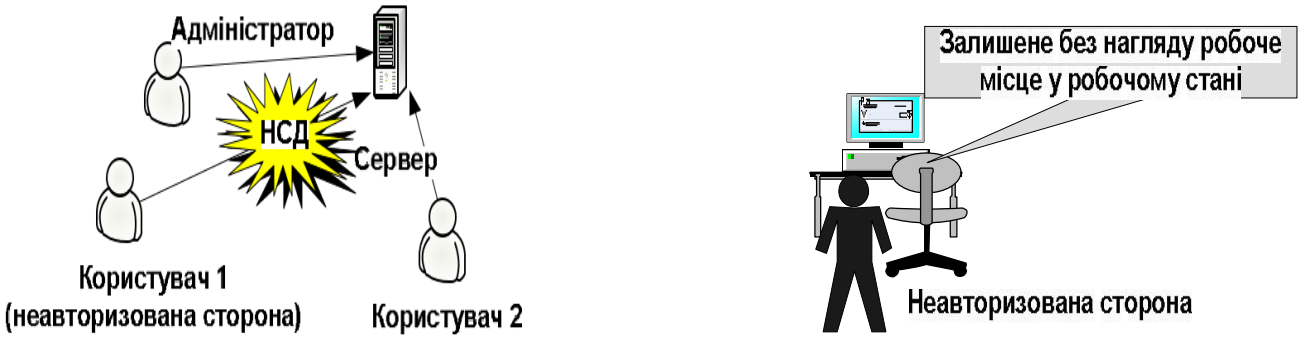
За *автоматизацією* кібератаки можна поділити на мануальні, автоматизовані та автоматичні (вірусні). Мануальні кібератаки (підглядання, збирання сміття, вилучення інформаційних носіїв тощо) реалізуються за прямою участю людини без використання будь-яких спеціальних засобів. На рис. 2.14, а наведено приклад реалізації мануальної кібератаки – збір сміття та вилучення інформаційних носіїв. Автоматизовані кібератаки здійснюються за постійною участю оператора з використанням широкого спектра програмних і апаратних засобів. Приклад автоматизованої кібератаки зображений на рис. 2.14, б, неавторизована сторона реалізовує НСД за допомогою апаратних та програмних засобів на робочу станцію при прямому підключені до мережі. Автоматичні кібератаки реалізуються без участі людини і, як правило, з використанням спеціалізованих програмних засобів, функціонування яких базується на вірусних технологіях. Прикладом автоматичної кібератаки є зараження ресурсів ІС вірусом під час підключення до глобальної мережі Internet без участі людини (рис. 2.14, в).



а б в

Рисунок 2.14 – Приклади кібератак за автоматизацією:
а – мануальна; б – автоматизована; в – автоматична

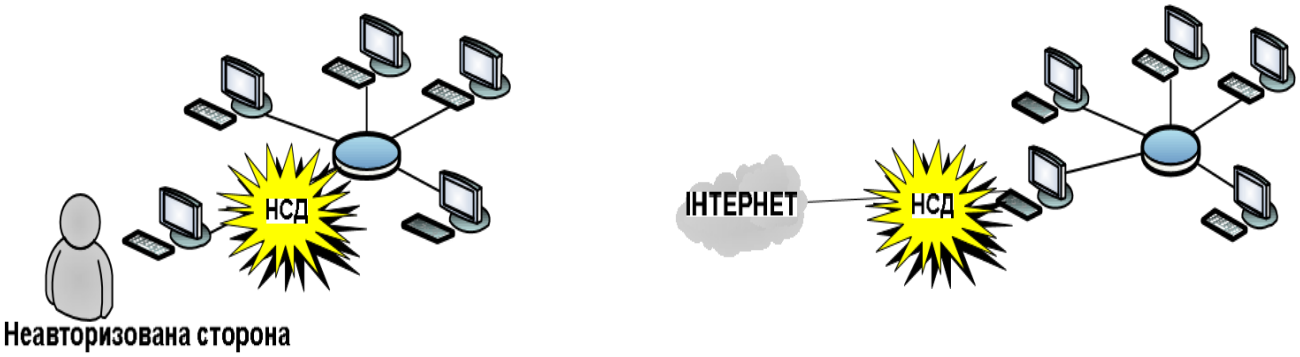
За *взаємодією з політикою безпеки ІС* кібератаки поділяють на постполітизаційні, деполітизаційні. Постполітизаційні кібератаки полягають у використанні недоліків у вже реалізованій політиці безпеки ІС. Такими недоліками можуть бути: невірно побудовані правила розмежування доступу, використання програмних і апаратних засобів з недостатнім рівнем захищеності, прорахунки при блокуванні каналів витоку інформації з обмеженим доступом тощо. Наприклад, якщо користувачу та адміністратору мережі надані однакові права доступу до сервера, то неавторизована сторона, що одержала права доступу Користувача 1, зможе реалізувати кібератаку на інформаційні ресурси ІС на рівні прав адміністратора (рис. 2.15, а). Деполітизаційні кібератаки пов’язані з помилками і недбалістю, які мають місце при реалізації заходів із забезпеченням вже існуючої політики безпеки. Це, в першу чергу, пов’язане з людським чинником і залежить від достатньої адміністративної підтримки, коректності виконання функцій захисту, своєчасного реагування на нештатні ситуації тощо. Наприклад, якщо Користувач залишає своє робоче місце, не дотримуючись політики безпеки (не закінчує сеанс роботи чи не блокує комп’ютер), то неавторизована сторона за час його відсутності має доступ до інформаційних ресурсів ІС через некоректність виконання користувачем функцій захисту (рис. 2.15, б).



а б

Рисунок 2.15 – Приклади кібератак за взаємодією з політикою безпеки ІС: а – постполітизаційна; б – деполітизаційна

За *дистанційністю* кібератаки поділяють на локальні та віддалені. Якщо кібератака на ресурс ІС здійснюється в локалізованій зоні його розташування (локальна обчислювальна мережа, робоча станція, принтер, носій інформації тощо), то вона називається локальною, у протилежному випадку – віддаленою. Наприклад, локальна кібератака може бути реалізована всередині сегмента, при цьому джерело кібератаки і ресурс, що піддався атаці, будуть знаходитись в межах одного сегмента. Приклади реалізацій локальної та віддаленої кібератак зображені на рис. 2.16.

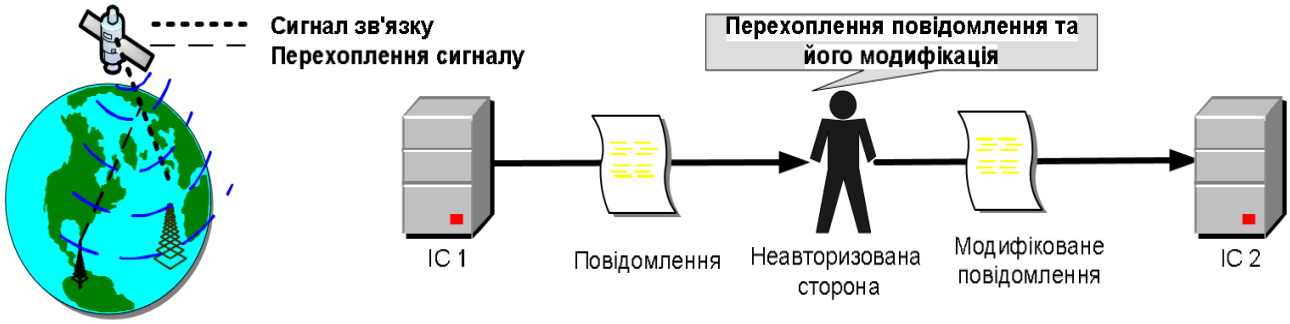


а б

Рисунок 2.16 – Реалізація кібератак за дистанційністю:
а – локальної; б – віддаленої

За *зовнішнім проявом* кібератаки поділяються на пасивні та активні. У результаті пасивної кібератаки не здійснюється безпосередній вплив на ресурси ІС, і можуть не порушуватись їх характеристики безпеки, наприклад, при перехопленні зашифрованих даних. У результаті активної кібератаки здійснюється безпосередній вплив на ресурси ІС і порушуються їхні характеристики безпеки. Практично всі типи віддалених кібератак є активними атаками, особливістю яких, у порівнянні з пасивними атаками, є принципова можливість їх виявлення, тому що в результаті безпосереднього впливу відбуваються певні зміни. На відміну від активних кібератак, пасивні не залишають слідів втручання.

Наприклад, перехоплення супутникового сигналу (рис. 2.17, а) без його модифікації належить до пасивної кібератаки. Перехоплення повідомлення неавторизованою стороною з подальшою його модифікацією (рис. 2.17, б) належить до активних кібератак.



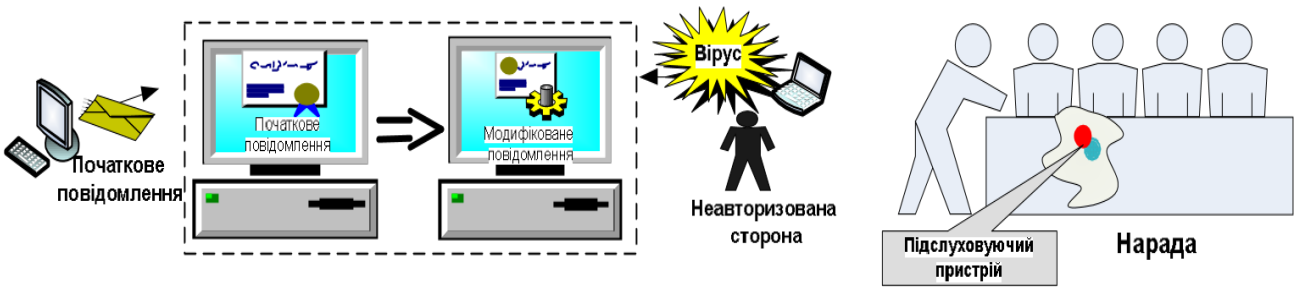
а б

Рисунок 2.17 – Реалізація кібератак за зовнішнім проявом: а – пасивної; б – активної

За *ініціалізаційною умовою* кібератаки поділяються на умовні та безумовні. Умовні ініціалізуються у випадку виникнення певної події (механізм логічної бомби) і в свою чергу можуть поділитися на пасивні і активні. Прикладом ініціалізації пасивної умовної кібератаки може бути передача від потенційної мети запиту певного типу, який і буде умовою початку атаки. У цьому випадку, наприклад, такою умовою можуть бути DNS- і ARP-запити в стеку протоколів TCP/IP. За активної умовної кібератаці здійснюється постійний моніторинг стану окремих ресурсів ІС і при його певній зміні формується сигнал ініціалізації. Прикладом такого стану може бути подія, пов’язана з перериванням сеансу роботи користувача із сервером без стандартної команди, наприклад, LOGOFF. Момент ініціалізації безумовної кібератаки не супроводжується певною зміною стану ресурсів і визначається джерелом кібератаки.

За використовуваними *інструментальними засобами* кібератаки поділяються на програмні, апаратні та нетипові. Програмні кібератаки ґрунтуються на спеціальних мікро- або макрокодованих засобах (наприклад, суперзапінгових утилітах, внутрішніх командах, сценаріях автоматизації тощо),

які функціонують в межах ІС для реалізації своїх функцій. Наприклад, віддалений комп'ютер (рис. 2.18, а) відправляє повідомлення на робочу станцію, до якої несанкціоновано підключається неавторизована сторона за допомогою портативного комп'ютера і реалізує зараження цієї станції вірусом, який модифікує це повідомлення. Апаратні кібератаки засновуються на різноманітних механічних, електричних, електромеханічних, електронних, електронно-механічних та інших пристроях, які використовуються автономно чи в поєднанні з іншою апаратурою для виконання відповідних функцій. Наприклад, в кімнаті для нарад (рис. 2.18, б) може бути встановлений "жучок" для прослуховування конфіденційних розмов. Нетипові кібератаки реалізуються на підґрунті таких засобів, які не належать до апаратних або програмних (наприклад, вибухівка, радіоактивні матеріали, кислоти, комахи, гризуни тощо).

