МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Циклова комісія *комп'ютерних систем та мереж*
(повна назва циклової комісії)

Допустити до захисту
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
(підпис) *Ірина КРАВЧУК* (ім'я, ПРІЗВИЩЕ)
« 16 » 06 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
ФАХОВИЙ МОЛОДШИЙ БАКАЛАВР

Тема: *Безпека персональних даних на підприємстві*

Група: *3-013* Спеціальність: *123 «Комп'ютерна інженерія»*

Здобувач освіти (підпис) *Анатолій БАЛАБАНОВ* (ім'я, ПРІЗВИЩЕ)

Керівник роботи (підпис) *Владислав СОБЧУК* (ім'я, ПРІЗВИЩЕ)

Консультант з оформлення пояснювальної записки (підпис) *Оксана ОСАДЧА* (ім'я, ПРІЗВИЩЕ)

Кривий Ріг 2025 р.

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Відділення *комп'ютерної та програмної інженерії*
Циклова комісія *комп'ютерних систем та мереж*
Освітній ступінь *фаховий молодший бакалавр*
Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
(підпис) *Ірина КРАВЧУК* (ім'я, ПРІЗВИЩЕ)
« *01* » *03* 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ОСВІТИ

Балабанову Анатолію Анатолійовичу
(прізвище, ім'я, по батькові)

1.Тема роботи *Безпека персональних даних на підприємстві*

Керівник роботи *Собчук Владислав Олегович*
викладач
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по коледжу від « *04* » *04* 2025 року № *50-ст*

2. Строк подання здобувачем освіти роботи з *01.03.2025* по *15.06.2025*

3. Вихідні дані до роботи *Нормативно-правова база. Міжнародні стандарти та регламенти. Дані про поточний стан підприємства*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз загроз інформації в сучасних комп'ютерних системах та мережах.
Технічний аналіз та запобігання спаму: деструктивні процедури.
Технології захисту інформації від шкідливих програм та програмних загроз.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Презентація Microsoft PowerPoint

6. Консультанти розділів роботи (проекту)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	*Узгодження технічного завдання*	*01.03.2025*	
2	*Огляд літератури по темі*	*15.03.2025*	
	кваліфікаційної роботи		
3	*Аналіз загроз інформації в сучасних*	*28.04.2025*	
	комп'ютерних системах та мережах		
4	*Технічний аналіз та запобігання спаму:*	*14.05.2025*	
	деструктивні процедури		
5	*Технології захисту інформації від шкідливих*	*26.05.2025*	
	програм та програмних загроз		
6	*Оформлення пояснювальної записки*	*06.06.2025*	
7	*Захист кваліфікаційної роботи*		

Здобувач освіти _____ *Анатолій БАЛАБАНОВ*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Владислав СОБЧУК*
(підпис) (ім'я, ПРІЗВИЩЕ)

StrikePlagiarism.com

Дата звіту 6/4/2025
Дата редагування ---

Документ прийнятий

Звіт подібності

метадані

Назва організації
Ukrainian national aviation university
Заголовок
Балабанов А_3-013_2025_КПІ
Автор Науковий керівник / Експерт
БалабановГринченко О
підрозділ
Криворізький Фаховий коледж

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

КП 1

КЦ

25	11633	93403
Довжина фрази для коефіцієнта подібності 2	Кількість слів	Кількість символів

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Безпека персональних даних на підприємстві» викладена на 66 с., містить 7 рис., 18 використаних літературних джерел.

ФЛУД, ETHERNET, LAN, TELNET, FTP, ВЕРИФІКАЦІЯ, БРАУЗЕР, АНТИ СПАМ, E-MAIL, DOS-АТАКИ, СПАМ

Тема кваліфікаційної роботи пов’язана з організацією захисту інформаційних комп’ютерних мереж від СПАМ, зокрема, аналізу та проектуванню систем та розробці технологій захисту інформаційних комп’ютерних мереж від СПАМ.

Об’єктом дослідження являються інформаційні комп’ютерні мережі та глобальна комп’ютерна мережа *Internet*.

Метою роботи є аналіззагрозінформаційних ресурсів комп’ютерних мереж, аналіз технологій анти-СПАМ, а також проектування та розробка систем захисту інформації комп’ютерних мереж від деструктивних програм.

Інструментальним засобом перевірки трафіку є аналізатора трафіка мережних протоколів *IP* – мережі - " Сніфер".

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА ТЕРМІНІВ

АІБ – Автоматизована інформаційна безпека

ДІБ – Департамент інформаційної безпеки (гіпотетично, якщо згадується структура підприємства)

ІБ – Інформаційна безпека

ІКС – Інформаційно-комунікаційна система

ІТ – Інформаційні технології

КЗІ – Комплексна система захисту інформації

КСЗІ – Комплексна система захисту інформації

ПЗ – Програмне забезпечення

РРО – Реєстратор розрахункових операцій (якщо актуально для підприємства)

СУІБ – Система управління інформаційною безпекою

ТЗІ – Технічний захист інформації

ЦОВВ – Центральні органи виконавчої влади (як регулятори)

ЦОД – Центр обробки даних (*Data Center*)

GDPR – General Data Protection Regulation (Загальний регламент про захист даних ЄС)

ISO/IEC 27001 – *International Organization for Standardization* / *International Electrotechnical Commission* 27001 (Міжнародний стандарт систем управління інформаційною безпекою)

NIST – National Institute of Standards and Technology (Національний інститут стандартів і технологій США)

CRM – Customer Relationship Management (Система управління відносинами з клієнтами)

VPN – Virtual Private Network (Віртуальна приватна мережа)

MFA / 2*FA – Multi-Factor Authentication* / *Two-Factor Authentication* (Багатофакторна автентифікація / Двофакторна автентифікація)

ВСТУП

Сьогодні комп'ютерні мережі – це не просто інструмент, а життєво важлива інфраструктура, що інтегрує виробництво, споживання та всі аспекти нашого повсякденного життя. Завдяки їхній постійно зростаючій обчислювальній потужності та телекомунікаційним можливостям, ми щодня користуємося такими сервісами, як відеоконференції, *IP*-телефонія, хмарні обчислення, віртуальна та доповнена реальність, а також безліччю інших інноваційних застосунків. Усі ці технології базуються на пакетній комутації – фундаментальному принципі, що дозволяє ефективно передавати дані через мережу.

Сукупність передових інформаційних технологій, мережевого обладнання, протоколів передачі даних та засобів управління формує сучасну розподілену інфраструктуру – інтегроване середовище для обробки, зберігання та передачі даних. Ця інфраструктура є основою для функціонування "розумних" міст, Інтернету речей (*IoT*), систем штучного інтелекту та інших передових рішень. Загрози кібербезпеки у цифрову епоху

Попри всі переваги, зростаюча залежність від комп'ютерних мереж робить нас вразливими до кібератак. ЗМІ регулярно повідомляють про інциденти, пов'язані з кіберзлочинністю, витоками даних та комп'ютерними вторгненнями. Визначити та класифікувати таку поведінку складно, адже інформація існує у безлічі форм – від окремих файлів та записів у базах даних до цілих програмних комплексів. Усі ці інформаційні об'єкти можуть стати мішенню для зловмисників.

Інформаційна атака – це навмисне порушення встановлених правил використання інформації, визначених її власником або уповноваженою особою. Зі стрімким збільшенням обсягів інформації, що зберігається в електронному вигляді, та розвитком мережевих технологій, навіть фізичний доступ до комп'ютера вже не є гарантією безпеки даних.

Наслідки інформаційних атак

Кібератаки можуть мати руйнівні наслідки для бізнесу та суспільства:

1. Фінансові збитки: Витік конфіденційної бізнес-інформації може призвести до значних прямих фінансових втрат, зокрема на конкурентних ринках. 2. Репутаційні ризики: Широкомасштабні витоки даних серйозно підривають довіру клієнтів та партнерів, завдаючи непоправної шкоди репутації компанії. 3. Втрата конкурентних переваг: Крадіжка критично важливої інформації може бути використана конкурентами, що в кінцевому підсумку може призвести до банкрутства компанії.

4. Операційні збої: Маніпуляції з внутрішньою інформацією підприємства під час передачі чи зберігання можуть спричинити величезні збитки та паралізувати діяльність.

5. Втрата довіри клієнтів: Кілька успішних атак на провайдерів інформаційних послуг знижують довіру споживачів до компанії, що прямо впливає на її доходи.

Причини пошкодження та винуватці кіберінцидентів

Причини пошкодження електронної інформації різноманітні. За статистикою, значний відсоток припадає на ненавмисні людські помилки (до 52%). Також вагомими факторами є навмисна людська поведінка (10%), відмови обладнання (10%), а також фізичні пошкодження, такі як пожежі (15%) та затоплення (10%). Важливо зазначити, що кожен десятий випадок пошкодження електронних даних пов'язаний саме з комп'ютерними атаками.

Щодо винуватців кіберінцидентів, статистика показує, що значна частина атак (до 81%) здійснюється чинними співробітниками установ. Лише 13% випадків припадає на повністю зовнішніх осіб, а 6% – на колишніх співробітників. Це підкреслює важливість внутрішньої політики безпеки та управління доступом.

Водночас, основні мотиви зловмисників розподіляються наступним чином: - 44% випадків зламу стосувалися прямої крадіжки коштів з електронних рахунків.

- 16% – деактивація програмного забезпечення.

- Не менш поширеною була крадіжка інформації з різними наслідками (16%). - 12% – фальсифікація інформації.

- 10% – використання зловмисником комп’ютера для особистих потреб або замовлення послуг, до яких він не мав права доступу.

Саме тому сучасні системи захисту інформації в комп'ютерних мережах мають бути максимально надійними та забезпечувати три ключові принципи: конфіденційність, цілісність та доступність інформаційних ресурсів. Розробка та вдосконалення технологій для забезпечення доступності інформації в комп'ютерних мережах залишається надзвичайно актуальною задачею у світі, де цифрові дані є однією з найцінніших валют.

РОЗДІЛ 1
АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЇ В СУЧАСНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

1.1 Загрози інформації в комп'ютерних мережах

У сучасному світі інформація є одним з найцінніших активів для будь-якого бізнесу та особистості. Користувачі цифрових систем прагнуть захистити свої дані від несанкціонованого доступу, викрадення, копіювання, спотворення чи знищення. Ігнорування цих загроз може призвести до значних економічних,
соціальних та репутаційних втрат.

Захист інформації стає все більш складним завданням через повсюдне поширення комп'ютерних мереж, географічно розподілених систем та хмарних сервісів, що дозволяють віддалений доступ до спільних ресурсів.

Основні фактори, що впливають на безпеку систем, можна розділити на дві категорії:

1. Фізичні та екологічні впливи: Сюди відносяться ризики для фізичної інфраструктури розподілених систем, що можуть змінюватися з часом. 2. Несанкціонований доступ: Це вплив на структуру, функції керування компонентами системи та взаємодію між різними механізмами безпеки. Фізична безпека зазвичай пов'язана з контролем електромагнітного випромінювання від мережевих каналів та вузлових пристроїв, а також забезпеченням безперервності зв'язку в умовах

різноманітних перешкод. Ці перешкоди можуть виникати з таких причин:

- Природні та техногенні катастрофи: Повені, урагани, землетруси, пожежі, збої в електромережі, кібератаки на критичну інфраструктуру.
- Відмови та несправності обладнання: Збої серверів, мережевого обладнання, систем зберігання даних.
- Операційні помилки: Помилки користувачів, адміністраторів, операторів (людський фактор).

- Помилки в проєктуванні та розробці: Вразливості в апаратних засобах, програмному забезпеченні, архітектурі даних, технологіях обробки інформації, які були допущені на етапі створення.