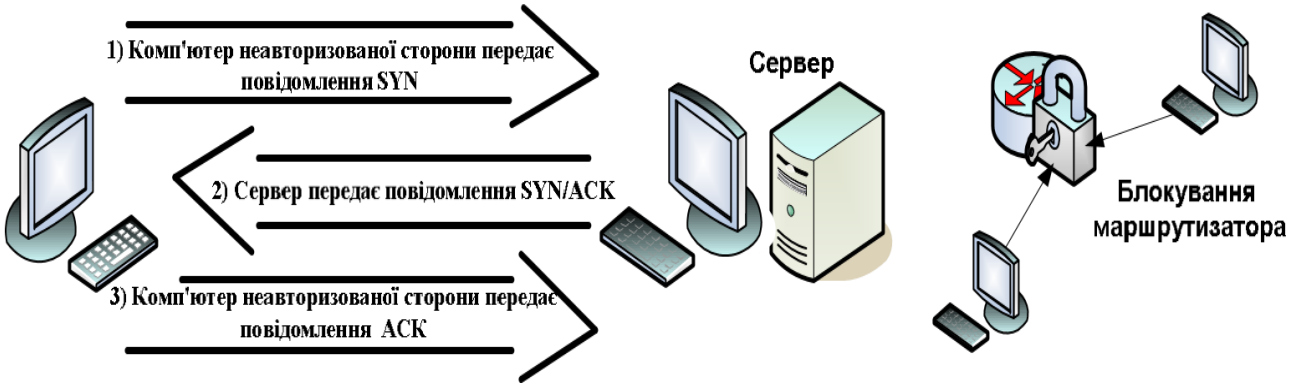


а б

Рисунок 2.18 – Приклади кібератак за інструментальними засобами:
а – програмна; б – апаратна

За *наявністю зворотного зв'язку* з ресурсом ІС, що піддався несанкціонованим діям, кібератаки бувають зі зворотним зв'язком та без нього. У процесі реалізації кібератаки зі зворотним зв'язком здійснюється отримання нею від ресурсу, що піддався несанкціонованим діям, відповіді на свої дії, які необхідні, наприклад, для подальшого продовження зазначеного процесу на більш ефективному рівні, що досягається завдяки аналізу реакцій об'єкта кібератаки на певні зміни. Прикладом атаки зі зворотним зв'язком є сканування портів спеціальним програмним забезпеченням. Під час сканування на порти сервера відправляється пакет синхронізації SYN. Якщо на це повідомлення (рис.

2.19, а) приходить відповідь (зворотний зв’язок) у вигляді пакета SYN/ACK, то це означає, що сканований порт знаходиться у стані очікування і можна виконувати наступну дію. Кібератаки без зворотного зв’язку реалізуються незалежно від реакції ресурсу ІС, що піддався атаці. Найбільш яскравим прикладом є відмова в обслуговуванні. Наприклад, блокування маршрутизатора (рис. 2.19, б), що призводить до відмови в обслуговуванні.



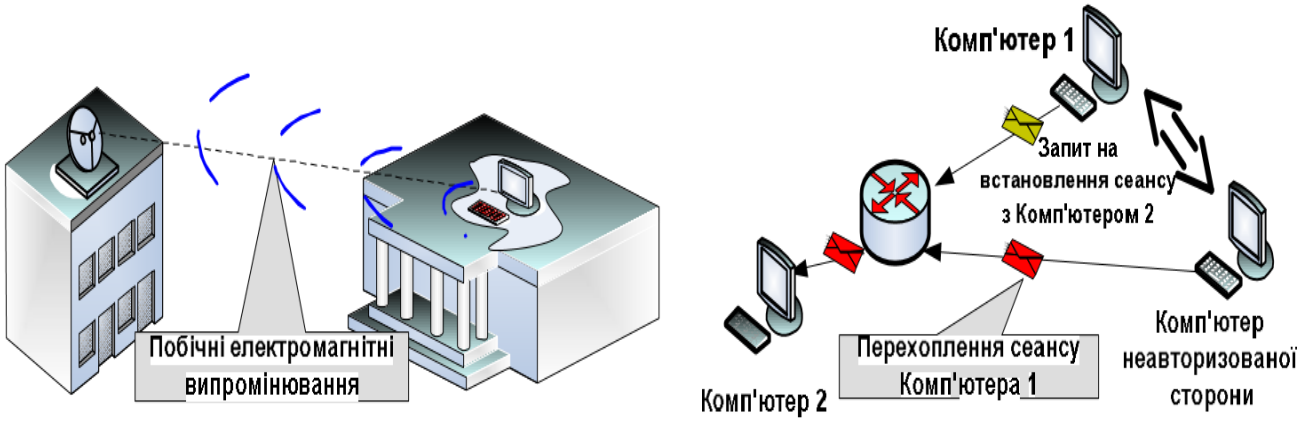
а б

Рисунок 2.19 – Реалізація кібератак:
а – із зворотнім зв’язком; б – без зворотного зв’язку

За типом *порушення базових характеристик безпеки* кібератаки бувають К-дії (порушення конфіденційності ресурсів ІС), Ц-дії (порушення цілісності), Д-дії (порушення доступності ресурсів). Якщо у процесі кібератаки порушуються різні характеристики безпеки, то результуючий тип буде комбінований на базі основних, наприклад, кібератака КЦД-дії – порушує конфіденційність, цілісність і доступність ресурсів ІС.

За *природою взаємодії* з ресурсами ІС кібератаки поділяються на фізичні та логічні. Для перших характерна фізична форма взаємодії, яка виявляється у вигляді різного роду прямих блокування, пошкоджень, проникнень, крадіжок тощо (наприклад, розмикання електричних з’єднань, пошкодження носіїв інформації, подолання фізичного кордону захисту, підслуховування тощо). Прикладом фізичної кібератаки може бути перехоплення побічних електромагнітних випромінювань з монітора комп’ютера спеціалізованою

апаратурою (рис. 2.20, а). Логічним кібератакам не властива пряма фізична взаємодія з ресурсами ІС, в основному вони пов’язані з логікою подій, наприклад, аналізом протоколів, перевантаженням, визначенням паролів, захопленням сеансів тощо. Прикладом логічної кібератаки може бути перехоплення сеансу зв’язку (рис. 2.20, б).



а б

Рисунок 2.20 – Приклади кібератак за природою взаємодії: а – фізична; б – логічна

За *реляційними ознаками* джерела НСД і ресурсу ІС, що піддався атакам, кібератаки поділяються на мономономні, полімономні, монополічні, поліполічні. Мономономні кібератаки реалізуються із одного джерела на один конкретний ресурс ІС. Часто такі кібератаки називають нерозподіленими, наприклад, мономономні кібератаки можна реалізувати за допомогою сканування портів комп’ютера з визначеною IP-адресою (рис. 2.21, а).

Полімономні кібератаки здійснюються одночасно з декількох джерел (два і більше) на один ресурс ІС і націлені на досягнення однієї конкретної мети. Такі кібератаки часто називають розподіленими (див. рис. 2.21, б). Монополічні кібератаки реалізуються з одного джерела одночасно на множину ресурсів ІС (два і більше) і направлені на досягнення конкретної мети (рис. 2.21, в).

Приклад такого типу кібератак може бути заснований на широкомовному передаванні повідомлення від джерела на всі комп’ютери сегмента ІС, адреси яких знаходяться під одною маскою підмережі.

Поліполічні кібератаки поєднують у собі полімономну і монополічну технології, за якими множина джерел здійснює кібератаки на множину ресурсів ІС з метою досягнення однієї конкретної мети (рис. 2.21, г).

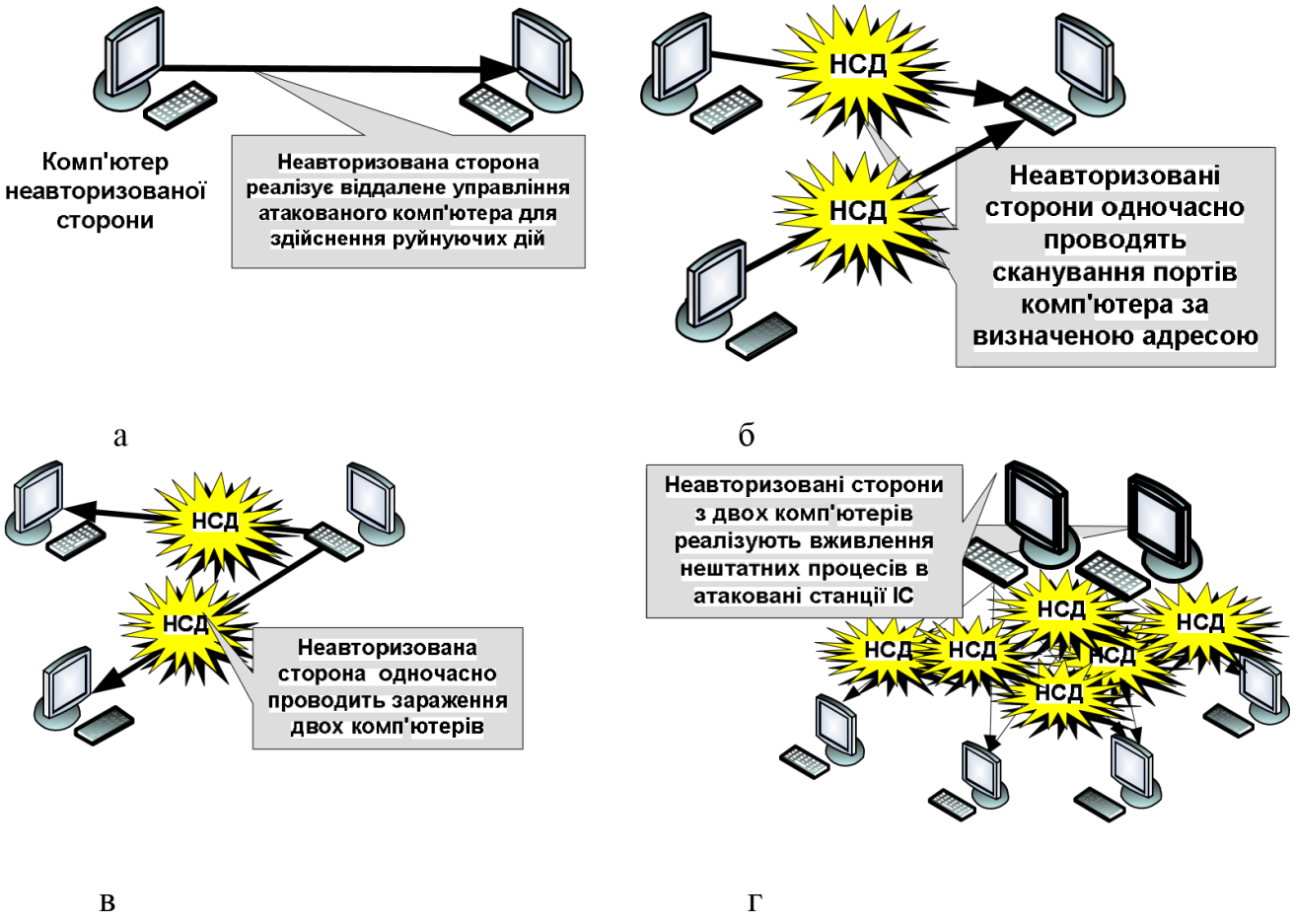


Рисунок 2.21 – Приклади реалізації кібератак за реляційними ознаками: а – мономономна; б – полімономна; в – монополічна; г – поліполічна

За *діями, породженими НСД,* кібератаки можна поділити на інтераптаційні, інтерсептаційні, модифікаційні, фальсифікаційні та вільні. Інтераптаційні кібератаки реалізуються шляхом переривання функціонування ресурсів ІС, інтерсептаційні – шляхом перехоплення різного роду інформації у ІС, модифікаційні кібератаки у процесі доступу до ресурсів ІС здійснюють їхнє

перетворення. Фальсифікаційні кібератаки впроваджують в ІС додаткові компоненти, а вільні кібератаки не направлені на реалізацію НСД до ресурсів ІС.

За *специфікою реалізації* кібератаки можна поділити на фрагментовані, без замовчувань, приховані, пігібекінгові, маскарадні, непрямі, соціотехнічні, криптоаналітичні, неспецифічні. Фрагментовані кібератаки базуються на принципі декомпозиції і поетапної реалізації, наприклад, на основі використання механізму розбиття IP-пакетів (на множину більш дрібних) і подальшого їх передавання (рис. 2.22, а). Такий підхід дозволяє обходити системи виявлення атак, які не розраховані на протидію декомпозиційним технологіям. Кібератаки, які реалізуються без використання значень за замовчуванням, орієнтовані на подолання систем виявлення атак, що засновуються на сигнатурних (шаблонних) технологіях за аналогією з антивірусними програмами, призначеними для захисту від сигнатурних вірусів.

Приховані атаки використовують різноманітні заходи (підміна контрольних сум, перехоплення різноманітних даних, модифікація ядра операційної системи, використання стандартних або схожих до стандартних імен тощо), які дозволяють залишатися невиявленими в локалізованій області атакованого ресурсу ІС. Технологія прихованої кібератаки за своєю ідеологією подібна до технології стелсвірусів.

Пігібекінгові кібератаки полягають у несанкціонованому одержанні доступу до тимчасово неконтрольованого ресурсу ІС. Маскарадні кібератаки грунтуються на формуванні такої поведінки порушника, яка дозволяє йому видати себе за легальне джерело, наприклад, шляхом обману (spoofing) атакувати ІС, привласнюючи IP-адресу, за допомогою якої долається система захисту. Непрямі кібератаки побудовані на тому, що напад здійснюється через третю особу (посередника), а істинне джерело нападу залишається невідомим, при цьому часто використовуються маскарадні технології (рис. 2.22, б).

Соціотехнічні (соціоінжинірингові) кібератаки пов’язані з отриманням даних (наприклад, імен користувачів, паролів, телефонних номерів віддаленого доступу тощо) від атакованих людей у процесі інформаційного обміну (рис. 2.22,

в). Криптоаналітичні кібератаки засновані на використанні широкого спектра криптоаналітичних методів та засобів для зламування ресурсів ІС, захищених різними криптографічними засобами. До неспецифічних кібератак належать ті, які не мають вищезазначених особливостей реалізації, при цьому слід враховувати, що технології кібератак постійно розвиваються і дана ознака може бути розширена [34].