Ще одним вагомим аргументом на користь підвищення уваги до кібербезпеки є стрімкий розвиток і поширення шкідливого програмного забезпечення (ШПЗ), такого як комп'ютерні віруси, трояни, *ransomware, spyware* тощо. Це програмне забезпечення може таємно проникати в систему та виконувати різноманітні несанкціоновані операції.

Сучасні тенденції у кіберзагрозах (Приклад оновленої статистики) Щоб краще зрозуміти актуальність проблеми, розглянемо поточні тенденції у кіберзагрозах. Наприклад, за даними досліджень, у певний період (наприклад, у першому кварталі 2024 року) спам та фішинг продовжували становити значну частку електронного трафіку, сягаючи в середньому 75-85% від загального обсягу електронних листів.

Розподіл тематики спаму постійно змінюється, відображаючи актуальні події та прагнення зловмисників. Зростає частка повідомлень, пов'язаних з: - Криптовалютами та інвестиціями: Привабливі, але часто шахрайські пропозиції.

- Фейковими повідомленнями від державних установ або банків: Фішинг для викрадення облікових даних.
- "Розумним" фішингом: Спрямованим на конкретних осіб або організації (*spear phishing*).

Одночасно може спостерігатися зниження кількості традиційних категорій, таких як "Фармацевтика" або "Спам для дорослих", що свідчить про адаптацію

спамерів до більш витончених та цілеспрямованих методів.

Особливості мережевих атак

Ключовою особливістю будь-якої мережевої системи є розподілене розміщення її компонентів у просторі. Зв'язок між цими компонентами відбувається як фізично (через мережеві кабелі – оптоволокно, вита пара; бездротові технології – *Wi-Fi*, 5*G*), так і програмно (через механізми обміну

повідомленнями та протоколи). Усі дані та керуючі повідомлення передаються через мережеві з'єднання у вигляді пакетів.

Окрім традиційних "локальних" атак, що відбуваються в межах однієї комп'ютерної системи, мережеві системи особливо вразливі до кібератак (або віддалених атак). Їхніми основними характеристиками є:

1. Географічна віддаленість зловмисника: Атакувальник може перебувати за тисячі кілометрів від цілі, що значно ускладнює його ідентифікацію та затримання. 2. Атака на передачу даних: Атака може бути спрямована не на конкретний фізичний комп'ютер, а на інформацію, що передається через мережеві з'єднання, або на самі мережеві протоколи.

Зі стрімким розвитком локальних і глобальних мереж (таких як Інтернет) віддалені атаки стали домінуючими як за кількістю спроб, так і за рівнем успішності. Тому забезпечення кібербезпеки в боротьбі з мережевими атаками стало критично важливим.

Під віддаленими атаками зазвичай розуміють цілеспрямовані дії, спрямовані на порушення роботи розподілених систем, викрадення або спотворення інформації, що передається каналами зв'язку. Це визначення охоплює дві фундаментальні характеристики мережевих систем – розподіл комп'ютерів та розподіл інформації.

Віддалені атаки можна поділити на два основні підтипи:

- Віддалені атаки на інфраструктуру та мережеві протоколи: Спрямовані на систему, що організовує зв'язок між мережевими об'єктами (маршрутизатори, комутатори, *DNS*-сервери, *VPN*-сервери) та протоколи, що забезпечують передачу даних (*TCP*/*IP*, *HTTP*, *DNS*).

- Віддалені атаки на операційні системи та застосунки: Націлені на програмне

забезпечення, що працює на віддалених комп'ютерах та забезпечує взаємодію з мережею (веб-сервери, бази даних, клієнтські застосунки, операційні системи).

Вплив шкідливого програмного забезпечення (ШПЗ) на функціональність мережі

Комп'ютерний вірус (від англ. *Computer Virus*) – це лише один з видів шкідливого програмного забезпечення. Сучасне ШПЗ набагато різноманітніше і включає:

- Трояни: Програми, що маскуються під легітимне ПЗ, але виконують шкідливі дії (крадіжка даних, надання віддаленого доступу).
- Віруси: ШПЗ, що самовідтворюється, прикріплюючись до інших програм або документів.
- Хробаки: ШПЗ, що самостійно поширюється мережами без участі користувача.
- Програми-вимагачі (*Ransomware*): Шифрують дані користувача і вимагають викуп за їх розшифровку.
- Шпигунське ПЗ (*Spyware*): Збирає інформацію про користувача без його відома.
- Руткіти (*Rootkits*): Приховують свою присутність та діяльність зловмисника в системі.
- Ботнети: Мережі скомпрометованих комп'ютерів, що використовуються для скоординованих атак.

ШПЗ може завдати значної шкоди: знищення та крадіжка даних, зниження продуктивності комп'ютера, повне блокування доступу до системи. Для захисту від ШПЗ критично важливо:

- Регулярно оновлювати операційні системи та програмне забезпечення для закриття виявлених вразливостей.
- Використовувати сучасні антивірусні та антивірусні програми та підтримувати їх в актуальному стані.
- Бути обережними з файлами, отриманими з невідомих джерел, особливо з вкладеннями в електронних листах або завантаженими з ненадійних сайтів. -

Застосовувати фільтри для спаму та фішингу.

- Регулярно створювати резервні копії важливих даних.

Динаміка зростання атак на комп'ютерні мережі

На жаль, тенденція до зростання кількості та складності атак на комп'ютерні мережі зберігається. Це можна ілюструвати гіпотетичним графіком рис. 1.1. Цей графік є ілюстративним і відображає загальну тенденцію до зростання кібератак, а не конкретні статистичні дані, які можуть змінюватися в залежності від джерела та методології.

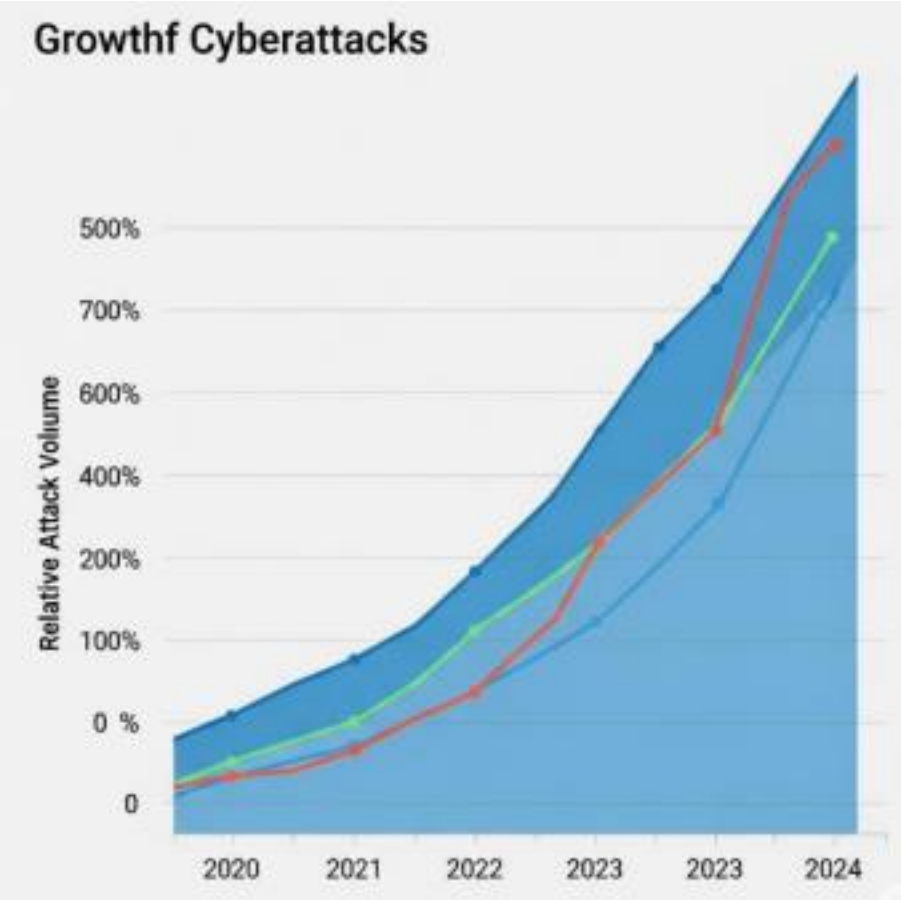

Рисунок 1.1 - Динаміка зростання кількості кібератак у 2020-2024 роках

Класифікація ШПЗ: Сучасні критерії

Раніше класифікація вірусів була доволі простою. Сьогодні, з еволюцією загроз, вона стала складнішою. Проте, ми можемо оновити деякі ключові критерії: За місцем "проживання" та розповсюдження:

- Файлові: Ті, що прикріплюються до виконуваних файлів (*exe*, *com*, *dll*), скриптів, а також документів, що містять макроси.

- Завантажувальні: Ті, що заражають завантажувальні сектори дисків.

- Мережеві (мережеві хробаки, ботнети): Ті, що поширюються активно через комп'ютерні мережі, експлуатуючи вразливості або використовуючи соціальну інженерію (фішинг, спам).

- Макровіруси: Ті, що заражають документи додатків *Microsoft Office* (*Word, Excel, PowerPoint*) та інші офісні формати, що підтримують макроси. - Веб-скриптові: Ті, що вбудовуються у веб-сторінки та виконуються браузером користувача.

За механізмом зараження та перебування в пам'яті:

- Резидентні: Ті, що після запуску залишаються в оперативній пам'яті та можуть заражати нові об'єкти (файли, диски) або перехоплювати системні виклики. - Нерезидентні: Ті, що активні лише протягом короткого періоду часу, виконуючи свої шкідливі дії та не залишаючись у пам'яті.

За функціоналом та ступенем небезпеки:

- Нешкідливі/*Low-impact*: Ті, що не впливають на роботу комп'ютера або завдають мінімальних незручностей (наприклад, зміна розміру файлу, виведення повідомлень без шкоди).

- Малонебезпечні/*Moderate-impact*: Дії, що порушують роботу системи, але не призводять до втрати даних чи серйозних збоїв (наприклад, періодичні перезавантаження, сповільнення роботи, невеликі зміни в інтерфейсі).

- Небезпечні/*High-impact*: Ті, що пошкоджують файли, призводять до частих "збоїв" системи, видалення програм або даних.

1.2 Технології захисту інформації в комп'ютерних мережах

Сучасні системи захисту інформації в комп'ютерних мережах еволюціонували, але їхні базові принципи залишаються актуальними. Аналіз вітчизняних та світових практик показує, що ефективні рішення базуються на таких ключових підходах:

1. Системний підхід: Захист інформації не є окремим завданням, а інтегрується в усі етапи життєвого циклу інформаційної системи. Це означає

врахування всіх взаємозалежних елементів, умов та факторів (як внутрішніх, так і зовнішніх) на етапі проєктування та протягом усього функціонування системи. 2. Комплексність та ешелонована оборона: Створення багатошарової системи захисту, що поєднує різноманітні заходи, методи та засоби. Важливо уникати "слабких ланок" між компонентами системи, щоб уникнути єдиної точки відмови. 3. Безперервність захисту: Заходи безпеки застосовуються постійно, починаючи з найперших етапів проєктування та розробки системи, продовжуючись протягом її експлуатації та навіть після виведення з експлуатації (наприклад, безпечне знищення даних).

4. Диференційований захист: Заходи безпеки адаптуються залежно від чутливості інформації, потенційних ризиків, ймовірності виникнення та потенційних наслідків загроз. Критичні дані потребують найвищого рівня захисту.

5. Зручність використання: Засоби захисту повинні бути інтуїтивно зрозумілими та не вимагати від користувачів глибоких технічних знань або виконання складних, рутинних операцій. Надмірна складність може призвести до обходу механізмів безпеки або їх ігнорування.

6. Гнучкість та адаптивність: Системи захисту повинні бути гнучкими для адаптації до мінливого ландшафту загроз, нових технологій та змін у бізнес процесах.

7. Принципи самозахисту та конфіденційності: Сама система захисту повинна бути захищеною. Це включає контроль її цілісності, можливість керування безпекою через спеціалізовані модулі (наприклад, *SIEM*-системи) та здатність до відновлення у разі пошкодження або збою обладнання.

8. Обґрунтована адекватність та прозорість: Створити абсолютно невразливу систему захисту принципово неможливо. Важливо визначити оптимальний (адекватний) рівень захисту, який забезпечує прийнятний баланс між витратами, ризиками та потенційними збитками. Це завдання вирішується через комплексний аналіз ризиків.

Основні механізми захисту інформації

Системи захисту, побудовані відповідно до цих принципів, зазвичай

використовують такі ключові механізми:

- Виявлення вторгнень та аномалій: Моніторинг мережевого трафіку та системних подій для виявлення підозрілої поведінки, що може свідчити про спробу вторгнення або вже активну атаку (систем *IDS/IPS, NTA*).

- Логування та аналіз подій (*SIEM*): Збір, агрегація та аналіз журналів подій з різних джерел у системі для виявлення закономірностей, виявлення інцидентів та проведення розслідувань.

- Ідентифікація, автентифікація та авторизація (IAA):

  - Ідентифікація: Процес присвоєння унікального імені або ідентифікатора суб'єкту (користувачу, пристрою, програмі).

  - Автентифікація: Перевірка справжності заявленого ідентифікатора (за допомогою паролів, біометричних даних, багатофакторної автентифікації тощо).

  - Авторизація: Розподіл прав доступу та повноважень до системних ресурсів після успішної автентифікації.

- Контроль доступу: Механізми, що визначають, хто, до чого і яким чином може отримувати доступ у системі (наприклад, на основі ролей, атрибутів, політик).

- Контроль цілісності: Забезпечення незмінності та достовірності системних ресурсів (файлів, конфігурацій, баз даних) від несанкціонованих модифікацій.

Механізми контролю доступу до ресурсів

Механізм контролю доступу до спільних системних ресурсів є одним з найважливіших факторів у розробці заходів безпеки. Існує чотири основні способи розподілу прав доступу:

1. Фізичний доступ: Суб'єкти отримують фізичний доступ до різних об'єктів (наприклад, доступ до певних серверних кімнат, окремих пристроїв, даних на різних носіях).

2. Часовий доступ: Різні суб'єкти з різними правами доступу до об'єкта отримують доступ у різні проміжки часу або за певним графіком. 3. Логічний доступ

(контекстний): Суб'єкти отримують доступ до спільних об'єктів у межах одного операційного середовища, але під керуванням інструментів розділення доступу, що емулюють віртуальні середовища. Це дозволяє гнучко управляти доступом на основі ролей, атрибутів або політик.

4. Шифрування: Усі об'єкти зберігаються або передаються в зашифрованому вигляді, а права доступу визначаються наявністю відповідного криптографічного ключа, що дозволяє розшифрувати об'єкт.

Запобігання несанкціонованому доступу (НСД)

Боротьба з несанкціонованим доступом є комплексним завданням. Існують два основні підходи, які найкраще працюють у поєднанні:

1. Виявлення НСД: Моніторинг та фіксація фактів несанкціонованого доступу до інформації (наприклад, модифікація даних, файлів, програм, несанкціоноване копіювання).

2. Блокування НСД: Превентивні дії, що блокують такий доступ шляхом аналізу непрямих ознак (виявлення підозрілих процесів, спроб зміни вмісту пам'яті, реєстрації нових користувачів з нетипових місць або у нетиповий час).

Стандартні методи запобігання доступу до інформації в комп'ютерній мережі: 1. Контроль доступу (*Access Control*): Застосування правил та механізмів, що визначають, хто може отримати доступ до ресурсів і які дії він може виконувати. Це включає списки контролю доступу (*ACL*), рольові моделі доступу (*RBAC*), атрибутивні моделі доступу (*ABAC*).

2. Посилений захист паролем/Багатофакторна автентифікація (*MFA*): Використання складних паролів, регулярна їх зміна, а також впровадження *MFA,* що вимагає кілька типів підтвердження особи (наприклад, пароль + код з телефону).

3. Шифрування (*Encryption*): Перетворення інформації у нечитабельний вигляд для захисту її конфіденційності під час зберігання та передачі. Це включає шифрування дисків, файлів, мережевого трафіку (*VPN*, *SSL*/*TLS*).

4. Брандмауери (*Firewalls*) та мережеві сегментація: Пристрої або програмне забезпечення, що контролюють вхідний та вихідний мережевий трафік на основі встановлених правил безпеки. Мережева сегментація дозволяє розділити мережу на

ізольовані зони для обмеження поширення потенційних атак.

Сучасні засоби та основні функції системи захисту інформації

Засоби захисту інформації на сучасному ринку можна розділити на кілька основних категорій:

- Апаратні засоби захисту:
  - Активні: Призначені для протидії витоку інформації через фізичні канали (наприклад, системи активного придушення електромагнітного випромінювання, пристрої для захисту від НСД до обладнання).
  - Пасивні: Забезпечують фізичну безпеку без активного впливу (наприклад, екрановані приміщення, системи контролю та управління доступом до об'єктів).
- Програмно-апаратні комплекси (ПАК):
  - Управління доступом та автентифікація: Апаратні токени, смарт-карти, біометричні системи, що забезпечують посилену ідентифікацію та автентифікацію користувачів.
  - Мережева безпека: Брандмауери наступного покоління (*NGFW*), системи запобігання вторгненням (*IPS*), шлюзи безпеки, *VPN*-шлюзи для захисту мережевого трафіку.
  - Захист даних: Апаратні модулі безпеки (*HSM*) для криптографічних операцій, шифрування дискових підсистем.
  - Захист кінцевих точок (*Endpoint Detection and Response - EDR*): Інтегровані рішення, що поєднують антивірусний захист, моніторинг поведінки, аналіз вразливостей на кінцевих пристроях.
- Програмні засоби захисту:
  - Антивірусне та антишкідливе ПЗ (*Anti-Malware*): Захист від вірусів, троянів, програм-вимагачів та інших видів ШПЗ.

  - Системи виявлення та запобігання вторгнень (*IDS*/*IPS*): Програмні рішення для моніторингу мережевого трафіку та системних подій на наявність ознак

атак.

- Системи управління інформаційною безпекою та подіями (*SIEM*): Збір, аналіз та кореляція подій безпеки з різних джерел.
- Системи запобігання витокам даних (*DLP*): Моніторинг та контроль передачі конфіденційної інформації за межі організації.
- Управління вразливостями та патчами (*Vulnerability Management*): Системи для сканування на наявність вразливостей та управління процесом встановлення оновлень.
- Захист веб-застосунків (*WAF*): Спеціалізовані брандмауери для захисту веб-додатків від атак.
- Організаційні та фізико-хімічні засоби:
- Організаційні політики та процедури: Розробка та впровадження політик інформаційної безпеки, навчання персоналу, плани реагування на інциденти.
- Фізико-хімічні засоби (наприклад, для фізичної безпеки документів): Засоби для захисту документів від підробки (голограми, спеціальні чорнила), безпечні сейфи, системи контролю доступу до приміщень, відеоспостереження.

Ці принципи та технології є фундаментом для створення стійкої та адаптивної системи кібербезпеки в сучасному цифровому середовищі.

РОЗДІЛ 2
ТЕХНІЧНИЙ АНАЛІЗ ТА ЗАПОБІГАННЯ СПАМУ: ДЕСТРУКТИВНІ ПРОЦЕДУРИ

2.1 Технологія спаму та його сучасні форми

Спам (від англ. *spam*) – це небажані, масові, часто анонімні повідомлення, що надсилаються користувачам без їхньої згоди. Переважно спам стосується рекламних розсилок, але його спектр значно ширший і включає різні форми шкідливого контенту.

Термін "спам" увійшов у широке вжиток у 1990-х роках, коли почалася

неконтрольована розсилка рекламних оголошень у групи новин *Usenet* та на електронні дошки оголошень, що не відповідали їхній тематиці. Сьогодні спам еволюціонував, адаптуючись до нових комунікаційних каналів та технологій.

Класифікація спаму в сучасних умовах

Сучасний спам можна класифікувати за основними цілями:

1. Комерційна реклама (найпоширеніший вид):

- Просування товарів/послуг: Компанії (або спеціалізовані спам-агентства) використовують спам для охоплення широкої аудиторії за мінімальних витрат. Попри активізацію законодавчої боротьби, повністю викорінити цей вид спаму складно через транскордонний характер інтернету та різницю в законодавствах різних країн.

- "Сірі" та нелегальні товари/послуги: Спам активно використовується для реклами заборонених товарів (наприклад, наркотики, зброя) або контенту (порнографія, азартні ігри), які не можуть бути просунуті через легальні рекламні канали.

2. Шахрайські схеми:

- "Нігерійські листи" (схеми авансового платежу): Класичний вид шахрайства, коли жертві обіцяють значну суму грошей (спадщина, виграш у лотерею, кошти від "таємних" угод) в обмін на невеликий авансовий платіж

(наприклад, для "оформлення документів" або "банківських комісій"). Кошти ніколи не повертаються, а жертва втрачає свої гроші.

- Фішинг (*Phishing*): Метод шахрайства, спрямований на викрадення конфіденційних даних (логінів, паролів, номерів банківських карток, даних для онлайн-платежів). Спамери маскуються під відомі організації (банки, соціальні мережі, державні служби), надсилаючи фальшиві повідомлення про "блокування рахунку", "підтвердження даних" або "необхідність термінового оновлення інформації". Повідомлення містять посилання на підроблені веб-сайти, які імітують оригінальні, але збирають введені користувачем дані.

- Смішинг (*Smishing*) та Вішинг (*Vishing*): Варіанти фішингу, що використовують

SMS-повідомлення (смішинг) та голосові дзвінки (вішинг) для виманювання інформації.

3. Деструктивний спам:

- Поширення шкідливого ПЗ (*Malware*): Спам-листи можуть містити вкладення зі шкідливим програмним забезпеченням (віруси, трояни, *ransomware*) або посилання на скомпрометовані веб-сайти, що автоматично завантажують шкідливі файли.

- *DDoS*-атаки через поштові системи: Масова розсилка величезної кількості листів може бути спрямована на перевантаження поштових серверів або інших інформаційних систем, викликаючи відмову в обслуговуванні (*DDoS*-атака).

- Дискредитація: Розсилання листів від імені інших осіб або організацій з метою їх дискредитації та створення негативного іміджу.

- Релігійний/політичний спам: Розсилки з релігійним або політичним змістом, що нав'язують певні погляди або пропаганду.

4. Випадкові/Ненавмисні розсилки:

- Поштові хробаки (*Mail Worms*): Це вид шкідливого ПЗ, який після зараження комп'ютера автоматично шукає адреси електронної пошти та розсилає себе на ці адреси. Часто такі хробаки підставляють випадкову адресу з адресної книги зараженого комп'ютера у поле "Від", що призводить до того, що люди отримують повідомлення про розсилку вірусу, хоча насправді не мають до цього

стосунку. Це створює навантаження на мережу та викликає помилкові спрацьовування антивірусних систем.

Сучасні канали розповсюдження спаму

Спам еволюціонував від електронної пошти та груп новин до використання нових каналів комунікації:

1. Електронна пошта (*Email*): Залишається основним каналом. За різними оцінками, сьогодні спам та шкідливі листи становлять від 70% до 90% загального електронного трафіку.

- Збір адрес: Спамери використовують спеціальні боти-збирачі (*harvesting bots*), які сканують веб-сторінки, форуми, соціальні мережі, списки розсилок, електронні

дошки оголошень та чати для збору адрес. Зібрані дані формують величезні бази електронних адрес, які потім продаються або використовуються для власних розсилок.