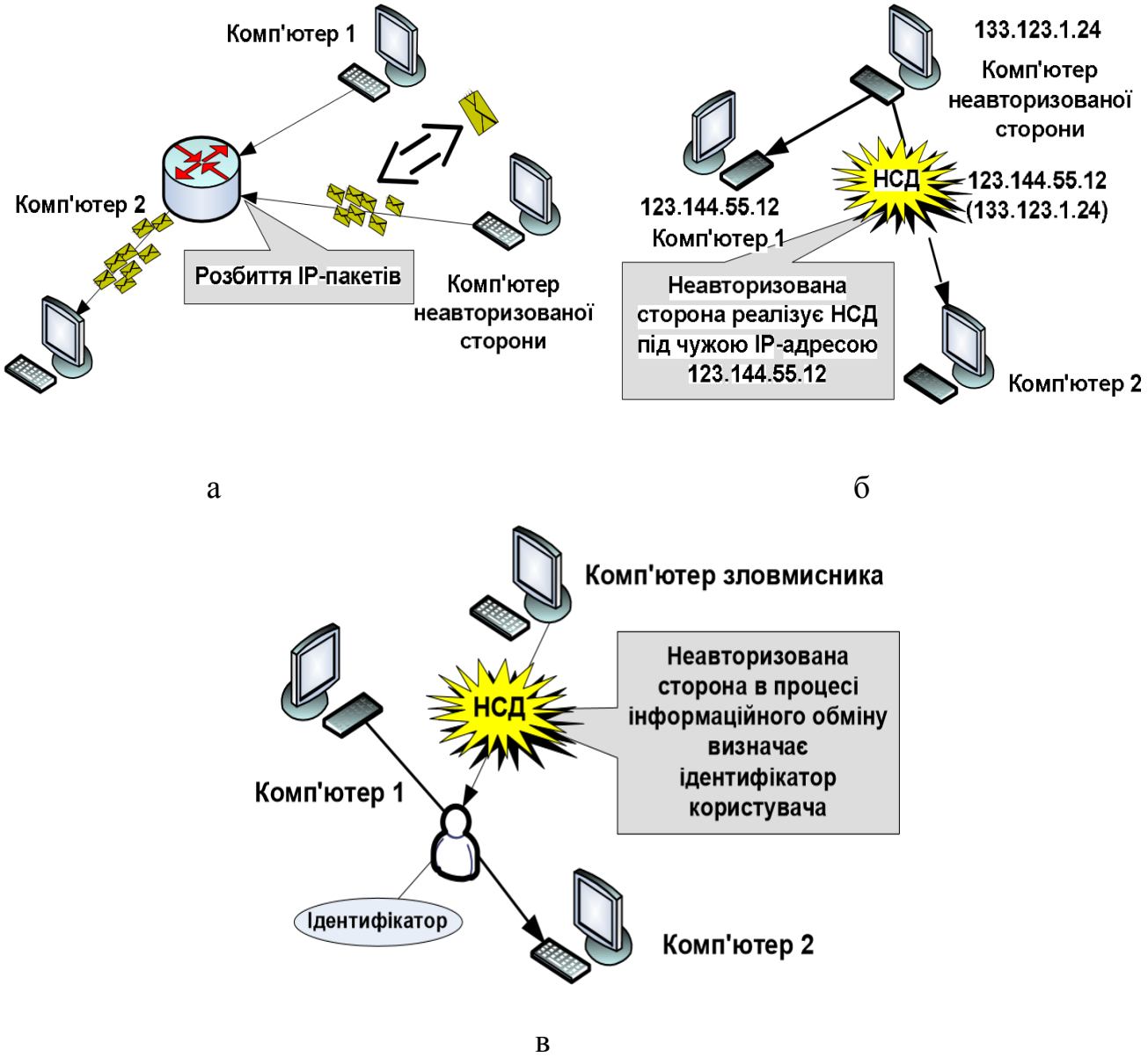


Рисунок 2.22 – Приклади реалізації кібератак за специфікою реалізації:
а – фрагментована; б – непряма; в – соціотехнічна

За *спрямованістю результату* кібератаки поділяються на розширюючі, викривляючі, розповсюджуючі, розкрадаючі, перевантажуючі, інформаційні, утримуючі, знищуючі.

Розширюючі кібератаки (рис. 2.23, а) орієнтовані на одержання більших повноважень на права доступу до ресурсів ІС, наприклад, на вхід до локальної обчислювальної мережі з правами адміністратора.

Викривляючі кібератаки пов’язані зі здійсненням будь-яких прямих змін в цільовому ресурсі ІС, наприклад, підробка полів баз даних, зміна часу і дати тощо.

Розповсюджуючі кібератаки спрямовані на отримання доступу до ресурсів ІС та їх розкриття без відповідних на це повноважень, наприклад, несанкціоноване одержання файлів даних з паролями і їх публікація на хакерських сайтах або розсилання серед абонентів ІС.

Розкрадаючі кібератаки направлені на використання ресурсу ІС без нанесення прямого збитку, наприклад, без зниження якості обслуговування користувачів здійснити тимчасове вилучення частини пам’яті (для розширення можливостей іншої системи), завантаження телекомунікаційних каналів, використання робочої станції або мережевого сервісу тощо.

Перевантажуючі кібератаки спрямовані на завантаження ресурсу до такого рівня, що він втрачає властивість щодо його використання. Результатом таких атак можуть бути “неможливість використання”, “перевантаження”, відмова в обслуговуванні тощо.

Прикладом таких атак (див. рис. 2.23, б) може бути перевантаження маршрутизатора. Інформаційні кібератаки пов’язані зі збиранням необхідних даних і не передбачають здійснення прямих атак на ресурси ІС, наприклад, одержання інформації в результаті аналізу публікацій, використання системних утиліт для виявлення активних робочих станцій, сервісів тощо (рис. 2.23, в).

Утримуючі кібератаки призначені для тимчасової затримки ресурсу ІС з метою зниження його актуальності, наприклад, притримування криптограми на проміжному вузлу при її передачі телекомунікаційними каналами загального користування (рис. 2.23, г).

Знищуючі кібератаки (рис. 2.23, д) орієнтовані на необоротну ліквідацію ресурсу ІС (дроблення інформаційного носія, низькорівневе форматування жорсткого диска тощо).

За *ступенем складності* кібератаки можна поділити на прості, складні та системні. Прості кібератаки є нескладними в реалізації діями, направленими на виконання окремих процедур, (наприклад, сканування портів, аналіз трафіка, пошук активних робочих станцій тощо) [34].

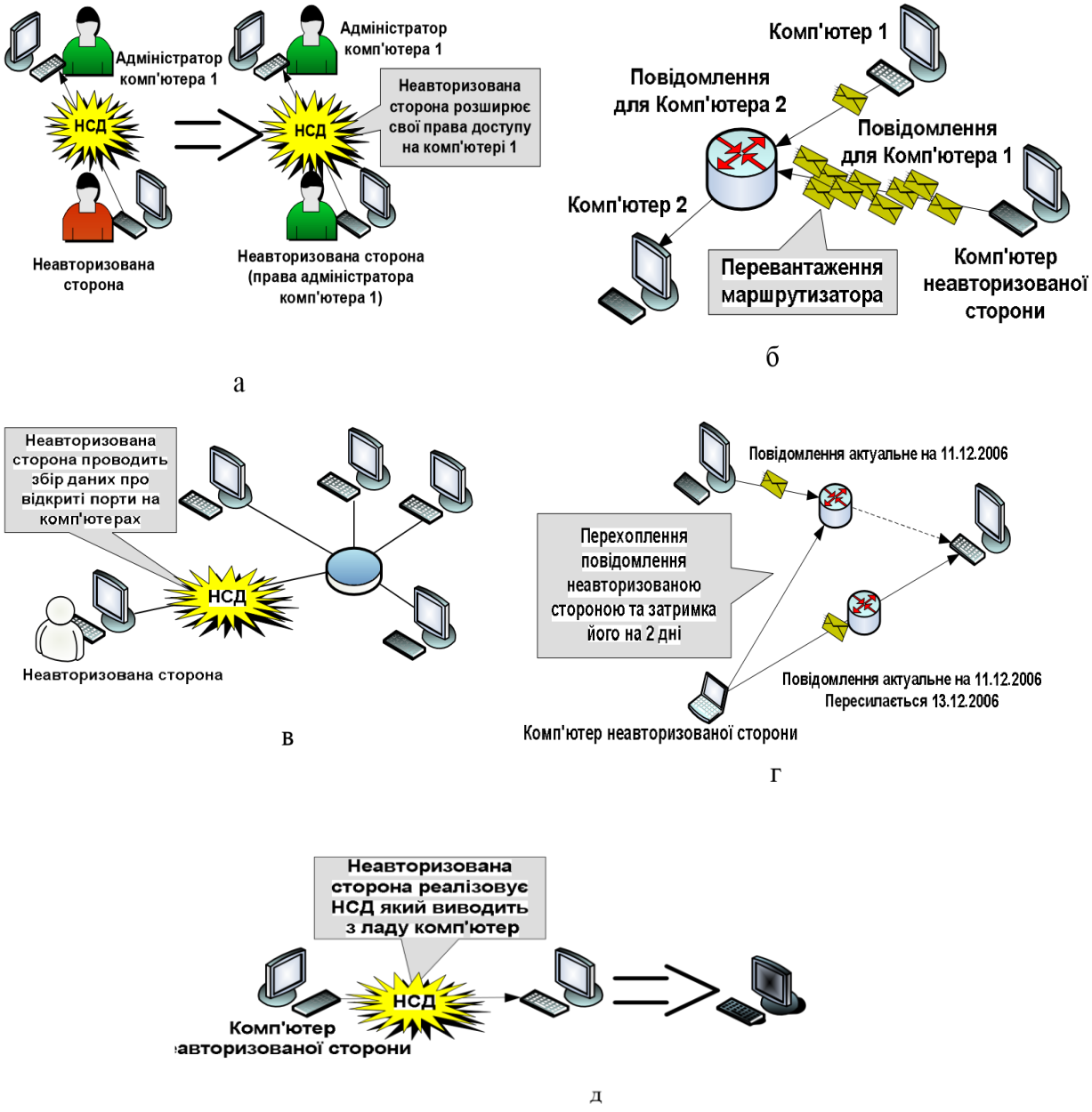


Рисунок 2.23 – Приклади реалізації кібератак за спрямованістю результату: а – розширююча; б – перевантажуюча; в – інформаційна; г – утримуюча; д – знищуюча

Складні кібератаки є комбінацією простих, призначених для реалізації низки необхідних функцій, (наприклад, виявлення активної робочої станції і здійснення віддаленого управління нею). Системні кібератаки будуються на основі сформованого системного підходу з багатокроковою комбінацією дій та використанням простих кібератак для ефективної реалізації спеціально направленого комплексу функцій (наприклад, пошук активних робочих станцій, моніторинг трафіка, несанкціоноване копіювання даних тощо).

За *типом базового ресурсу*, на який орієнтовані кібератаки, можна виділити кібератаки на вузли обчислювальної мережі (ВОМ-ресурсні), кібератаки, спрямовані на локальні обчислювальні мережі (ЛОМ-ресурсні), кібератаки на інформаційні носії (ІНресурсні), кібератаки на операційні системи (ОС-ресурсні), кібератаки на протоколи взаємодії (ПВ-ресурсні), кібератаки, спрямовані на персонал ІС (ПІС-ресурсні), кібератаки на сценарії автоматизації (СА-ресурсні), кібератаки на файли даних (ФД-ресурсні) тощо.

Міжнародна організація стандартизації (ISO) запропонувала семирівневу еталонну модель з метою розмежування функцій різних протоколів у процесі передачі інформації від одного абонента іншому. Таких класів функцій виділено сім. Вони отримали назву рівнів, кожний з який виконує певні завдання у процесі передачі блоку інформації, причому відповідний рівень з боку приймача виконує перетворення, протилежні тим, що зроблені на тому ж рівні на передавальному боці [34].

2.4 Висновки до розділу 2

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

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;

компромісним варіантом є протоколи мережної безпеки IPSec, що функціонують на мережному рівні. З одного боку, вони "прозорі" для додатків, а з іншого – можуть працювати практично в усіх мережах, тому що базуються на широко розповсюдженому протоколі IP. Протоколи IPSec домінують на сьогоднішній день у більшості реалізацій віртуальних приватних мереж і здійснюються як програмним чином (наприклад, протоколи реалізовані в операційній системі Windows компанії Microsoft), так і у вигляді програмно-апаратних реалізацій (рішення Cisco, Nokia). Незважаючи на велику кількість різних способів вирішень, усі реалізації мають високу сумісність одна з одною;

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 у протоколах IPSec з метою забезпечення цілісності й автентичності пакетів даних у всіх реалізаціях мереж IPv6.

Розглянута класифікація кібератак за ознаковим принципом дозволяє сформувати принципи моделі попередження кібератак та формалізувати можливості превентивних систем для підвищення ефективності їх вибору і формування вимог при їх проектуванні та розробці.

Крім того, кібератаки, які класифікуються за ознаковим принципом, можуть у кожному конкретному випадку при визначенні загального класу

містити не лише одну, й більше компонент за будь-якою з вищеперелічених базових ознак.

3 ПРАКТИЧНА ЧАСТИНА МОДЕЛЮВАННЯ ПРОЦЕСУ КІБЕРАТАКИ

3.1 Моделювання процесів кібербезпеки на основі моделі класів кібератак

При моделюванні процесів кібербезпеки значна увага приділяється різноманітності класів кібератак (КБа), варіації їх ознак та особливостям прояву у кожному конкретному випадку.

На сьогодні відомо багато різних підходів до класифікації КБа, але більшість з них має переважно умовний характер, що не дозволяє визначити належність КБа до того чи іншого класу, найбільш точно зробити це сьогодні дозволяє узагальнена класифікація (рис. 3.1.), що розроблена професором Корченко О. Г [13].

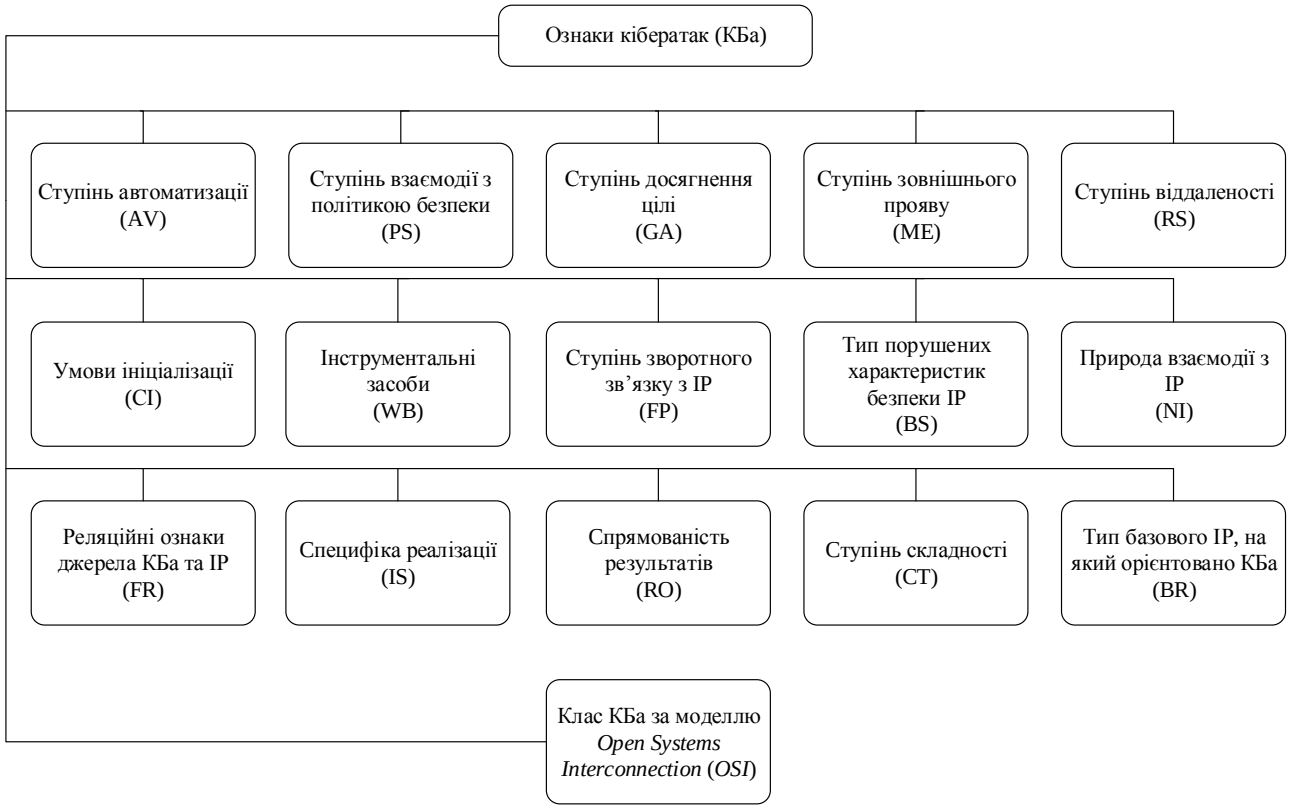


Рисунок 3.1 – Узагальнена класифікація О. Г. Корченко

В свою чергу кожна з ознак описується деякою базовою множиною.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Моделями, що найбільш адекватно і точно описують КБа, згідно прийнятої вище шістнадцятки параметрів, є КБа І-го та ІІ-го класів.

КБа І-го класу: {AV_2 – «автоматизована» ∪ PS_1 – «постполізаційна» ∪ RS_2 – «віддалена» ∪ GA_5 – «вільна» ∪ ME_1 – «пасивна» ∪ CI_2 – «безумовна» ∪ WB_1 – «програмна» ∪ FP_1 – «зі зворотним зв'язком» ∪ BS_1 – «К-дії» ∪ NI_2 – «логічна» ∪ FR_1 – «мономономна» ∪ IS_9 – «неспецифічна» ∪ RO_6 – «інформаційна» ∪ CT_3 – «системна» ∪ BR_1 – «ХОМ-ресурсна» ∪ ISO_{36} – «ISO-36»}

КБа ІІ-го класу: {AV_2 – «автоматизована» ∪ PS_1 – «постполізаційна» ∪ RS_2 – «віддалена» ∪ GA_1 – «інтераптаційна» ∪ ME_2 – «активна» ∪ CI_1 – «умовна» ∪ WB_1 – «програмна» ∪ FP_2 – «без зворотного зв'язку» ∪ BS_3 – «Д-дії» ∪ NI_2 – «логічна» ∪ FR_4 – «поліполічна» ∪ IS_6 – «непряма» ∪ RO_5 – «перевантажувальна» ∪ CT_3 – «системна» ∪ BR_1 – «ХОМ-ресурсна» ∪ ISO_{5E} – «ISO-5E»}.

Фізичний зміст ознакової класифікації визначає, що КБа І- та ІІ-го класів є:

- автоматизованими. КБа здійснюються з постійним втручанням хакера з використанням широкого спектру програмних і апаратних ресурсів які пов'язані з суперзапінгом, снупінгом, снифінгом, підключенням додаткових терміналів (наприклад бот-мереж), використанням мережених аналізаторів тощо;

- постполітизаційними. КБа, що ґрунтуються на застосуванні недоліків у вже реалізованій політиці безпеки. Наприклад застосовуються програмні засоби, що не забезпечують заданий РЗ;

- віддаленими. КБа на ІР при реалізації яких джерело КБа та ІР знаходяться у різних сегментах комп'ютерної мережі;

- вільними (КБа І-го класу) та інтераптаційними (КБа ІІ-го класу). Вільні КБа не орієнтовані на порушення прийнятої політики безпеки. Вони спрямовані на збір інформації, наприклад ведення елементів мереженої розвідки, таких як визначення топології мережі, визначення активних IP-адрес та доступних сервісів тощо. Інтераптаційні КБа здійснюються шляхом припинення функціонування ІР шляхом втрати їх функціональності або виведення їх у незахищений стан, наприклад з використанням блокуючи механізмів тощо;

- пасивні (КБа І-го класу) та активні (КБа ІІ-го класу). Пасивні КБа не здійснюють безпосередній вплив на ІР та не порушують характеристики його безпеки. Активні КБа здійснюють безпосередній вплив на ІР, що призводить до порушення характеристик безпеки;

- безумовні (КБа І-го класу) та умовні (КБа ІІ-го класу). Безумовні – КБа ініціалізуються без змін стану ІР й визначаються джерелом КБа. Умовні КБа ініціалізуються з настанням певної події в системі, наприклад надходження запиту на запуск роботи АС в складі бот-мережі;

- програмні. КБа, в основу яких покладено спеціальні мікро- або макрокодовані засоби;

- зі зворотним зв’язком (КБа І-го класу) та без зворотного зв’язку (КБа ІІ-го класу). При реалізації КБа зі зворотним зв’язком здійснюється отримання від ІР, що атакується відповіді на певні дії, які необхідні для подальшого продовження вказаного процесу на більш ефективному рівні. Це досягається за рахунок аналізу реакції об’єкта КБа на певні зміни. КБа без зворотного зв’язку реалізує механізм КБн незалежно від реакції ресурсу, що атакується;

- К-дії (КБа І-го класу) та Д-дії (КБа ІІ-го класу). КБа К- та Д-дії спрямовані на порушення таких характеристик ІР як конфіденційність та цілісність;

- логічні. Логічні КБа не передбачають прямої фізичної взаємодії з ресурсами. Такі КБа пов’язані в основному з логікою подій, перенавантаженням тощо;

- мономономні (КБа І-го класу) та поліполічні (КБа ІІ-го класу). Мономономні КБа реалізуються з одного джерела на один конкретний ресурс.

Поліполічні КБа реалізують процес КБн одночасно з одного джерела одночасно на декілька IP або з декількох джерел на один IP для досягнення конкретної мети;

- неспецифічні (КБа I-го класу) та непрямі (КБа II-го класу). Неспецифічні КБа – це ті КБа, що характеризуються невідомими на момент її реалізації характеристиками. Непрямі КБа полягають в тому, що процес КБн реалізується через підставну IP-адресу з використанням маскарадних технологій;

- інформаційні (КБа I-го класу) та перевантажувальні (КБа II-го класу). Інформаційні КБа полягають у зборі необхідних даних для реалізації подальших дій. Перевантажувальні КБа спрямовані на завантаження IP до такого рівня, за якого IP втрачає свої функціональні властивості;

- системні. Системні КБа ґрунтуються на системному підході з багатокроковим механізмом реалізації цілого комплексу спеціальних функцій;

- XOM-ресурсні. XOM-ресурсні КБа спрямовані на окремі хости обчислювальної мережі;

ISO-36 (КБа I-го класу) та ISO-5E (КБа II-го класу). ISO-36 – це КБа, яка за семирівневою еталонною моделлю ISO визначається як двійковий код, що подано шістнадцятирічним кодом $36_{(16)} = 0110110 = 2^6 + 2^5+2^3 +2^2 =$ K6 + + K5 + K3 + K2. Тобто КБа ISO-36 інтерпретує процес КБн на канальному, мереженому, сеансовому рівнях та рівні відображення. ISO-5E – це КБа, яку можна подати шістнадцятирічним кодом $7E_{(16)} = 1111110 = 2^6+2^5+2^4+2^3+2^2+2^1 =$ = K6+ K5 + K4 + K3 + K2 + K1. КБа ISO-7E реалізується на фізичному, мереженому, транспортному, сеансовому рівнях та рівні відображення.

Для формування загроз и виявлення аномальної роботи сформуємо класифікатор, який на відмову від відомих забезпечує врахування синергізму і гібридності сучасних загроз.

3.2 Формалізація принципів побудови класифікатора загроз складових безпеки БІн: інформаційної безпеки, кібербезпеки, безпеки інформації

Перша платформа – класифікації загроз за складовими безпеки БІР ОБС: інформаційна безпека (ІБ) (01), безпека інформації (БІ) (02), кібербезпека (КБ) (03). Введемо такі дефініції.

Дефініція 1. *Безпека банківських інформаційних ресурсів (Б БІР)* – стан захищеності банківських інформаційних ресурсів, що характеризується здатністю користувачів, технічних засобів і інформаційних технологій забезпечити конфіденційність, цілісність автентичність і доступність банківських інформаційних ресурсів при їх обробці в АБС.

Дефініція 2. *Інформаційна безпека банківських інформаційних ресурсів (ІБ БІР)* – стан захищеності інформаційного середовища ОБС, що забезпечує її формування, використання і розвиток в інтересах громадян і ОБС.

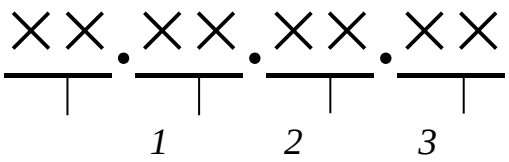
Дефініція 3. *Кібербезпека банківських інформаційних ресурсів (КБ БІР)* – набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до управління ризиками, дій, професійної підготовки, страхування і технологій, які використовуються для захисту кіберсереди АБС, ресурсів і користувачів ОБС.

Друга платформа – класифікація загроз за характером напрямків: нормативно-правовий (01), організаційний (02), інженерно-технічний (03);

Третя платформа – класифікація загроз у відповідності з основними особливостями інформації: конфіденційність (01), цілісність (02), доступність (03), автентичність (04).

Четверта платформа – класифікація загроз за рівнями ієрархії інфраструктури АБС: *FL* – фізичний рівень (01), *NL* – мережевий рівень (02), *OSL* – рівень операційних систем (ОС) (03), *DBL* – рівень систем управління базами даних (04), *BL* – рівень банківських технологічних застосунків і сервісів (05).

Частини класифікатора поділяються точкою і мають вигляд, зображений на рис. 3.2.



(*1* – синергетична складова безпеки БІР, *2* – характер напрямків;
3 – особливості інформації; *4* – рівні ієрархії інфраструктури АБС).

Рисунок 3.2 – Складові узагальненого класифікатора

На рис. 3.3 наведено взаємозв’язок структурної схеми класифікатора загроз з АБС ОБС.