- Джерела розсилок: Спам розсилається з різних джерел, часто з метою приховати справжнього відправника:
  - Неправильно налаштовані сервери (*Open Relays*/*Proxies*): Поштові сервери, які дозволяють будь-кому відправляти пошту через них без автентифікації.
  - Веб-поштові сервіси: Сервіси, що пропонують анонімний доступ або спрощену реєстрацію, яку можуть експлуатувати боти.
  - Ботнети (Зомбі-комп'ютери): Мережі скомпрометованих комп'ютерів користувачів, які були заражені шкідливим ПЗ і віддалено керуються зловмисниками для масових розсилок. Це дозволяє спамерам приховувати своє справжнє місцезнаходження та використовувати тисячі *IP*-адрес для розсилок.
- Обфускація повідомлень: Для обходу спам-фільтрів спамери спотворюють текст повідомлень, використовуючи схожі за написанням символи (наприклад, "0" замість "*O*"), латинські літери замість кирилиці, додають випадкові пробіли чи спеціальні символи.

2. Групи новин та форуми: Багато відкритих форумів та старих груп новин *Usenet*, де немає належної модерації, досі заповнені спамом, що відштовхує користувачів.

3. Миттєві повідомлення (*Instant Messaging*) та соціальні мережі: З розвитком месенджерів (*Viber*, *Telegram*, *WhatsApp*) та соціальних мереж (*Facebook*, *Instagram*, *LinkedIn*) спамери активно використовують їх для розсилки небажаних повідомлень, часто використовуючи списки контактів або автоматизовані боти для розсилок.

4. Блоги, Вікі та коментарі: Відкриті платформи, що дозволяють вільно редагувати контент (наприклад, коментарі в блогах, сторінки Вікі), часто стають мішенню для спамерів, які розміщують небажані посилання або рекламні тексти.

5. *SMS*-повідомлення (*SMS-Spam*): Розсилка небажаних рекламних повідомлень

або фішингових посилань на мобільні телефони. Це особливо дратує, оскільки в роумінгу за такі повідомлення може стягуватися плата.

6. *Push*-сповіщення: Зловмисники можуть обманом змусити користувачів підписатися на небажані *push*-сповіщення у браузерах або мобільних додатках. 7. Голосовий спам (*Spam Calls*/*Robocalls*): Автоматизовані телефонні дзвінки, що просувають продукти/послуги або використовуються для шахрайства. Небезпека спаму та його негативні наслідки

Хоча вартість надсилання спаму для зловмисників мінімальна, він несе значні витрати та ризики для одержувачів та інфраструктури:

- Фінансові витрати для користувачів: Споживачі, особливо в роумінгу або з обмеженими тарифними планами, можуть платити за отримання спам-повідомлень (наприклад, *SMS*).

- Витрати часу та ресурсів:

  - Користувачі: Витрачають час на видалення небажаних листів, фільтрацію повідомлень та відсіювання важливої інформації від спаму. - Організації: Витрачають значні ресурси (час, електроенергія, апаратні потужності) на обробку та фільтрацію величезних обсягів спам-трафіку на поштових серверах, шлюзах безпеки та інших компонентах мережевої

  інфраструктури. Це знижує продуктивність систем та збільшує операційні витрати.

- Втрата важливої інформації: Агресивні спам-фільтри можуть помилково ідентифікувати легітимні повідомлення як спам, що призводить до втрати важливої ділової або особистої кореспонденції.

- Ризики кібербезпеки: Спам є одним з основних векторів для поширення шкідливого ПЗ, фішингових атак та інших видів кібершахрайства, що може призвести до витоку даних, фінансових втрат та компрометації систем.

- Зниження довіри та дратівливість: Постійний потік небажаних повідомлень знижує довіру користувачів до електронної комунікації та створює негативний досвід взаємодії.

Для ефективної боротьби зі спамом необхідний комплексний підхід, що включає технічні рішення (фільтри, ШІ-алгоритми), законодавчі ініціативи та підвищення обізнаності користувачів.

2.2 Організація захисту від спаму та деструктивних процедур

Ефективна боротьба зі спамом вимагає комплексного підходу, що поєднує превентивні заходи з використанням передових технологій. Найкращий захист – це запобігання потраплянню вашої електронної адреси до баз спамерів. Хоча це непросто, існують дієві запобіжні кроки:

- Обережність при публікації адрес: Уникайте необґрунтованої публікації своєї основної електронної адреси на загальнодоступних веб-сайтах, форумах, у соціальних мережах або старих групах новин. Спамерські боти постійно сканують інтернет для збору адрес.

- Використання одноразових або додаткових адрес: Для реєстрації на нових, підозрілих або навіть корисних, але некритичних веб-сайтах, створіть спеціальну, "одноразову" або вторинну електронну адресу. Це дозволить зберегти основну скриньку чистою.

- Ніколи не взаємодійте зі спамом: Категорично не відповідайте на спам повідомлення, не натискайте на посилання "відписатися" (якщо ви не впевнені, що це легітимна розсилка, на яку ви підписувалися) і не завантажуйте зображення, якщо ваш поштовий клієнт не блокує їх за замовчуванням. Будь-яка взаємодія підтверджує спамеру, що ваша адреса активна, і призведе до збільшення обсягу спаму.

- Вибір надійної адреси: При створенні нової електронної скриньки намагайтеся обирати складну для вгадування адресу, використовуючи комбінації літер, цифр та символів.

- Розгляд зміни адреси (як крайній захід): Якщо ваша поштова скринька вже сильно забруднена спамом, зміна адреси може бути радикальним, але ефективним рішенням. Однак це створює незручності, оскільки потрібно повідомити важливі

контакти про нову адресу.

Сучасні технології захисту від спаму

Для автоматичного виявлення та фільтрації спаму використовується спеціалізоване програмне забезпечення, що може працювати як на стороні користувача, так і на поштових серверах. Існують два основні підходи до такої фільтрації:

1. Контентний аналіз: Цей метод аналізує вміст електронного листа (текст, зображення, посилання) та інші характеристики (заголовки, вкладення) для визначення, чи є він спамом. Якщо лист класифіковано як спам, він може бути позначений, переміщений до окремої папки ("Спам") або автоматично видалений.

- Переваги: Висока точність при хорошому "навчанні" фільтра. - Недоліки: Лист все одно повністю завантажується, що споживає трафік і ресурси, особливо якщо фільтрація відбувається на клієнтському комп'ютері. 2. Аналіз джерела та репутації відправника: Цей метод намагається визначити спамера, не аналізуючи вміст повідомлення. Програмне забезпечення працює переважно на поштовому сервері, який безпосередньо отримує повідомлення. - Переваги: Зменшує навантаження, оскільки повідомлення може бути відхилено на ранній стадії без повного завантаження.

- Недоліки: Спамери постійно змінюють *IP*-адреси та методи обходу, що робить цей метод менш ефективним у ізольованому вигляді. Він може вимагати постійного оновлення баз даних та взаємодії з іншими серверами для перевірки репутації.

Розміщення антиспам-програмного забезпечення (на комп'ютері кінцевого користувача або у провайдера поштового сервера) визначає, хто несе витрати, пов'язані з фільтрацією спаму:

- Фільтрація на стороні користувача: Користувач платить за весь отриманий трафік (включаючи спам), оскільки повідомлення спочатку завантажується, а вже потім фільтрується.

- Фільтрація на стороні сервера (провайдера): Усі витрати, пов'язані з отриманням та фільтрацією спаму, лягають на власника поштового сервера.

Користувач отримує вже очищену від спаму пошту, що є більш вигідним. Сучасні методи фільтрації електронної пошти:

1. Чорні списки (*Blacklists*): Списки *IP*-адрес або доменних імен, відомих як джерела спаму. Використовуються локальні списки або глобальні, що підтримуються спеціалізованими сервісами (наприклад, *DNSBL - DNS-based Blackhole Lists*).

- Актуальність: Ефективність знизилася. Спамери швидко змінюють *IP* адреси та використовують скомпрометовані "зомбі-комп'ютери", що не дозволяє чорним спискам оперативно реагувати. Більше того, блокування цілих мережевих діапазонів може призвести до блокування легітимних користувачів.

2. Авторизація поштового сервера (*Sender Authentication*): Методи, що перевіряють, чи дійсно відправник листа має право надсилати пошту від імені зазначеного домену. До них відносяться:

- *SPF* (*Sender Policy Framework*): Дозволяє власникам доменів публікувати записи про те, які *IP*-адреси дозволено надсилати пошту від їхнього домену. - *DKIM* (*DomainKeys Identified Mail*): Дозволяє поштовому серверу підписувати вихідні листи криптографічним ключем, що підтверджує їхню цілісність та походження.

- *DMARC* (*Domain-based Message Authentication, Reporting, and Conformance*): Поєднує *SPF* і *DKIM*, дозволяючи власникам доменів визначати, що робити з листами, які не пройшли автентифікацію.

- Актуальність: Надзвичайно актуальні та ефективні, є галузевим стандартом для автентифікації пошти.

3. Сірі списки (*Greylisting*): Метод, заснований на поведінці спамерських програм. При першій спробі доставки листа з невідомого відправника поштовий сервер відхиляє його з тимчасовою помилкою. Легітимні поштові сервери, відповідно до протоколу *SMTP*, спробують повторно надіслати лист через деякий час, і тоді він буде прийнятий та доданий до "білого списку". Спамерські програми зазвичай не повторюють спробу.

- Актуальність: Досі ефективний для фільтрації значної частини спаму (до 90%).

- Недоліки: Може викликати затримки в доставці перших листів від нових

відправників (до півгодини або більше), що може бути неприйнятним для термінової кореспонденції. Також може некоректно працювати з деякими поштовими сервісами, які не повністю дотримуються стандартів *SMTP*.

4. Методи статистичної фільтрації (*Statistical Filtering*): Ці методи аналізують вміст листа (слова, фрази, їх частоту) та інші атрибути, щоб визначити ймовірність того, що це спам. Найуспішніші алгоритми базуються на теоремі Байєса (*Bayesian Filtering*).

- Принцип роботи: Фільтр "навчається" на великих обсягах кореспонденції, вручну класифікованої як "спам" або "не спам". На основі цього навчання він будує статистичні моделі.

- Актуальність: Дуже ефективні, можуть ідентифікувати до 95-99% спаму після належного навчання. Широко використовуються в поштових сервісах та клієнтах.

5. Інші (додаткові) методи:

- Жорсткі вимоги до заголовків та відправників: Відмова від листів з неіснуючими зворотними адресами, перевірка відповідності доменних імен *IP*-

адресам відправників. Хоча ці заходи застарілі для комплексного захисту, вони допомагають відфільтрувати найпримітивніший спам.

- *Challenge-Response* системи: Вимагають від відправника підтвердження, що він не є роботом (наприклад, введення *CAPTCHA*) перед тим, як лист буде доставлений.

- Клієнтські антиспам-модулі: Вбудовані в поштові клієнти або браузери фільтри, що дозволяють налаштовувати вибіркове завантаження контенту або блокувати небажані елементи (наприклад, "антиспам браузера" для блокування небажаного контенту на веб-сторінках, що включає захист самого браузера,
модулів та стороннього ПЗ для фільтрації трафіку).

- Хмарні антиспам-рішення: Багато провайдерів використовують хмарні сервіси для фільтрації спаму до того, як він досягне поштового сервера клієнта, що значно знижує навантаження.