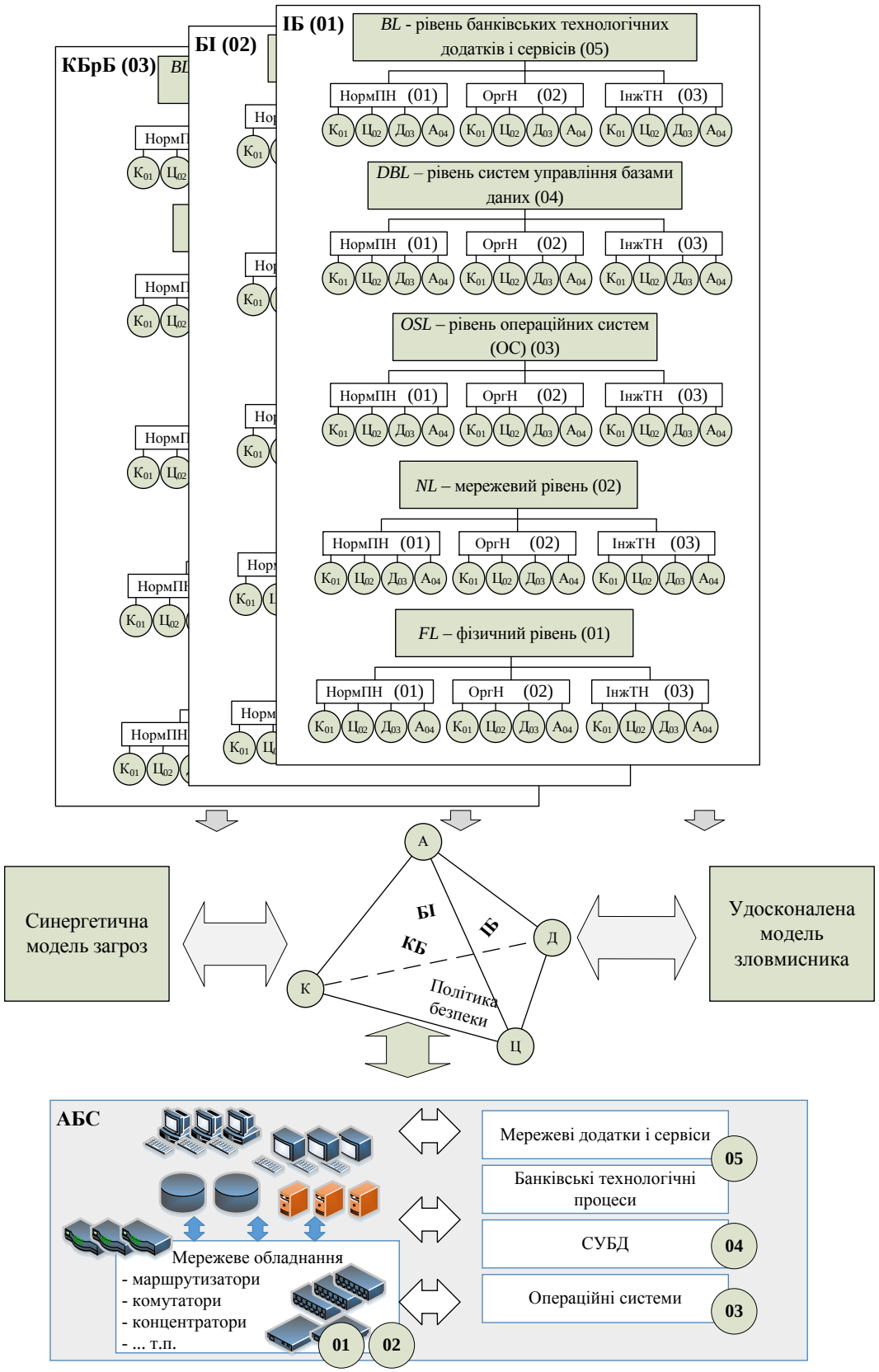


Рисунок 3.3 – Взаємозв’язок структурної схеми класифікатора загроз з АБС ОБС

Множину загроз інформаційній безпеці, кібербезпеці, безпеці інформації на банківські інформаційні ресурси запропоновано використовувати з електронного ресурсу (http://bdu.fstec.ru/vul) [29].

Крок 1.1. Формування метричних коефіцієнтів загроз експертами за послугами безпеки. Нехай j – послуги безпеки БІР. Основними послугами безпеки БІР є C –конфіденційність; I – цілісність; A – доступність; Au – автентичність. Тоді класифікатор за чотирма послугами безпеки описується виразом вигляду $j = \{C, I, A, Au\}$ Класифікатор містить N загроз. У складанні вагових коефіцієнтів прояву кожної загрози на послуги безпеки БІР брали участь K експертів.

Позначимо через i поточний номер загрози $(\{i\}_1^N)$, через k – поточний номер експерта, який виконував оцінку $(\{k\}_1^K)$. Середнє значення оцінки експертів за всіма загрозами для певної послуги безпеки може бути записане:

$$w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j, \qquad (3.1)$$

де w_{ik}^j – значення метричного коефіцієнта, виставленого k-м експертом для i-ї загрози j-ї послуги безпеки; N – кількість загроз; K – кількість експертів.

Крок 1.2. Формування ідентифікаторів загроз за складовими класифікатора. На цьому кроці експерти формують цифрове значення (код) ідентифікатора загрози за відповідними складовими класифікатора.

Крок 1.3. Вибір вагових коефіцієнтів α_i, що визначають умови прояву i-ї загрози (табл. 3.1).

Таблиця 3.1 – Таблиця вибору вагових коефіцієнтів α_i прояву i-ї загрози

Вагові коефіцієнти α_i	Умови прояву загрози
0,067	загроза проявляється не частіше одного разу на 5 років
0,133	загроза проявляється не частіше одного разу на рік
0,2	загроза проявляється не частіше одного разу на місяць
0,267	загроза проявляється не частіше одного разу на тиждень
0,333	загроза проявляється щодня

Крок 1.4. Визначення реалізації кожної i-ї загрози з урахуванням імовірності прояву атаки (її виникнення) здійснюється за виразом:

$$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j. \qquad (3.2)$$

Для кожної послуги безпеки та *i*-ї загрози:

$$w_i^C \alpha_i^C = \frac{1}{K} \alpha_i^C \sum_{k=1}^{K} w_{ik}^C \text{ – послуга конфіденційність;}$$

$$w_i^I \alpha_i^I = \frac{1}{K} \alpha_i^I \sum_{k=1}^{K} w_{ik}^I \text{ – послуга цілісність;}$$

$$w_i^A \alpha_i^A = \frac{1}{K} \alpha_i^A \sum_{k=1}^{K} w_{ik}^A \text{ – послуга доступність;}$$

$$w_i^{Au} \alpha_i^{Au} = \frac{1}{K} \alpha_i^{Au} \sum_{k=1}^{K} w_{ik}^{Au} \text{ – послуга автентичність,}$$

де $w_{ik}{}^C$, $w_{ik}{}^I$, $w_{ik}{}^A$, $w_{ik}{}^{Au}$ – експертні вагові коефіцієнти послуг безпеки: конфіденційності, цілісності, доступності, автентичності; α_i^C, α_i^I, α_i^A, α_i^{Au} – ваговий коефіцієнт послуги безпеки: конфіденційності, цілісності, доступності, автентичності прояву атаки *i*-ї загрози.

Крок 1.5. Визначення реалізації виникнення декількох загроз для обраної послуги розраховується з урахуванням виразу (3.2):

$$W_{synerg}^C = \sum_{i=1}^{M} w_i^C \alpha_i^C \text{ – послуга конфіденційність;}$$

$$W_{synerg}^I = \sum_{i=1}^{M} w_i^I \alpha_i^I \text{ – послуга цілісність;}$$

$$W_{synerg}^A = \sum_{i=1}^{M} w_i^A \alpha_i^A \text{ – послуга доступність;}$$

$$W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au} \text{ – послуга автентичність,} \qquad (3.3)$$

де M – кількість декількох загроз, які вибрані експертом з ІБ банку з множини $\{i\}_i^M$, яка є підмножиною усієї множини загроз класифікатора, тобто $M \le N$.

При формуванні метричних коефіцієнтів уважається, що отримані результати належать до незалежних загроз, у випадку їх залежності (збіг

класифікатора загроз) необхідно скористатися виразом визначення повної ймовірності залежних подій:

$$P(AB) = P(A) + P(B) - P(AB).$$

Статистична обробка результатів оцінювання можливості впливу *i*-ї загрози на послугу безпеки в АБС експертами проводиться за методикою, описаної в роботі. Підсумкова оцінка *i*-ї загрозі осереднюється за кількістю експертів відповідно до виразу:

$$x_i = \frac{\sum_{k=1}^{K} x_k \times k_k}{K}, \tag{3.4}$$

де x_k– оцінка *k*-го експерта впливу *i*-ї загрози;

k_k – рівень компетентності експерта;

K– кількість експертів.

Мірою погодженості думок експертів вважається дисперсія, що обчислюється за виразом:

$$\sigma_x^2 = \frac{1}{K}\sum_{k=1}^{K} k_k \left(x_k - x_i\right)^2. \tag{3.5}$$

Статистична значимість отриманих результатів з імовірністю 1 – α_i, становить: $[\widetilde{x_i} - \Delta, \widetilde{x_i} + \Delta]$, де величина x_i розподілена за нормальним законом із центром у $\widetilde{x_i}$ і дисперсією σ_x^2 . Тоді Δ визначається за виразом:

$$\Delta = t\sqrt{\sigma_x^2 / N}, \tag{3.6}$$

де *t* – величина, що підкоряється розподілу Стьюдента для *K* – 1 ступенів свободи, *K* – кількість експертів.

Крок. 1.6. Визначення сумарної загрози за складовими безпеки з урахуванням виразу (3.3) розраховується:

$$W_{synerg}^{IS} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}\right)\alpha_i,$$

$$W_{synerg}^{CS} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}\right)\alpha_i,$$

$$W_{synerg}^{SI} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) \alpha_i . \quad (3.7)$$

Крок. 1.7. Визначення узагальненої синергетичної загрози на БІР:

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB} \cup W_{synerg}^{BI} . \quad (3.8)$$

Крок 1.8. Визначення узагальненої синергетичної загрози з урахуванням її гібридності розраховується:

$$W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{C} \cap W_{synerg}^{\text{I}} \cap W_{synerg}^{A} \cap W_{synerg}^{Au}. \quad (3.9)$$

Результати досліджень загроз з максимальною частотою їх прояву на БІР наведені у табл. 3.2

Таблиця 3.2 – Результати оцінювання загроз на основі синергетичного підходу

Складові безпеки	Послуги безпеки				
	C, W_{synerg}^{C}	*I*, W_{synerg}^{I}	*A*, W_{synerg}^{I}	*Au*, W_{synerg}^{Au}	Підсумок
IB, W_{synerg}^{IB}	0,023	0,223	0,193	0,207	0,0002
KB, W_{synerg}^{KB}	0,222	0,234	0,197	0,134	0,0014
BI, W_{synerg}^{BI}	0,226	0,109	0,152	0,189	0,0007
Підсумок	0,471	0,566	0,542	0,53	
$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB} \cup W_{synerg}^{BI} =$ =0,0002+0,0014+0,0007=**0,0223**			$W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{\text{C}} \cap W_{synerg}^{\text{I}} \cap W_{synerg}^{A} \cap W_{synerg}^{Au}$ = =0,471×0,566×0,542×0,53=**0,0766**		

3.3 Висновки до розділу 3

КБа І-го та ІІ-го класів достатньо повно перекривають найнебезпечніші та найбільш розповсюджені класи КБа. Одержує подальшого розвитку формалізований підхід до опису ознакової класифікації КБа, що сприяє формуванню формалізованих вимог до побудови високоефективних прогресивних СЗІ.

Класи кібератак мають різноманітні варіації ознак та особливості прояву у кожному конкретному випадку. Представлена у даному розділі класифікація кібератак за ознаковим принципом надає можливість розробити концептуальні аспекти моделі попередження кібератак та формалізувати можливості превентивних систем для підвищення ефективності їх вибору і формування вимог при їхньому проектуванні та розробці.

Кібератаки, які класифікуються за ознаковим принципом, можуть у кожному конкретному випадку при визначенні загального класу містити не лише одну, а більше компонент за будь-якою з вище перелічених базових ознак. Однак з появою нових методів та засобів реалізації кібератак ознаки запропонованої класифікації можуть бути розширені.

Запропонований класифікатор загроз забезпечує можливість формування єдиного підходу щодо визначення загрози та її врахування під час виявлення аномальної роботи, або відхилення від нормальної роботи в середовищі безпровідних мереж на прикладі АБС.

4 СПЕЦІАЛЬНА ЧАСТИНА

В розділі описано сучасні програми - аналізатори мережевого трафіку

Аналізатор трафіку, або sniffer - мережевий аналізатор трафіку, програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу трафіку, або виключно з метою аналізу мережевого трафіку, призначеного для інших вузлів. Аналіз трафіку який пройшов через sniffer дає можливість: знайти паразитний, вірусний і закільцований трафік, присутність якого підвищує завантаження мережевого обладнання та каналів зв'язку (сніфери тут малоефективні; як правило, для цих цілей застосовують збір різної статистики серверами і активним мережним устаткуванням і її подальший аналіз); перехопити будь-який незашифрований (а іноді і зашифрований) користувачем трафік для отримання паролів та іншої інформації; локалізувати несправність мережі або помилку конфігурації мережевих агентів (для цієї мети сніфери зазвичай застосовуються системними адміністраторами). У зв'язку з тим, що в «класичному» сніффері аналіз трафіку відбувається вручну, з використанням лише найпростіших засобів автоматизації (дослідження протоколів, відновлення TCP-потоку), то він підходить для аналізу тільки невеликих його обсягів.

4.1 Програма Wireshark

Wireshark (раніше – Ethereal) - програма-аналізатор трафіку для комп'ютерних мереж Ethernet і деяких інших. Він має графічний інтерфейс користувача. Wireshark - це програма, яка «знає» структуру самих різних мережевих протоколів, і тому дозволяє розібрати мережевий пакет, показуючи значення кожного поля протоколу будь-якого рівня. Так як для захоплення пакетів застосовується pcap, є можливість захоплення даних виключно з тих мереж, які підтримуються цією бібліотекою. Тим не менш, Wireshark уміє працювати з безліччю форматів вихідних даних, отже, можна

відкривати файли даних, захоплених іншими програмами, що підвищує можливості їх захоплення.

Можливості Wireshark:

- працює на більшості сучасних операційних систем (Microsoft Windows, Mac OS X, UNIX). Wireshark - програмний продукт з відкритим вихідним кодом, поширюється на підставі ліцензії GPL. Він може бути використаний на будь-якій кількості комп'ютерів, не остерігаючись введення ліцензійних ключів, продовження ліцензії та інші неприємних заходів. Таким чином, співтовариству дуже легко додати в його підтримку нових протоколів як плагінів або вшити їх безпосередньо у вихідний код;
- перехоплення трафіку мережевого інтерфейсу в режимі реального часу. Wireshark може захопити трафік від різних мережевих пристроїв, відображаючи його ім'я (у тому числі бездротові пристрої). Підтримка пристрою залежить від багатьох факторів, наприклад від операційної системи;
- різноманітність протокольних декодувальників (TELNET, FTP, POP, RLOGIN, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, MSN, YMSG та інші);
- збереження і відкриття раніше збереженого мережевого трафіку;
- імпорт і експорт файлів з інших аналізаторів пакетів. Wireshark може зберегти перехоплені пакети у великій кількості форматів іншими аналізаторами пакетів, наприклад: libpcap, tcpdump, Sunsnoop, atmsnoop, Shomiti / FinisarSurveyor, NovellLANalyzer, MicrosoftNetworkMonitor, AIX'siptrace;
- дозволяє виконувати фільтрацію пакетів за кількома критеріями;
- дозволяє шукати пакети для різних критеріїв;
- дозволяє виділити перехоплені пакети різних протоколів;
- дозволяє створювати різні статистичні дані.

Інтерфейс програми Wireshark показаний на рисунку 4.1.

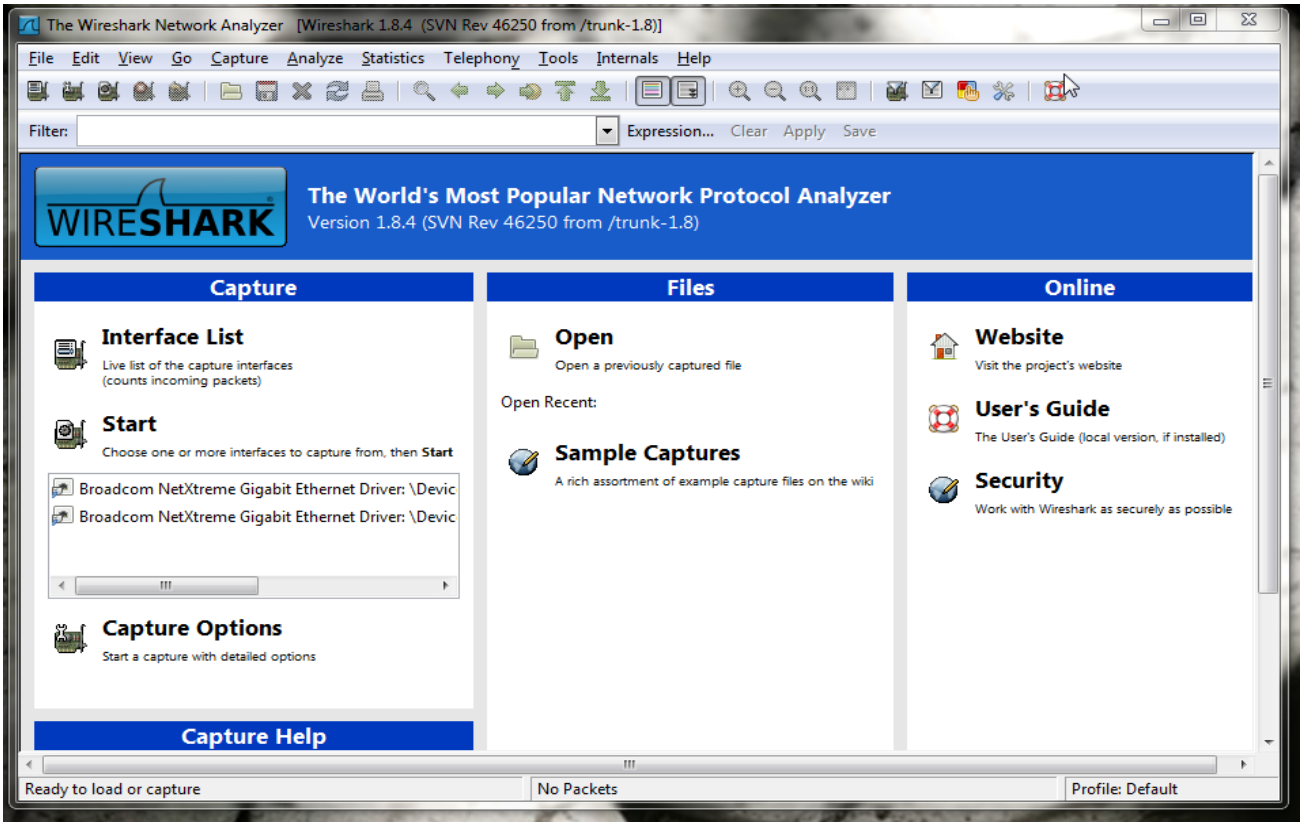


Рисунок 4.1 - Головне вікно програми Wireshark

Аналізатори протоколів незамінні в цілях дослідження реальних мереж, однак вони не забезпечують кількісної оцінки характеристик для ще не існуючих мереж, які знаходяться в стадії проектування. У цих випадках можна використовувати засоби моделювання, за допомогою яких розробляються моделі, які відтворюють інформаційні процеси, що протікають в мережах.

4.2 Netflow analyzer

Netflow analyzer - мережевий протокол, призначений для обліку мережевого трафіку, розроблений компанією Cisco Systems. Є фактично промисловим стандартом і підтримується не тільки обладнанням Cisco, а й багатьма іншими пристроями (зокрема, Juniper і Enterasys). Також існують вільні реалізації для UNIX-подібних систем.

Існує кілька версій протоколу, найбільш поширеними з яких на 2011 рік є версії 5 і 9. На основі версії 9 (див. рис.2.2) також був розроблений відкритий

стандарт під назвою IPFIX (Internet Protocol Flow Information eXport, експорт інформації про потоки IP).

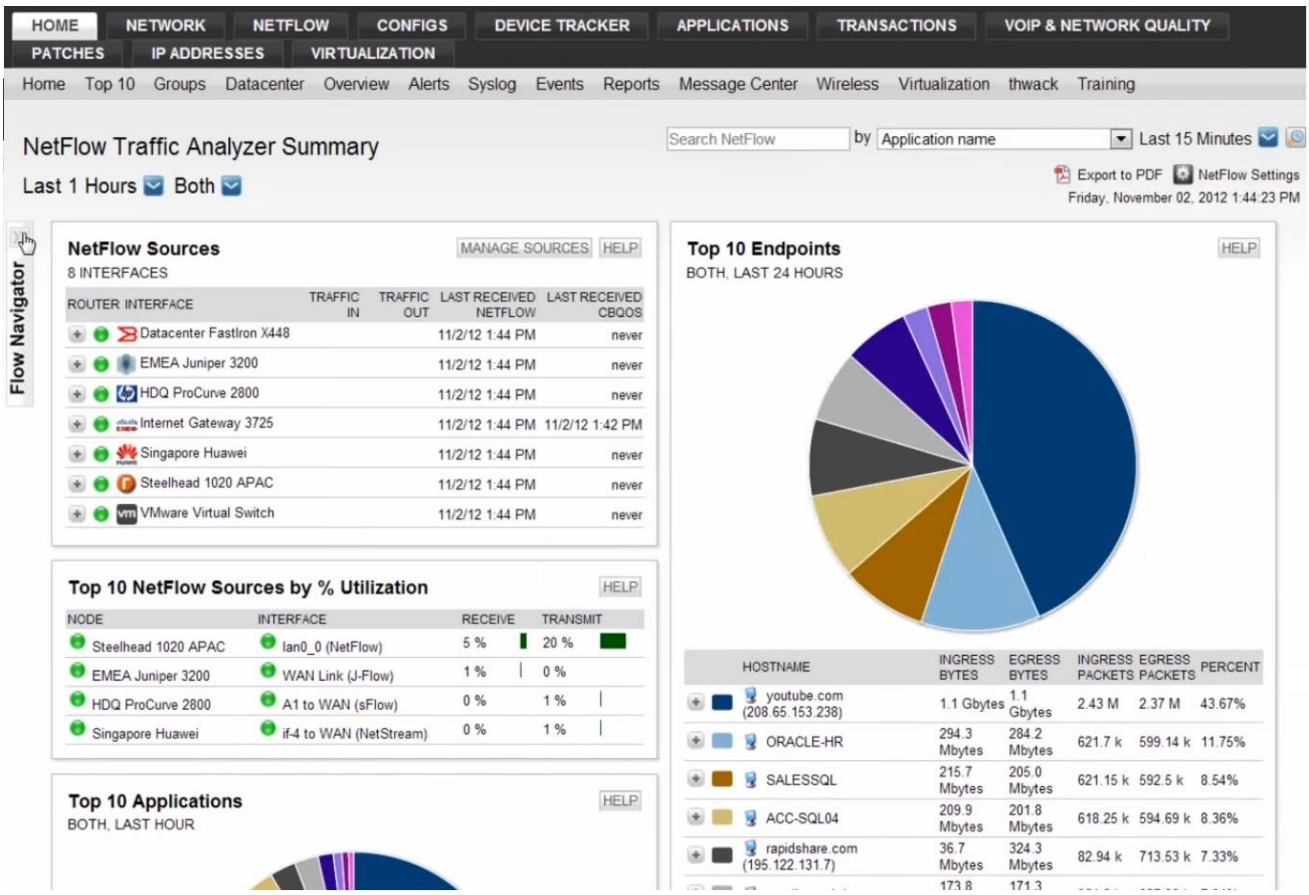


Рисунок 4.2 – Головне вікно програми Netflow analyzer

Архітектура системи будується на сенсорі, колекторі і аналізаторі:

- сенсор збирає статистику про трафік який через нього проходить. Сенсори є краще ставити в «вузлових точках» мережі, наприклад, на віддалених маршрутизаторах сегментів мережі;
- колектор здійснює збір інформації від сенсорів. Отримані дані він скидає в файл для подальшої обробки. Різні колектори зберігають дані в різних форматах;
- аналізатор, або система обробки, зчитує ці файли і генерує звіти у формі, більш зручній для людини. Ця система повинна бути сумісна з форматом даних, що надаються колектором. У сучасних системах колектор і аналізатор часто об'єднані в одну систему.

Зазвичай колектор і аналізатор є частинами одного програмного комплексу, який працює на сервері. Різновидів ПО колектор / аналізатор безліч, платні і безкоштовні, під Windows і Unix-системи.

Колектор і аналізатор є «пасивними» елементами системи. Сенсор посилає на колектор звіти про трафік, колектор приймає, аналізатор аналізує, і заповнює свою базу даних на сервері. По суті, при піднятому сервері, нам не потрібно вручну підключати пристрої, які підпадають під моніторинг, на сервері. Поки сенсор формує і посилає звіти, колектор їх приймає, аналізатор реєструє. Якщо сенсор вимкнений, він «зникає» з поточної «он-лайн» статистики.

NetFlow використовує UDP або SCTP для передачі інформації про трафік колектора. Як правило, колектор слухає порт 2055, 9555 або 9995 (або той, який ви вкажете при налаштуванні колектора і сенсора).

Сенсор виділяє з трафіку потоки, що характеризуються наступними параметрами:

- адреса джерела;
- адреса призначення;
- порт джерела для UDP і TCP;
- порт призначення для UDP і TCP;
- тип і код повідомлення для ICMP;
- номер протоколу IP;
- мережевий інтерфейс (параметр ifindex SNMP);
- IP Type of Service.

Потоком вважається набір пакетів, що проходять в одному напрямку. Коли сенсор визначає, що потік закінчився (зі зміни параметрів пакетів, або по скиданню TCP - сесії), він відправляє інформацію в колектор. Залежно від налаштувань він також може періодично відправляти в колектор інформацію про всі потоки що ще не закінчилися.