Основна мета спаму: від реклами до деструкції

Кінцева мета спаму залишається незмінною – доставити повідомлення якомога

більшій кількості одержувачів за мінімальну ціну, незважаючи на склад аудиторії, а здебільшого на кількість. Однак, форми цієї мети еволюціонували:

1. Реклама продукції/послуг: Класичний спам, що просуває реальні або шахрайські товари/послуги, надаючи посилання на веб-сайти або контактні дані. 2. Просування веб-сайтів (*SEO*-спам): Метою є підвищення рейтингу веб сайту в пошукових системах або збільшення трафіку, навіть якщо вміст не відповідає очікуванням користувача. Часто використовуються редиректи або приховані лічильники.

3. Фінансові шахрайства:

- "Таксофонні" схеми: Запрошення зателефонувати на номер з високою тарифікацією, де користувач чує лише автовідповідач або музику, а потім отримує величезний рахунок.
- Пірамідальні схеми/мережевий маркетинг: Обіцянки надзвичайно легкого та високого прибутку за умови початкового внеску або залучення нових учасників.

4. Збір інформації (*Data Harvesting*): Під виглядом опитувань, розіграшів або замовлень пропонується заповнити анкети, метою яких є збір персональних даних (імені, адреси, телефону, інтересів) для подальшого продажу або використання в інших шахрайських схемах.

5. Поширення шкідливого ПЗ: Спам є одним з основних каналів для поширення троянських програм, вірусів, програм-вимагачів (*ransomware*) та шпигунського ПЗ. Ці програми збирають конфіденційну інформацію (паролі, дані банківських карток, доступ до акаунтів) та надсилають її зловмисникам, або блокують систему, вимагаючи викуп.

Боротьба зі спамом є постійною гонкою озброєнь між спамерами та засобами захисту. Користувачі повинні залишатися пильними та використовувати багаторівневі рішення для забезпечення своєї безпеки.

РОЗДІЛ 3
ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ШКІДЛИВИХ ПРОГРАМ ТА ПРОГРАМНИХ ЗАГРОЗ

3.1 Програмні засоби інформаційної безпеки комп'ютерних систем: Сучасні тенденції

Сучасний ландшафт кібербезпеки вимагає постійного вдосконалення та адаптації засобів захисту інформації. Аналіз актуальних публікацій та практичного досвіду виділяє такі ключові напрямки розвитку:

- Відкриті стандарти та інтеграція: Сучасні інструменти кібербезпеки повинні базуватися на відкритих стандартах для забезпечення сумісності та взаємодії між рішеннями різних виробників. Важливим є інтеграційний підхід, що дозволяє об'єднувати функціональність різних компонентів (наприклад, між брандмауерами, *VPN*-шлюзами, системами виявлення вторгнень, рішеннями для управління ідентифікацією та доступом) для створення єдиної, скоординованої системи захисту.

- Масштабованість: Засоби захисту повинні ефективно працювати в умовах зростання кількості користувачів, пристроїв та обсягів даних, що обробляються корпоративними мережами.

Ключові тенденції у розвитку засобів кібербезпеки:

1. Скоординований контроль доступу: Впровадження єдиної політики контролю доступу, що діє на всіх рівнях мережі (периметр, внутрішні сегменти, хмарні ресурси) та для різних точок доступу.

2. Сегментація внутрішньої мережі: Використання кількох брандмауерів або механізмів мікросегментації всередині корпоративної мережі для обмеження поширення загроз у разі компрометації одного сегмента.

3. Диференційований контроль доступу: Надання різних рівнів доступу до ресурсів для різних категорій користувачів (наприклад, на основі ролей, відділів, чутливості інформації), реалізуючи принцип найменших привілеїв.

4. Удосконалення автентифікації та контролю вмісту: Розробка надійних методів автентифікації (наприклад, багатофакторна автентифікація – *MFA*, біометрія) та інструментів для контролю вмісту переданої інформації (наприклад, системи *DLP - Data Loss Prevention*).

5. Захист даних у загальнодоступних мережах: Забезпечення конфіденційності

та цілісності даних під час їх передачі через публічні мережі (Інтернет) за допомогою шифрування та віртуальних приватних мереж (*VPN*).

6. Інтеграція контролю доступу та *VPN*: Об'єднання функцій контролю доступу з технологіями *VPN* для спрощення управління безпекою та забезпечення безшовного захисту віддалених підключень.

7. Виявлення та реагування на вторгнення (*EDR*/*XDR*): Впровадження сучасних систем виявлення вторгнень (*IDS*) та запобігання вторгненням (*IPS*), а також більш комплексних рішень *Endpoint Detection and Response* (*EDR*) та *Extended Detection and Response* (*XDR*) для проактивного виявлення та нейтралізації загроз.

8. Висока ефективність та продуктивність: Забезпечення того, щоб захисні засоби не сповільнювали роботу мережі та систем, відповідаючи вимогам сучасної високошвидкісної інфраструктури.

9. Надійність та відмовостійкість: Збільшення надійності та відмовостійкості систем захисту шляхом резервування, кластеризації та автоматичного перемикання у разі збоїв.

10. Безпека та ефективність управління *IP*-інфраструктурою: Забезпечення захисту та ефективного управління мережевими адресами, зокрема за допомогою автоматизованих систем управління *IP*-адресами (*IPAM*).

11. Централізоване управління: Розробка платформ для централізованого управління всіма засобами безпеки, що дозволяє спростити конфігурацію, моніторинг та реагування на інциденти.

12. Відкриті стандарти для інтеграції: Використання відкритих стандартів для забезпечення сумісності засобів безпеки від різних виробників, що дозволяє створювати гнучкі та адаптивні рішення.

Роль брандмауерів та *VPN* у сучасній архітектурі безпеки

Реалізація вищезазначених тенденцій можлива завдяки постійному вдосконаленню та розширенню функціональності брандмауерів наступного покоління (*Next-Generation Firewalls - NGFW*) та активному використанню віртуальних приватних мереж (*VPN*). Сучасні брандмауери повинні мати такі можливості:

- Інтеграція з мережевими каталогами: Використання облікових даних, що зберігаються в службах мережевих каталогів (наприклад, *Active Directory, LDAP*), для створення правил доступу та виконання брокерської автентифікації – виступаючи посередником між користувачами та корпоративною системою автентифікації.

- Підтримка цифрових сертифікатів та *PKI*: Сучасні брандмауери повинні підтримувати широко розповсюджену технологію автентифікації в Інтернеті на основі цифрових сертифікатів *X*.509 та інфраструктури відкритих ключів (*PKI*). Це забезпечує надійну автентифікацію та безпечну передачу даних.

- Розширена функціональність та взаємодія: Брандмауери повинні не лише виконувати свої базові функції, але й взаємодіяти зі спеціалізованими продуктами (наприклад, передаючи їм автентифікацію певних повідомлень, інтегруючись з системами виявлення шкідливого ПЗ).

VPN-технології є критично важливими для організації безпечних тунелів для передачі корпоративних даних через загальнодоступні мережі. Основою для створення безпечних *VPN*-тунелів є набір інтернет-стандартів *IPsec*, який пропонує можливості використання цифрових сертифікатів та інфраструктури *PKI* для автентифікації та генерації сеансових ключів. Це робить *IPsec*-рішення масштабованими, сумісними з іншими інструментами безпеки та дозволяє забезпечувати конфіденційність, цілісність та автентифікацію трафіку.

Для захисту віддаленого доступу *VPN*-рішення вимагають клієнтських компонентів, сумісних з основними операційними системами, які не підтримують *IPsec* "з коробки". *VPN*-шлюзи повинні бути високомасштабованими, щоб підтримувати сотні, а то й тисячі одночасних безпечних з'єднань.

Зважаючи на обчислювальну складність багатьох операцій, що виконуються засобами безпеки (особливо шифрування та автентифікації), спостерігається тенденція до апаратної реалізації цих функцій. Це може бути реалізовано як у вигляді спеціалізованих апаратних прискорювачів, що доповнюють стандартні комп'ютерні платформи, так і у вигляді автономних, спеціалізованих пристроїв, що виконують всі функції брандмауера або *VPN*-шлюзу.

Надійність та відмовостійкість систем захисту, особливо в критичних

застосуваннях, підвищується за рахунок резервування та надмірності на рівні самих засобів захисту (наприклад, кластери брандмауерів, *VPN*-пристроїв, систем виявлення вторгнень).

VPN-шлюзи також забезпечують приховування внутрішніх *IP*-адрес шляхом інкапсуляції пакетів, що дозволяє передавати їх у зовнішню мережу з адреси зовнішнього інтерфейсу шлюзу, захищаючи внутрішню топологію мережі.

Найбільш перспективним для побудови комплексного захисту корпоративних мереж є інтеграція функцій брандмауера та *VPN*-шлюзу в одному продукті. Роздільне використання цих інструментів може створювати проблеми сумісності та управління.

Приклади сучасних ініціатив у сфері кібербезпеки:

- Комплексні платформи безпеки: Замість окремих продуктів, компанії розробляють інтегровані платформи безпеки (*Security Platforms*), які об'єднують функції виявлення атак, сканування вразливостей, управління ідентифікацією та доступом, захисту даних та реагування на інциденти. Наприклад, рішення *EDR*/*XDR*, що об'єднують можливості антивірусу, моніторингу поведінки та автоматизованого реагування.

- Динамічна мережева інфраструктура: Розвиток технологій, що дозволяють створювати динамічні *IP*-адреси та змінювати мережеві координати для підвищення безпеки. Це ускладнює дії зловмисників, оскільки цілі постійно змінюють своє мережеве розташування. Прикладом є концепції мереж з нульовою довірою (*Zero Trust*), де кожен запит на доступ автентифікується та авторизується, незалежно від його походження.

- Безпечні онлайн-транзакції: Удосконалення систем онлайн-платежів та електронних гаманців для забезпечення безпечних транзакцій між покупцями, інтернет-магазинами та банками. Це включає використання надійних шлюзів, шифрування даних та багатофакторну автентифікацію.

Безпека програмного забезпечення (*Software Security*)

Безпека програмного забезпечення (ПЗ) у широкому сенсі означає здатність програмного продукту функціонувати належним чином, не створюючи негативних наслідків для комп'ютерної системи, на якій він працює. Рівень безпеки ПЗ

відображає ймовірність отримання коректних функціональних результатів за певних умов експлуатації.

Причини аномальної поведінки програмного забезпечення можуть бути різними: збої апаратного забезпечення, помилки програмістів та операторів, а також дефекти програмного забезпечення. Ці дефекти поділяються на два основні типи: навмисні дефекти (закладки, уразливості, бекдори) та ненавмисні дефекти (баги, помилки). Навмисні дефекти зазвичай є результатом зловмисних дій, тоді як ненавмисні виникають через людські помилки або недоліки в процесі розробки.

Проблема захисту ПЗ від навмисних недоліків:

При вивченні проблеми захисту програмного забезпечення від навмисних недоліків виникають такі ключові питання:

- Можливість практичної реалізації деструктивних закладок: Чи можуть бути впроваджені шкідливі програмні закладки у виконуваний код, і наскільки це складно?

- Мотивація зловмисників: Які мотиви спонукають суб'єктів впроваджувати такі недоліки?

- Виявлення дефектів: Як виявити наявність навмисного дефекту в програмному забезпеченні?

- Відмінність від помилок: Як відрізнити навмисні дефекти від звичайних програмних помилок?

- Наслідки запуску деструктивних програм: Які найбільш ймовірні наслідки активації шкідливих програмних засобів під час роботи комп'ютерної системи?

- Відповідаючи на перше питання, слід зазначити, що впровадження деструктивних закладок можливе, особливо з боку:

- Безпосередніх розробників: Люди, які мають глибокі знання технологій розробки програмного забезпечення, досвід створення алгоритмів та програм, розуміють складність тестування та можуть приховати шкідливі функціональності.

- Висококваліфікованих сторонніх програмістів: Фахівці, що володіють

навичками реверс-інжинірингу (дизасемблювання виконуваного коду, отримання оригінального тексту), здатні впроваджувати деструктивні програми, перекомпільовувати та модифікувати ідентифікаційні характеристики програми, щоб вона виглядала як оригінальна.