4.3 Висновки до розділу 4

В розділі наведено особливості роботи, переваги та недоліки найбільш популярних сучасних програм - аналізаторів мережевого трафіку

РОЗДІЛ 5. ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Об’єктом дослідження є відділ підприємство «Степ». Компанія спеціалізується на розробці та впровадженні програмного забезпечення й інтеграції систем керування інформацією.

Для компанії велике значення має захист інформації, оскільки розроблене програмне забезпечення має велику цінність. Специфікою фірми «Степ» є робота з бухгалтерськими базами даних клієнтів. Витік такої інформації допустити не можна, оскільки вона становить фінансову таємницю, містить клієнтські бази фірм-партнерів з персональними даними.

Дослідимо економічну доцільність розгортання захищеної wi-fi мережі в офісі «Степ» напротивагу оренді такої мережі. Мережа складається з перемикачів (switches), з’єднаних цифровим середовищем передачі даних. Кінцеве обладнання, наприклад, маршрутизатори, зв’язуються через мережу в одному чи кількох напрямах. У стандартній термінології, перемикачі FR належать до класу пристроїв DCE (Data Communications Equipment), а кінцеве обладнання користувача — до класу DTE (Data Terminal Equipment).

5.1. Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{ві} = q_{\text{і}} \cdot p_{\text{і}} , \qquad (5.1)$$

де: $q_{\text{і}}$ – кількість витраченого матеріалу і–го виду; $p_{\text{і}}$ – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{ві} . \qquad (5.2)$$

Розрахунки занесемо у таблицю 5.1.

Таблиця 5.1- Специфікація обладнання для розгортання захищеної мережі wi-fi.

№ п/п	Назва обладнання	Ціна	Кількість	Вартість
1.	Коммутатор Cisco SB SF250-48HP 48-port 10/100 PoE Switch (SF250-48HP-K9-EU)	₴ 17 155	3	₴ 51 465
2.	Кабель оптичний FinMark UT004-SM-15	₴ 4,06	1000	₴ 4060
3.	Маршрутизатор Cisco RV345 Dual WAN Gigabit VPN Router (RV345-K9-G5)	₴ 9435	2	₴ 18870
Всього				**₴ 74395**

5.2. Розрахунок норм часу на розгортання захищеної мережі wi-fi

Ефективне використання часу має велике значення тому, що коефіцієнт корисної дії залежить від оптимального використання часу.

Основні етапи розгортання мережі frame relay:

1. Розробка топології мережі;

2. Встановлення обладнання;

3. Налаштування обладнання.

Для оцінки тривалості виконання окремих робіт використовують нормативи часу.

Витрати часу по окремих операціях технологічного процесу відображені в таблиці 5.2.

Таблиця 5.2 – Операції технологічного процесу та час їх виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Розробка топології мережі	системний адміністратор	10
2.	Встановлення обладнання	інженер	48
3.	Налаштування обладнання	системний адміністратор	12

Разом	70

Загальні затрати часу на реалізацію даної роботи становлять 70 годин, найбільш трудомістким є встановлення обладнання – 48 годин.

5.3 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується за виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Згідно закону України «Про Державний бюджет України на 2019 рік», зокрема статтею восьмою мінімальна заробітна плата у погодинному розмірі становить 25,13 грн. Рекомендовані тарифні ставки: системний адміністратор – 150,00-250,00 грн./год., інженер – 100,00-200,00 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г\ , \qquad (5.3)$$

де $Т_с$ – тарифна ставка, грн.; $К_г$ – кількість відпрацьованих годин.

Основна заробітна плата буде розраховуватись за формулами 5.4, 5.5.

$$З_{осн.\ сисадм.} = 200{,}00 \cdot 22 = 4400{,}00 \text{ грн.} \qquad (5.4)$$

$$З_{осн.\ інж.} = 150{,}00 \cdot 48 = 7200{,}00 \text{ грн.} \qquad (5.5)$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \qquad (5.6)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод} = 11600{,}00 \cdot 0{,}15 = 1740{,}00 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.} = З_{осн.} + З_{дод.} \qquad (5.7)$$

$$В_{о.п.} = 11600{,}00 + 1740{,}00 = 13340{,}00 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи:

- єдиний соціальний внесок ЄСВ (прибутковий податок) – 22%;
- військовий збір – 1,5%.

У сумі зазначені відрахування становлять 23,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$B_{с.з.} = Ф_{оп} \cdot 0{,}235 \quad (5.8)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

$$B_{с.з.} = 13340{,}00 \cdot 0{,}235 = 3134{,}90 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці наведено у таблиці 5.2.

Таблиця 5.2 – Розрахунки витрат на оплату праці

з/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Відрахування $Ф_{ОП}$, грн.	Всього витрати на плату праці, грн. (6=3+4+5)
		Тарифна ставка, грн.	Кількість відпрацьованих год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1.	Системний адміністратор	200	22	4400	660	1189,1	6249,1
2.	Інженер	150	48	7200	1080	1692	9972
Всього							**16221,1**

З таблиці розрахунки витрат на оплату праці видно що всього витрати на оплату праці становить 16221,1 грн.

Надамо основні техніко-економічні та фінансові показники інвестиційного проекту, розрахованого на суму інвестицій 90616,1 грн.

1) для придбання обладнання необхідна сума 74395 грн;

2) на заробітну плату фахівців з розгортання мережі 16221,1 грн;

3) тариф оренди wi-fi мережі становить плату за підключення 2000 грн та щомісячну абонплату 2300 грн.

Період окупності (РР) є одним з найбільш розповсюджених і зрозумілих показників ефективності інвестицій.

Період окупності – це термін, по закінченні якого суми, що надходять, стають прибутком. Упродовж цього періоду відбувається відшкодування капітальних витрат по проекту за рахунок чистого грошового потоку.

Для визначення терміну окупності отриманий чистий грошовий потік сумують до тих пір, поки він не стане рівний величині початкових інвестицій проекту, тобто:

$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1+i)^t} = \sum_{t=0}^{n} \frac{K_t}{(1+i)^t} . \qquad (5.9)$$

5.4 Висновки до розділу 5

Термін окупності інвестиційного проекту для фірми «Степ» становить 3 роки і 3 місяці.

Основною позитивною рисою методу оцінки ефективності проектів за періодом окупності є простота. Цей показник корисний також для оцінки ризикованості проекту (чим вищий термін окупності, тим вищий ризик). Особливістю розглянутого показника є те, що він не враховує динаміку подій після того, як проект окупить себе, не вимірює прибутковості інвестиційного проекту, а виявляє його ліквідність.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Охорона праці

6.1.1 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 людини в процесі трудової діяльності. Дія цього Закону поширюється на всіх юридичних та 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 кількістю працюючих 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)

Облаштування робочого місця працівника з екранними пристроями має відповідати вимогам Санітарних норм виробничого шуму, ультразвуку та інфразвуку ДСН 3.3.6.037-99, затверджених постановою Головного державного санітарного лікаря України від 01 грудня 1999 року № 37 та враховувати:

- належні умови освітлення приміщення і робочого місця, відсутність відблисків;
- оптимальні параметри мікроклімату;
- м'яке рентгенівське випромінювання;
- наявність шуму та вібрації;
- електромагнітне випромінювання;
- ультрафіолетове та інфрачервоне випромінювання;
- електростатичне поле між екраном і оператором.

Вимоги безпеки до робочих місць працівників з екранними пристроями передбачають:

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

2. 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.

3. 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.

4. Освітлення робочого місця працівника з екранними пристроями має створювати відповідний контраст між екраном і навколишнім середовищем (з урахуванням виду роботи) та відповідати вимогам ДСанПІН 3.3.2.007-98.

5. Мікроклімат виробничих приміщень з робочими місцями працівників з екранними пристроями має підтримуватись на постійному рівні та відповідати вимогам Санітарних норм мікроклімату виробничих приміщень ДСН 3.3.6.042-99, затверджених постановою Головного державного санітарного лікаря України від 01 грудня 1999 року № 42 (далі - ДСН 3.3.6.042-99).

6. 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.

7. 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.

6.1.2 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 зовнішніх установок 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 менше 6,0 $м^2$, 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:

- працювати поблизу відкритих струмовідних частин, крім випадків, обумовлених «Вимогами охорони праці під час експлуатації електронно-обчислювальних машин».

- залишати без догляду увімкнуте в мережу живлення устаткування, прилади, що використовуються при проведенні робіт.

- залишати на устаткуванні, приладах запобіжники, з'єднувачі, провід, залишки флюсу, припою тощо.

- розміщувати на одному робочому столі (місці) два або більше увімкнутих в мережу живлення відеотермінали з знятими футлярами.

- 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.

- проводити всередині відеотерміналу операції, що виконуються однією рукою.

6.2 Безпека в надзвичайних ситуаціях

6.2.1 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.

Природне освітлення має здійснюватись через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечувати коефіцієнт природною освітленості (КПО) не нижче ніж 1,5%. Розраховується КПО за методикою, викладеною в ДБН В.2.5-28-2006.

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 застосовувати світильники таких класів світлорозподілу:

– світильники прямого світла – П;

– переважно прямого світла – Н;

– 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 запасу (Кз) відповідно до ДБН В.2.5-28-2006 для освітлювальної установки загального освітлення слід приймати рівним 1,4.

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 природного та 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.

6.2.2 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 властивості хлору є основними вражаючими чинниками при його аварійних викидах.

Комплекс заходів щодо зберігання і використання хлору включає [ ]:

- використання безпечних технологій;
- 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;

- раціональне розміщення хлору з урахуванням можливих наслідків аварій;

- 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 умов зберігання 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 в грунт 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 привести до 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:

- одягання на потерпілого промислового протигаза типу В або громадянського ДП-5, ГП-7;
- винесення потерпілого на незаражену територію і зняття протигаза;
- звільнення від тісного одягу;
- при відсутності дихання – штучне дихання, переважно методом “рот в рот”;
- вдихання, для пом’якшення подразнення, аерозолю 0,5% розчину соди, а також кисню;
- промивання шкіри і слизових оболонок 2% содовим розчином;
- рясне питво (тепла вода з содою, чай, кава);
- максимальне обмеження самостійного пересування потерпілого, подальше транспортування тільки в лежачому положенні;
- у холодну пору – відігрівання і забезпечення повного спокою;
- накласти асептичні пов’язки на рани і іммобілізувати пошкоджені кінцівки;
- евакуювати уражених у медичні пункти для надання першої лікарської допомоги та подальшого лікування.

6.3 Висновки до розділу 6

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.

7 ЕКОЛОГІЯ

7.1 Радіоекологія – один з новітніх розділів загальної екології.

Радіоекологія – це розділ загальної екології, який вивчає процеси попадання і накопичення радіоактивних речовин живими організмами, їх міграцію у біосфері, вплив іонізуючого випромінювання на екосистеми. Вона пов'язана з такими науками як: радіобіологія, радіологія, радіохімія, рентгенологія, ядерна хімія, ядерна медицина, радіаційна генетика, ядерна фізика, дозиметрія іонізуючого випромінювання. Як галузь знань радіоекологія належить до радіобіології.

У радіоекології виділяють дві основні тісно взаємопов'язані проблеми:

1. Міграція радіонуклідів у екосистемі. Фундаментальними характеристиками міграції радіонуклідів є :

– коефіцієнт накопичення;

– коефіцієнт переходу радіонуклідів з певного оточення в певні організми;

– розподіл за глибиною грунтів, на поверхню яких нанесені радіонукліди;

– коефіцієнти сорбції нуклідів детритом (перегноєм, гумусом).

2. Вплив на організми радіонуклідів, що накопичено в них. На відміну від радіобіології, радіоекологія вивчає вплив іонізуючого випромінювання не стільки на сам організм, скільки на його репродуктивні функції, тобто на здатність підтримувати чисельність популяції

Радіоактивні випромінювання дуже небезпечні, якщо перевищується допустимий їх рівень дії. Вони відносяться до факторів фізико-хімічної дії. Першим у 1895 р. дію природного радіоактивного випромінювання від мінералу, що містить сполуки урану, спостерігав французький вчений Анрі Беккерель. У цьому ж році німецький фізик К. Рентген опублікував повідомлення про Х-промені - радіоактивні промені штучного походження. Але раніше, ще у 1893 р. український вчений Іван Пулюй першим у світі вже отримав, як тепер кажуть,

рентгенівський знімок кисті руки людини. Пізніше, вже у Першій світовій війні, німці використовували так звані рентгенівські апарати.

Радіоактивні випромінювання ділять на дві групи: корпускулярні - альфа частки (α) - ядра атомів гелію (^{4}He), бета (β) - електрони (e^{-1}), або позитрони (e+), протони (P+), нейтрони (n^O) та квантові або електромагнітні випромінювання - гамма-частки (у), що мають природне - космічне випромінювання, або штучне походження. Гамма-випромінювання - це електромагнітне (квантове) природне випромінювання великої проникаючої спроможності. Рентгенівське випромінювання виникає при зіткненні бета - випромінювання з атомами важких металів. Альфа та бета випромінювання мають невелику проникаючу спроможність і тому вони гальмуються навіть такими перепонами, як одяг, папір, скло. Інші мають велику енергію і тому можуть проникати навіть через цегляні, металеві перепони. Їх можуть гальмувати товсті прошарки свинцю.