Можливі мотиви впровадження закладок та дефектів:

Наявність алгоритмічної або програмної закладки в компоненті ПЗ може бути зумовлена кількома факторами:

- Зловмисні дії розробників: Пряма кримінальна діяльність безпосередніх розробників алгоритмів та програм.

- Діяльність спеціальних служб та організацій: Впровадження "бекдорів" або шкідливих функцій на замовлення розвідувальних або кіберзлочинних груп. - Використання скомпрометованих засобів розробки: Використання інструментів розробки програмного забезпечення (компіляторів, бібліотек), які самі містять шкідливі властивості та автоматично генерують деструктивні програмні засоби. Це підкреслює важливість безпеки ланцюга постачання ПЗ. Щодо мотивації злочинної поведінки, можна виділити такі аспекти: - Психологічна нестабільність: Несприятливі умови праці, загроза звільнення, особистісні кризи можуть призвести до бажання помсти. - Невизнані амбіції: Прагнення довести власні інтелектуальні здібності, відчуття недооціненості, що може штовхати до демонстрації деструктивних навичок.

- Економічна вигода/Перехід до конкурентів: Зацікавленість у фінансовій винагороді за впровадження закладок, викрадення інформації або саботаж для конкурентів.

- "Усунення помилок": Надання винагороди за виявлення та "усунення" раніше впроваджених власних "програмних збоїв".

- Творчий виклик: Для деяких розробка шкідливого ПЗ є формою самовираження та творчого виклику, при цьому можливі наслідки можуть ігноруватися або недооцінюватися.

Варто зазначити, що у сучасному кіберландшафті, на відміну від простих "електронних закладок" минулого, шкідливе програмне забезпечення (ШПЗ) є

набагато складнішим, його використання є більш прихованим та ефективним, що робить його однією з найсерйозніших загроз.

Загрози безпеці програмного забезпечення та приклади їх реалізації Загрози інформаційній та програмній безпеці комп'ютерних мереж виникають не лише під час експлуатації систем, а й на всіх етапах їхнього життєвого циклу, особливо під час розробки програмного забезпечення, баз даних та інших інформаційних компонентів. Це підкреслює важливість концепції *Security by Design* (безпека за задумом) та *DevSecOps*, що інтегрують безпеку в кожен етап розробки.

Найбільш вразливими з точки зору безпеки інформаційних ресурсів є так звані критичні інформаційні інфраструктури (КІІ). Це складні комп'ютеризовані організаційні, технічні та технологічні системи, які є життєво важливими для функціонування держави та суспільства. Блокування або перебої в їхній роботі можуть призвести до:

- Втрати стабільності національних систем управління та контролю. - Компрометації національної обороноздатності.
- Колапсу фінансових систем.
- Хаосу в національних енергетичних, комунікаційних та транспортних системах.
- Техногенних катастроф або значного впливу на глобальне довкілля. - Компрометації критичних даних, що використовуються в роботі цих систем. Наразі одним із найнебезпечніших та найпоширеніших засобів компрометації інформації в комп'ютерних системах є шкідливі програми – від класичних

комп'ютерних вірусів до сучасних шифрувальників (*ransomware*) та цільових шкідливих програм.

Поряд з іншими засобами інформаційного впливу, алгоритмічні та програмні закладки також є ключовим засобом шкідливого (деструктивного) впливу на комп'ютерні мережі.

- Алгоритмічна закладка – це навмисно приховане спотворення будь-якої частини алгоритму або його побудови на етапі проєктування. Це призводить до того, що коли алгоритм реалізовано у програмному компоненті, він або обмежений у

виконанні визначених функцій, або взагалі не виконує їх за певних умов (які залежать від даних, що обробляються). Крім того, можуть з'являтися непередбачені специфікацією функції, які активуються за суворо визначених умов.

- Програмна закладка – це набір команд або фрагментів коду, включених у прихованій формі до виконуваного коду програмного компонента на будь-якому етапі його розробки. Вона реалізує несанкціонований алгоритм, який обмежує або запобігає виконанню програмою необхідних функцій за певних умов, або надає програмі функції, не зазначені у специфікації, які можуть бути виконані лише за певних суворих умов.

Поведінку алгоритмічних та програмних закладок можна поділити на три основні категорії:

- Зміна функціональності комп'ютерної системи (мережі): Деформація або викривлення логіки роботи системи.

- Несанкціоноване зчитування інформації (витік даних): Негласне отримання доступу до конфіденційних даних.

- Несанкціонована модифікація інформації (порушення цілісності): Зміни даних або програмного коду, аж до їх знищення.

Важливо зазначити, що ці категорії впливу часто перетинаються.

Несанкціонований доступ до інформації:

Сучасні приклади несанкціонованого доступу до інформації включають: - Викрадення облікових даних: Зчитування паролів, токенів автентифікації та ідентифікації конкретних користувачів.

- Отримання конфіденційної інформації: Ексфільтрація чутливих даних (фінансових, медичних, комерційної таємниці, особистих даних) з системи. - Моніторинг запитів користувачів: Визначення, яку інформацію шукає або генерує користувач.

- Маніпуляції з доступом: Зміна паролів або прав доступу для отримання подальшого несанкціонованого доступу.

- Шпигунство за активністю: Моніторинг активності користувачів (веб серфінг, комунікації) для отримання непрямої інформації про їхню взаємодію та характер обмінюваних даних.

Несанкціонована модифікація інформації:

Це один із найнебезпечніших видів впливу шкідливого ПЗ, оскільки він може призвести до катастрофічних наслідків. Цей тип впливу включає: - Пошкодження даних та виконуваного коду: Внесення ледь помітних або руйнівних змін до інформаційних масивів, баз даних, конфігураційних файлів або програмного коду.

- Впровадження закладок у інші програми/модулі: Механізм, схожий на дії вірусів, що дозволяє поширювати шкідливі функціональності. - Викривлення/пошкодження системних повідомлень: Маніпуляції з повідомленнями сервера, що призводять до збоїв або некоректної роботи мережевих служб.

- Модифікація мережевих пакетів: Зміна даних у мережевому трафіку "на льоту".

Підсумовуючи, алгоритмічні та програмні закладки мають широкий спектр руйнівного впливу на інформацію, що обробляється обчислювальними ресурсами в комп'ютерній мережі. Тому при контролі технічної безпеки програмного забезпечення необхідно враховувати його використання та склад апаратного та програмного середовища комп'ютерної мережі.

Залежно від часу введення в програму, програмні закладки можна розділити на дві категорії:

- Апріорні закладки ("нативні закладки"): Введені під час процесу розробки програмного забезпечення.

- Апостеріорні закладки ("пост-закладки"): Введені під час тестування, експлуатації чи модернізації програмного забезпечення.

Хоча останні більше стосуються операційної безпеки, ніж технічної, методи комплексного тестування ПЗ, методи розрахунку ймовірності існування дефектів та оцінки рівня безпеки значною мірою перетинаються та доповнюють один одного. Ефект від активації програмних закладок майже однаковий, незалежно від етапу життєвого циклу ПЗ, на якому вони були впроваджені.

Отже, ці програмні засоби з деструктивним впливом зазвичай мають шкідливий характер, а наслідки їх активації та використання можуть завдати значної або навіть непоправної шкоди тим сферам людської діяльності, де використання комп'ютерних систем є критично важливим. У зв'язку з цим такі шкідливі програми називаються деструктивними програмними засобами (ДПЗ), які загалом класифікуються наступним чином:

- Комп'ютерні віруси та черв'яки: Програми, здатні до самовідтворення, приєднання до інших програм, поширення через мережі передачі даних, проникнення та виведення з ладу систем управління (наприклад, промислових контролерів).
- Програмні закладки (*Backdoors*): Компоненти, попередньо встановлені в системах, які активуються після отримання сигналу або у встановлений час, спотворюючи інформацію, порушуючи роботу програмного та апаратного забезпечення, або надаючи несанкціонований доступ.
- Методи та засоби впровадження та керування: Інструменти та техніки, що дозволяють впроваджувати шкідливе ПЗ та дистанційно ним керувати (наприклад, *C*2-сервери).

Основні принципи безпеки програмного забезпечення

Для забезпечення технічної та операційної безпеки програмного забезпечення необхідно враховувати весь набір програмних компонентів у конкретній комп'ютерній мережі. Домінуючою має бути політика здійснення комплексного

наскрізного контролю на всіх етапах життєвого циклу програмних компонентів (від проєктування до експлуатації та виведення з експлуатації). Заходи щодо забезпечення технічної та операційної безпеки повинні зберігатися конфіденційними. Необхідно забезпечити постійний, комплексний та проактивний контроль діяльності розробників та користувачів компонентів.

Окрім загальних принципів, необхідно виділити принципи забезпечення безпеки на кожному етапі життєвого циклу програмного забезпечення: Принципи забезпечення технічної безпеки на етапах планування та аналізу проєкту:

1. Комплексність безпеки ПЗ: Враховувати безпеку інформації та обчислювальних процесів, усі структури комп'ютерних мереж, потенційні канали

витоку інформації та несанкціонованого доступу, а також комплексне застосування організаційних та технічних заходів.

2. Планування впровадження засобів безпеки: Акцент на спільний системний дизайн програмного забезпечення та його засобів безпеки, планування їх використання за очікуваних умов експлуатації. Це відображає концепцію *Security by Design*.

3. Ефективність заходів безпеки ПЗ: Включає оцінку рівнів безпеки за допомогою методів глибокого аналізу (*deep science*), прогнозування загроз та проведення комплексних апріорних оцінок показників захисних заходів.

4. Адекватність процесуального забезпечення: Необхідність пошуку найефективніших та найнадійніших заходів безпеки при мінімізації їхніх витрат, що є результатом аналізу ризиків.

5. Гнучкість управління захистом ПЗ: Система управління забезпеченням інформаційної безпеки ПЗ повинна мати здатність діагностувати, нейтралізувати та проактивно та ефективно усувати нові загрози в умовах швидких змін середовища "інформаційної війни".

6. Раннє впровадження безпеки: Засоби забезпечення безпеки та контролю виробництва ПЗ повинні розроблятися якомога раніше, включаючи превентивні заходи для забезпечення технічної безпеки на всіх етапах.

7. Документування методик створення програм: Розробка повного комплекту нормативно-технічної документації для контролю наявності навмисних дефектів у програмних засобах.

Принципи впровадження технічної безпеки в процесі розробки програмного забезпечення:

1. Стандартизація етапів розробки: Впорядкування етапів, визначення проміжних контрольних точок, стандартизація специфікацій програмних модулів, функцій та форматів представлення даних.

2. Автоматизований моніторинг дефектів: Використання автоматизованих інструментів для виявлення дефектів у керуючих та обчислювальних програмах. Створення бібліотек типових алгоритмів, примітивів та програмних засобів для

виявлення навмисних дефектів (наприклад, *SAST - Static Application Security Testing*).

3. Функціональна ітерація та поетапне керування: Використання ітераційних підходів та поетапного контролю в процесі створення програмних модулів для їхньої фільтрації та виявлення проблем на ранніх стадіях.

4. Стандартизація алгоритмів та уніфікація: Забезпечення сумісності інформації, технологій та ПЗ. Максимальна уніфікація всіх компонентів та інтерфейсів для зменшення складності та потенційних вразливостей.

5. Централізоване управління та контроль доступу: Централізація управління базами даних програмних проєктів та технологіями їх розробки, суворе розділення функцій та обмеження доступу на основі засобів діагностики, контролю та захисту.

6. Запобігання несанкціонованому доступу: Захист від несанкціонованого доступу співвиконавців та користувачів мережі, підключених до місця розробки програми.

7. Логування процесів розробки: Збір та ведення системних журналів всіх процесів розробки ПЗ для постійного контролю технічної безпеки. 8. Використання сертифікованих інструментів: Застосування лише сертифікованих та перевірених інструментів для розробки програм, особливо для

нових методів обробки інформації та перспективних архітектур обчислювальних систем.

Принципи забезпечення технічної безпеки під час тестування та приймальних випробувань:

1. Комплексне тестування ПЗ: Розробка широких наборів тестів, що охоплюють різні категорії програм, дозволяючи функціонально та статистично контролювати поведінку програми при різних вхідних та вихідних даних (наприклад, *Fuzzing, Unit Testing, Integration Testing*).

2. Тестування під екстремальними навантаженнями: Ретельне тестування програми в умовах екстремальних навантажень, що імітують вплив активних загроз або помилок.

3. "Фільтрація" програмних комплексів: Виявлення можливих навмисних

недоліків на основі створення моделей загроз та відповідних програмних засобів сканування (наприклад, *DAST - Dynamic Application Security Testing, Penetration Testing*).

4. Розробка та тестування засобів верифікації: Створення та експериментальне тестування інструментів для верифікації програмних продуктів. 5. Виявлення "вузьких місць": Тестування ПЗ на стендах для виявлення ненавмисних помилок у проєктуванні та розробці, які можуть призвести до нефункціональності програми, а також для виявлення "вузьких місць", що можуть мати руйнівні наслідки.

6. Захист від несанкціонованих змін: Розробка заходів, що запобігають внесенню зловмисниками несанкціонованих змін до програмного забезпечення після його розробки та тестування.

7. Сертифікація ПЗ: Сертифікація програмних продуктів згідно з вимогами безпеки, видача сертифікатів відповідності технічним характеристикам. Принципи забезпечення безпечної роботи програмного забезпечення: 1. Захист стандартів ПЗ: Зберігання та обмеження доступу до стандартів програмного забезпечення та запобігання їхній несанкціонованій модифікації.

2. Проактивне тестування та сканування: Профілактичне вибіркове тестування та повне сканування програмного забезпечення для виявлення навмисних дефектів. Це включає безперервний моніторинг безпеки (*Continuous Security Monitoring*).

3. Виявлення загроз у процесі налагодження: Виявлення загроз безпеці ПЗ під час налагодження на основі очікуваних загроз та засобів їхнього контролю. 4. Модульність та гнучкість модифікації: Забезпечення можливості модифікації програмного продукту під час роботи шляхом заміни окремих модулів без зміни загальної структури та зв'язків з іншими компонентами. 5. Суворий облік та каталогізація: Точний облік та каталогізація всіх підтримуваних програмних засобів, а також зібраної, обробленої та збереженої інформації.

6. Статистичний аналіз аномалій: Статистичний аналіз всіх процесів, робочих операцій та інформації про відхилення від нормальних режимів роботи програмного забезпечення (наприклад, *SIEM*-системи, *User and Entity Behavior Analytics - UEBA*).

7. Гнучке застосування додаткових засобів захисту: Швидке впровадження

додаткових засобів захисту ПЗ у разі неочікуваного виявлення нових, непередбачених загроз інформаційній безпеці.

Методи та інструменти аналізу безпеки програмного забезпечення Для виявлення елементів шкідливих програм (ДПЗ), від найпростіших антивірусних сканерів до складних аналізаторів та дизасемблерів, використовується різноманітне програмне забезпечення. Саме на основі цих засобів розроблено набір методів аналізу безпеки програмного забезпечення. Методи аналізу та оцінки безпеки програмного забезпечення можна класифікувати за принциповою різницею в перспективі об'єкта дослідження (програми), не враховуючи тип інструменту (наприклад, статичний чи динамічний аналіз). Це дозволяє зосередитися на логіці перевірки, а не лише на її реалізації. Класифікація методів аналізу безпеки ПЗ (див. рисунок 3.1).

Рисунок 3.1- Діаграма, що ілюструє різні методи аналізу безпеки програмного забезпечення, згруповані за підходами до дослідження об'єкта

Загальна система дослідження безпеки програмного забезпечення повинна охоплювати:

- Інспекцію: Ручний або автоматизований перегляд коду.
- Тестування: Виконання програми для виявлення дефектів.
- Контрольно-інспекційний аналіз: Моніторинг поведінки програми. - Аналітичний аналіз: Формальний аналіз коду без його виконання. - Логічний аналіз: Доведення властивостей програми на основі формальних моделей.

Повна система має повною мірою використовувати переваги кожного методу. З методологічної точки зору, логічні та аналітичні методи є більш ефективними,

оскільки вони дозволяють оцінити достовірність отриманих результатів та простежити порядок їх отримання (за допомогою зворотного міркування). Однак ці методи є більш трудомісткими, ніж інспекція та тестування.

Методи інспекції, тестування та контролю для аналізу безпеки ПЗ: Ці методи використовуються для виявлення порушень вимог безпеки в системі, де програма призначена для використання. Тестування програм базується на стандартах безпеки програм і може проводитися за допомогою: - Тестових запусків: Виконання програми з різними вхідними даними. - Виконання у віртуальному програмному середовищі (пісочниці): Ізольоване середовище для безпечного виконання потенційно шкідливого коду. - Символічного виконання: Аналіз усіх можливих шляхів виконання програми.

- Інтерпретації програм: Виконання коду крок за кроком для аналізу

поведінки.

- Методи перевірки, тестування та контрольно-перевіркової роботи поділяються на:

- Контроль процесу виконання програми: Моніторинг внутрішніх операцій. - Відстеження змін в операційному середовищі: Моніторинг впливу програми на файлову систему, реєстр, мережу.

Ці методи є найпоширенішими, оскільки не потребують глибокого формального аналізу, дозволяють використовувати існуючі апаратні та програмні засоби та швидко створювати готові рішення. Наприклад, метод тестових запусків у спеціальному середовищі, що фіксує спроби порушення систем захисту та обмежень доступу.

Формалізація задачі аналізу безпеки за допомогою цих методів: Припустимо, задано набір обмежень на функціональність програми, що визначають її відповідність вимогам безпеки операційної системи. Ці обмеження задані у вигляді предикатів $C=\{ci(a1,a2,...am)|i=1,...,N\}$, які залежать від набору параметрів $A=\{ai\ |i=1,...,M\}$. Цей набір A складається з двох підмножин:

- Обмежена підмножина ресурсів апаратного забезпечення та ОС (ОЗП, процесорний час, системні ресурси, інтерфейси).

- Обмежена підмножина, що обмежує доступ до об'єктів (області пам'яті, файли), які містять дані.

Щоб довести відповідність програми вимогам безпеки, необхідно довести, що програма не порушує жодної з умов у C. Для цього визначається набір параметрів $P=\{pi|i=1,...,K\}$, які контролюються під час тестового запуску. Вибір P має забезпечити, що значення A можна отримати зі значень P. Після виконання T-тестів для отриманого вектора значень параметра Pi, можна побудувати вектор значень незалежної змінної Ai. Тоді задача аналізу безпеки формалізується: Якщо для будь якого випробування $i=1,...,T$ множина предикатів $C=\{cj(a1i,a2i...ami)|j=1,...,N\}$ є істинною, то програма не містить деструктивних програмних засобів (ДПЗ).

Очевидно, що результати виконання програми залежать від вхідних даних, середовища тощо. Тому методи контролю та тестування не обмежуються лише тестовими запусками, а також включають механізми виведення результатів тестування, такі як символічні методи тестування та інші методи, що спираються на теорію верифікації програм.

Схема аналізу безпеки ПЗ з використанням методів контролю та тестування (див. рисунок 3.2).

Підхід до тестування починається з визначення набору контрольованих параметрів для середовища або процесу, що залежить від апаратного та програмного забезпечення та досліджуваного процесу. Далі розробляються та виконуються процедури тестування для перевірки вимог безпеки програми в очікуваному операційному середовищі, базуючись на зафіксованій роботі програми та змінах у середовищі, а також використовуючи екстраполяцію та випадкові методи (наприклад, *Fuzzing*).

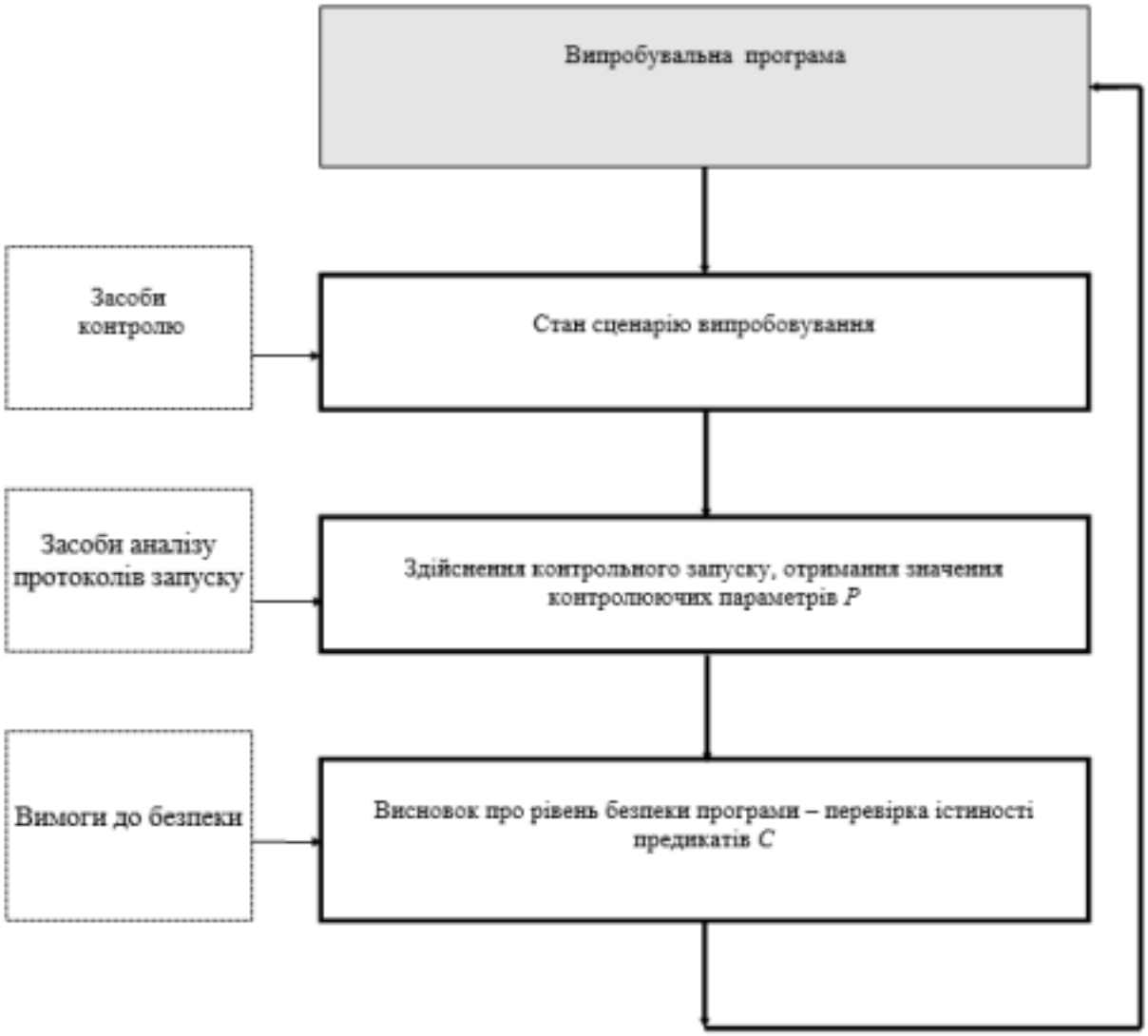

Рисунок 3.2 - Блок-схема, що ілюструє процес аналізу безпеки програмного забезпечення

Метод логічного аналізу для контролю безпеки програми:

При використанні методів логічного аналізу для аналізу безпеки (див. рисунок 3.3) необхідно побудувати формальну модель програми та довести еквівалентність між досліджуваною моделлю програми та моделлю ДПЗ.