Всі радіоактивні елементи, розпадаючись, перетворюються в інші елементи через суворо визначені проміжки часу (Т), відповідно до закону радіоактивного розпаду: L=0,693/T, де L - постійна розпаду для даного елемента. Для кожного радіоактивного елемента час напіврозпаду є величина постійна і, наприклад, складає для торію 13,9 млрд років, урану - 4,51 млрд років, радію - 1617, ізотопів цезію - 137 - 30 років, кобальту - 60 - 5,3 роки.

Таким чином, знаючи вміст в певному об'єкті (скам'янілі рештки, мінерали) концентрацію радіоактивного ізотопу та період його піврозпаду, можна визначити час виникнення об'єкта. Важливими характеристиками радіоактивних речовин, випромінювань є такі параметри: активність, поглинена доза, потужність цієї дози, еквівалентна доза випромінювання і її потужність.

7.2 Робота з банками екологічної інформації

Під час розв’язування прикладних задач доводиться реалізовувати алгоритми обробки масивів даних, які є не одноманітними масивами (множинами) числових значень або текстів, а важливими струк-турними

відношеннями між елементами даних. Найпростіша струк-тура – це вектор елементів. У загальному вигляді це можуть бути дво- або n-вимірні масиви.

Дані – це факти та ідеї, подані у формалізованому вигляді для оброблення за допомогою певного процесу (алгоритму) або для передачі.

Для зручності вводу, виводу, збереження та обробки інформації в організаціях почали використовувати бази даних. Бази даних стали реальністю завдяки створеним комп'ютерам і пристроям довготермінової пам'яті, здатних зберігати у цифровій формі значні обсяги інфор-мації. Комп'ютер з допомогою відповідного програмного забезпечення дозволяє оперувати необхідною інформацією, яка є у довготерміновій пам'яті, представляти її в потрібній формі та послідовності. Вперше термін база даних з'явився ще в 1962 р.

База даних – це впорядкована сукупність спеціально організованих і логічно зв'язаних інформаційних елементів, яка відображає стан об'єктів та їх характерні параметри у предметній ділянці, що розглядається. База даних – це сукупність взаємозв'язаних даних (файлів), призначених для спільного застосування.

На відміну від простих наборів даних бази даних володіють характерними перевагами відносно організованої іншим чином інформації:

– для баз даних характерним є одноразове введення та багаторазове використання інформації, введена інформація застосовується для вирішення багатьох проблем, забезпечується її багатоцільове і сумісне використання;

– бази даних існують незалежно від конкретних прикладних програм, що забезпечує уніфікацію засобів організації даних і незалеж-ність прикладних програм від організації даних;

– бази даних володіють модельністю (структурованістю, що відображає певну предметну ділянку);

– бази даних дозволяють встановити мінімально необхідний рівень надлишковості даних (тобто дані не дублюються при їх використанні різними користувачами);

– в базі даних забезпечується дотримання стандартів представ-лення даних, що спрощує їх створення та обслуговування;

– в базах даних забезпечується централізоване управління інформаційними ресурсами, синхронна підтримка даних для всіх прик-ладень, включаючи мови запитів і засоби захисту.

Комплекс програм, які забезпечують взаємодію користувача з базою даних – це система управління базами даних (СУБД).

СУБД забезпечують вирішення таких основних завдань:

– створення бази даних;
– занесення, коректування і вилучення даних;
– упорядкування даних;
– вибір сукупності даних, що відповідають заданим критеріям;
– оформлення вихідних даних тощо.

Сукупність СУБД і бази даних – це банк даних.

До переваг підходу, який ґрунтується на концепції банку даних, належать:

– задоволення інформаційних потреб різних типів користувачів;
– вірогідність і несуперечність інформації, що зберігається;
– санкціонований доступ до даних;
– адаптація інформаційної моделі до змін предметної області;
– видача інформації у формі, встановленій користувачем;
– одноразове введення даних і багаторазове їх використання;
– можливість виключення надмірності даних, що зберігаються.

Недоліком цього підходу є необхідність великої ємності пам’яті персонального комп’ютера.

Структурні блоки будь-якої системи моніторингу формуються на основі комплексу маркерних критеріїв, які підлягають обліку та спостереженню, а також потребують корегування в необхідному напрямку. Основними блоками екологічного моніторингу є:

– стан атмосферного повітря: середньорічні та максимальні концентрації основних забруднювачів, відсоток лабораторних досліджень, що не відповідають гігієнічним стандартам (ДЕСТ);

– якість питної води: середньорічні і максимальні концентрації основних забруднювачів, кількість випадків перевищення ГДК;

– рівень забруднення ґрунтового покриву: середні і максимальні концентрації забруднювачів, кількість випадків перевищення ГДК, су-марний показник забруднення;

– архітектурно-планувальна і соціальна інфраструктура: поверховість районів міста, містобудівний баланс, віддаленість від великих об’єктів екологічного ризику (промислові площадки, звалища), транспортно-промислове навантаження, наявність об’єктів соціально-куль-турної сфери;

– ландшафтно-екологічні умови: висотність і неоднорідність рельєфу, мікрокліматичні характеристики і потенціал самоочищення атмосфери, глибина залягання ґрунтових вод і наявність зон підтоплення.

Блок параметрів нормативно-довідкової інформації:

– чисельність населення контрольованих районів міста;

– ГДК забруднюючих речовин;

– перелік підприємств, які забруднюють навколишнє середовище.

Залежно від мети і завдань спостережень, система екологічного моніторингу може містити блок параметрів стану біотичних компонентів екосистем, блок параметрів стану здоров’я населення тощо.

Формування банку даних для екологічного моніторингу потребує залучення інформації медичних, природоохоронних, гігієнічних, містобудівних служб, ландшафтно-функціонального картографування, експертно-статистичного оцінювання.

7.3 Висновки до розділу 7

В розділі наведено відомості по радіоекології та роботі з банками екологічної інформації

ВИСНОВКИ

Процес інтенсивного розвитку і впровадження обчислювальної техніки, систем і мереж, що використовують протоколи глобальних інформаційних систем в усі сфери життєдіяльності сучасного суспільства , значно збільшив обсяг послуг , що надаються сервісами всесвітньої мережі Інтернет , але також примножив ризики виникнення кіберзлочинів, пов'язаних з порушенням безпеки інформації в комунікаційних системах.

Незважаючи на широке застосування комплексних систем захисту інформації (КСЗІ), більш досконалих систем забезпечення інформаційної безпеки комунікаційних систем, актуальною проблемою залишається достовірне оцінювання легітимності виконуваних операцій. Особливо гострою дана проблема є для комунікаційних систем, що забезпечують національну безпеку держави (військові системи, системи подвійного призначення, економічні, комунікаційні системи і ін.). Важлива роль при вирішенні викладеної проблеми відводиться системам виявлення атак (СВА).

Важливу роль в процесі класифікації кібератак грають вхідні дані. За основу вхідних тестових даних доцільним вбачається застосування загальнодоступної бази даних NSL-KDD, що не містить надлишкових записів і дає більший відсоток виявлення атак порівняно до KDD - 99. Такий підхід дозволять отримувати кількісну характеристику кібератак.

Для отримання якісної оцінки кібератак і їх подальшої класифікації, пропонується застосувати відому просторі ознак класифікацію. Такий підхід дозволить розширити простору ознак для опису невідомих класів кібератак.

Кібератаки, які класифікуються за ознаковим принципом, можуть у кожному конкретному випадку при визначенні загального класу містити не лише одну, а більше компонент за будь-якою з вище перелічених базових ознак. Запропонований класифікатор загроз забезпечує можливість формування єдиного підходу щодо визначення загрози та її врахування під час виявлення

аномальної роботи, або відхилення від нормальної роботи в середовищі безпровідних мереж на прикладі АБС.

БІБЛІОГРАФІЯ

1. Бурячок В. Л. Політика інформаційної безпеки [Текст] : підручник / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко ; під заг. ред. проф. В. О. Хорошка. – К. : ПВП «Задруга», 2014. – 222 с.

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

3. ГОСТ 34.310-95. Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма [Текст]. – К.: Госстандарт Украины, 1998.

4. ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хеширования [Текст]. – К.: Госстандарт Украины, 1998.

5. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма [Текст]. – Национальный стандарт.

6. Евсеев С.П. Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины/ С.П. Евсеев// Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 3, p. 297 – 309.

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

8. ДСТУ 7564–2014. Інформаційні технології. Криптографічний захист інформації. Функція ґешування [Текст]. – К. : Держстандарт України, 2014. – 39 с.

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

10. Евсеев С.П. Анализ законодательной базы к системе управления инфор-мационной безопасностью НСМЭП / С.П. Евсеев, О.Г. Король, Г.П. Коц. // Восточно-европейский журнал передовых технологий. – Харьков. – 2015. – Вып. 5/3(77). – С. 48–59.

11. Евсеев С.П. Анализ защиты в национальной системе масовых электронных платежей // Інформаційна безпека. – 2014. – № 3(15), № 4 (16) – С. 15– 28.

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

13. Корченко А. А. Банківська безпека [Текст] / А. А. Корченко Л. Н. Скачек В. А. Хорошко. – Київ, 2014. – 185 с.

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) [Текст]. – К.: НБУ., 2010. – 67 с.

15. Ярочкин В. И. Информационная безопасность [Текст]: учебник / В. И. Ярочкин; 2-е изд. – М.: Академический Проект; Гаудеамус, 2004. – 544 с.

16. Security of Internet Banking - A Comparative Study of Security Risks and Legal Protection in Internet Banking in Thailand and Germany [Electronic resource]. – Available at: http://www.thailawforum.com/articles/internet-banking-thailand.html. Accessed on: Des. 09, 2019.

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

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

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

20. Національний Банк України. Платіжна організація національної системи масових електронних платежів. [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/va119500-08. Accessed on: Des. 09, 2019.

21. Ревенков П. В. Защита информации в банке: основные угрозы и борьба с ними [Електронний ресурс] / П. В. Ревенков. – Режим доступа: http://www.crmdaily.ru/novosti-rynka-crm/568-zashhita-informacii-v-banke-osnovnye-ugrozy-i-borba-s-nimi.html. Accessed on: Des. 09, 2019.

22. Симаков М. Н. V Съезд директоров по информационной безопасности [Електронний ресурс] / М. Н. Симаков. – Москва, 2012. – Режим доступу: http://www.cso-summit.ru/data/2012/presentations/cso2012_013_express-tula_simakov.pdf. Accessed on: Des. 09, 2019.

23. Слободенюк Д. Банковские технологии, Средства защиты информации в банковских системах [Електронний ресурс] / Д. Слободенюк. – 2013. – Режим доступа:http://www.arinteg.ru/about/publications/press/sredstva-zashchity-informatsii-v-bankovskikh-sistemakh-131107.html. Accessed on: Des. 09, 2019.

24. Старинський М. В. Щодо визначення поняття “банківська інформація” та виділення її видів / [Електронний ресурс]. – Режим доступу: uabs.edu.ua/images/.../K.../Starinskii_s_015.pdf. Accessed on: Des. 09, 2019.

25. Химка С. С. Разработка моделей и методов для создания системы информационной безопасности корпоративной сети предприятия с учетом различных критериев [Електронний ресурс] / С. С. Химка. – Режим доступа: http://masters.donntu.org/2009/fvti/khimka/diss/index.htm. Accessed on: Des. 09, 2019.

26. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375. Accessed on: Des. 09, 2019.

27. С. Евсеев, “Синергетическая модель оценки безопасности банковской информации”, Науково-технічний журнал “Інформаційна безпека”, № 4 (24), с. 104 – 118, 2016.

28. Hryshchuk R., Yevseiev, S. Shmatko A. Construction methodology of information security system of banking information in automated banking systems: monograph, 284 p., Vienna.: Premier Publishing s. r. o., 2018.

29. Банк данных угроз безопасности информации. [Электроний ресурс]. Доступно : http://bdu.fstec.ru/vul. Дата обращения: Декабрь, 5.2019.

30. О. К. Юдін, та С. С. Бучик, “Класифікація загроз державним інформаційним ресурсам нормативно-правового спрямування. Методологія побудови класифікатора”, Захист інформації, Том 17 (2), с. 108 – 116, 2015.

31. ISO/IEC 18045:2014 Information technology – Security techniques – Guidelines for cybersecurity [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46412. Accessed on: Des. 09, 2019.

32. Д. Домарєв, В. Домарєв та С. Прокопенко, “Методика оцінювання захищеності інформаційних систем за допомогою СУІБ “Матриця”, Захист інформації, том 15, №1, с. 80 – 86, 2013.

33. С. В. Павленко, “Метод оцінки захищеності інформаційних систем”, Системи озброєння і військова техніка, № 4(20), с. 149 – 154, 2009.

34. Корченко О.Г. Системи захисту інформації: Монографія / Корченко О.Г. - К.: НАУ, 2004. – 264 с.

35. Олифер Н. Организация защищенного канала с помощью AH, ESP и IKE / Н. Олифер // Журнал сетевых решений/LAN. 2001. – № 03 [Электронный ресурс] – Режим доступа : http://www.osp.ru/lan/2001/03/134690/. Accessed on: Des. 09, 2019.

ДОДАТКИ