Рисунок 3.3 - Блок-схема, що демонструє метод логічного аналізу безпеки ПЗ

У найпростішому випадку моделлю програми може бути її бінарний образ, а моделлю шкідливого ПЗ — набір сигнатур (*signatures*). Доказ еквівалентності полягає у знаходженні цих сигнатур у програмі (що є основою для багатьох антивірусних сканерів). Більш складний підхід передбачає використання формальної моделі, заснованої на наборі властивих певній групі ДПЗ ознак.

Формальне формулювання задачі аналізу безпеки з використанням логічного аналізу: Виберемо систему моделювання програм *Z*. Досліджувані програми представлені своїми моделями $M \in Z$. Має бути задана множина моделей ДПЗ $V=\{vi$

$|i=1,...,N\}$, яку можна отримати шляхом побудови моделей усіх відомих ДПЗ або

генерації моделей усіх можливих ДПЗ. Множина V є підмножиною Z. Крім того, має бути задано відношення еквівалентності $E(x,y)$, що визначає наявність ДПЗ у моделі програми. Це відношення виражає ідентичність програми x та ДПЗ y, де x – модель програми, а y – модель ДПЗ ($y \in V$). Задача аналізу безпеки зводиться до доведення того, що модель досліджуваної програми M належить відношенню $E(M,v)$, де $v \in V$.

На основі отриманих результатів можна зробити висновки про рівень безпеки програми. Ключовими поняттями тут є "метод представлення" та "модель програми". Комп'ютерну програму можна розглядати з багатьох точок зору (алгоритм, послідовність команд процесора, файл байтів). Усі ці поняття складають ієрархію моделей. Можна вибрати будь-який рівень моделі, головне – однаково задати моделі ДПЗ та програми. Створення формальних моделей програм та ДПЗ є серйозною проблемою. Механізм визначення зв'язку залежить від методу представлення моделі. Найбільш перспективним є використання семантичних діаграм та об'єктно-орієнтованих моделей.

Загалом, повний процес аналізу програмного забезпечення включає три типи аналізу:

- Лексичний аналіз валідації: Ідентифікація та класифікація різних "токенів" (сигнатур) у виконуваному коді, що представляють об'єкт дослідження. Це включає пошук:

  - Характеристик вірусів.

  - Підписів елементів ДПЗ.

  - Підписів "підозрілих функцій".

  - Підписів стандартних процедур використання системних ресурсів та зовнішніх пристроїв. Для цього використовуються спеціальні сканери сигнатур.

- Синтаксичний аналіз валідації: Пошук, ідентифікація та класифікація синтаксичної структури програми, а також побудова структурних та алгоритмічних

моделей самої програми. Виявлення синтаксичної структури ДПЗ є важливим, оскільки дозволяє шукати елементи ДПЗ, які не мають сигнатур. Структура та алгоритмічна модель програми є вирішальними для реалізації наступного типу аналізу – семантичного.

- Семантичний аналіз програм: Вивчення програм шляхом аналізу вмісту їхніх складових функцій (процедур) та їхньої поведінки в операційному середовищі комп'ютерної системи. На відміну від попередніх статичних аналізів, семантичний аналіз зосереджений на вивченні динаміки програми – її взаємодії з середовищем. Процес дослідження здійснюється у віртуальному операційному середовищі (динамічний аналіз, "пісочниці"), що дозволяє повністю контролювати роботу програми та відстежувати її алгоритм роботи за допомогою структурованої алгоритмічної моделі.

Актуальність: Семантичний аналіз є найефективнішим і найбільш трудомістким типом аналізу, оскільки він дозволяє виявляти складні, раніше невідомі загрози (наприклад, 0-*day* експлойти), які не можуть бути виявлені сигнатурними методами.

Сучасні підходи поєднують ці три аналітичні методи. Розроблені стандарти дозволяють раціонально комбінувати різні види аналізу, значно скорочуючи час дослідження без шкоди для якості.

3.2 Апаратні та програмно-апаратні рішення для захисту інформації

Сучасні стандарти віртуальних приватних мереж (*VPN*) ґрунтуються на багаторічному досвіді розробки засобів захисту інформації. Вони забезпечують комплексні функції, такі як керування ключами (наприклад, через протоколи, що прийшли на зміну *SKIP*, такі як *IKE*/*IKEv*2), автентифікацію, цілісність даних, конфіденційність та повне екранування локальної мережі. Сучасні *VPN*-рішення часто складаються з програмних та/або апаратних модулів, орієнтованих на захист різних елементів корпоративної мережі:

- Офісний шлюз (*Site-to-Site VPN*): Для захисту зв'язку між сегментами корпоративної мережі (наприклад, між головним офісом та філіями). - *VPN*-сервер (*Remote Access VPN*): Для надання безпечного віддаленого доступу співробітникам (мобільні клієнти, віддалені робочі місця). - Клієнтський модуль (*VPN Client*): Програмне забезпечення для кінцевих користувачів, що дозволяє їм безпечно підключатися до корпоративної мережі. - Модулі управління *VPN* та брандмауера: Централізовані системи для конфігурації, моніторингу та управління політиками безпеки.

Роль брандмауерів у захисті мережевої інформації

Брандмауери (*Firewalls*) є наріжним каменем мережевої безпеки, контролюючи інформаційний потік всередині та/або за межами автономної системи на основі встановлених адміністратором правил. Розміщення брандмауерів на межах локальних та глобальних мереж дозволяє фільтрувати вхідний та вихідний трафік, блокувати небажані з'єднання та запобігати несанкціонованому доступу до ресурсів.

Для захисту корпоративних мереж від атак з відкритих мереж (Інтернету) критично важливим є впровадження багаторівневого захисту (*Deep Defense*), часто реалізованого за допомогою послідовного (каскадного) розміщення декількох фільтрів. Типовим підходом є створення демілітаризованої зони (*DMZ*) (рисунок 3.4: "Схема мережі з *DMZ*, що показує зовнішній брандмауер, внутрішній брандмауер та сервери, розташовані в *DMZ* між ними.").

DMZ — це сегмент мережі, що містить інформаційні ресурси (наприклад, веб сервери, поштові сервери, *DNS*-сервери), які доступні з відкритої мережі, але відокремлені від внутрішньої корпоративної мережі. Це дозволяє надавати публічні послуги, не наражаючи внутрішню мережу на прямий ризик у разі компрометації зовнішнього сервера. У *DMZ* часто використовуються проксі сервери (як частина зовнішніх/внутрішніх брандмауерів або як окремі пристрої) для додаткової фільтрації та покращення безпеки, оскільки вони виступають посередниками між зовнішніми користувачами та внутрішніми ресурсами.

Брандмауери виконують роль зовнішнього та внутрішнього фільтрів, що

контролюють трафік на входах до *DMZ* та до внутрішньої мережі відповідно.

Рисунок 3.4 - Схема мережі з *DMZ*

Крім того, як у *DMZ*, так і в корпоративних мережевих середовищах, активно використовуються системи виявлення вторгнень (*IDS*) та системи запобігання вторгненням (*IPS*). Вони виявляють аномалії та вторгнення (наприклад, спричинені неправильною конфігурацією брандмауера або помилками програмного забезпечення) на основі непрямих ознак, таких як незвичайна мережева активність, сигнатури відомих атак або аномалії поведінки.

На практиці, сучасний брандмауер, особливо брандмауер наступного покоління (*NGFW*), часто є комплексним програмно-апаратним рішенням або спеціалізованим програмним продуктом, встановленим на обчислювальній платформі з кількома мережевими інтерфейсами. Це дозволяє забезпечити:

- Сегментацію мережі: Розділення мережі на ізольовані сегменти з незалежними політиками безпеки.
- Політики безпеки: Набір правил фільтрації для кожної пари інтерфейсів (сегментів корпоративної мережі). Наприклад:

- Зовнішні користувачі можуть отримувати доступ до певних сервісів у відкритих сегментах мережі (наприклад, веб-серверів) через визначені комунікаційні протоколи.

- Користувачі корпоративної мережі мають доступ до критично важливої інформації, розташованої на внутрішніх серверах, а також можуть використовувати проксі-сервіси в *DMZ* для доступу до зовнішніх мереж. - Управління безпекою часто здійснюється віддалено, що вимагає використання захищених каналів зв'язку (наприклад, *VPN*).

Мережеві рішення та засоби захисту на рівні протоколів

Інформаційна безпека мережі також значною мірою залежить від використання рішень та засобів захисту, що забезпечують безпеку на рівні протоколу *TCP*/*IP*. Хоча протокол *SKIP* (*Simple Key Management for Internet Protocol*) з 1994 року згаданий в оригіналі, наразі він застарів і його функції перейняли та значно розвинули інші протоколи, такі як *IPsec* (*Internet Protocol Security*) та *TLS* (*Transport Layer Security*).

1. *IPsec*: Це набір протоколів для забезпечення безпеки на мережевому рівні (рівень *IP*). *IPsec* надає такі функції:

- Автентифікація: Перевірка справжності відправника даних.

- Цілісність даних: Гарантія того, що дані не були змінені під час передачі. - Конфіденційність: Шифрування даних для запобігання несанкціонованому перегляду.

- Керування ключами: Автоматизоване генерування та обмін криптографічними ключами (наприклад, через протокол *IKE*/*IKEv2*). *IPsec* є основою для багатьох сучасних *VPN*-рішень.

2. Засоби на основі *IPsec* (аналоги "*SKIP bridge*", "*Sun Screen*"): Сучасні *VPN* шлюзи та апаратні брандмауери часто мають вбудовану апаратну підтримку *IPsec*. Ці пристрої, встановлені на межі внутрішньої та зовнішньої мережі, шифрують та фільтрують трафік, що проходить між ними, забезпечуючи безпеку даних та централізоване управління. Вони здатні виконувати розширену фільтрацію пакетів,

автентифікацію та забезпечувати конфіденційність трафіку, а також підтримують протоколи керування ключами для безпечної роботи та конфігурації. Переваги

використання брандмауерів:

Брандмауери значно покращують безпеку організації, одночасно контролюючи доступ до мережевих ресурсів. Розглянемо їхні ключові переваги: 1. Запобігання вразливостям сервісів: Брандмауери істотно покращують мережеву безпеку, фільтруючи служби, які за своєю суттю є небезпечними або вразливими. Це значно зменшує загрози для підмережі, оскільки лише безпечні протоколи можуть проходити через брандмауер. Наприклад, брандмауер може блокувати використання вразливих служб (як застарілий *NFS*) ззовні мережі, дозволяючи їх безпечне використання всередині. Це дозволяє безпечно використовувати зручні, але потенційно ризиковані служби, знижуючи витрати на управління. Крім того, брандмауери захищають від атак на основі маршрутизації, таких як атаки маршрутизації джерела або команди перенаправлення *ICMP*. Вони можуть блокувати такі пакети та сповіщати адміністраторів про спроби атак. 2. Керування доступом до мережевих систем: Брандмауери є ключовим інструментом для контролю доступу до мережевих хостів. Вони дозволяють налаштовувати детальні політики: наприклад, деякі хости (як-от веб-сервери) можуть бути доступні ззовні, тоді як інші (внутрішні бази даних) повністю заборонені до зовнішнього доступу. Мережа може блокувати зовнішній доступ до всіх своїх хостів, за винятком спеціально дозволених (наприклад, поштових або інформаційних серверів). Ці функції є критично важливими для реалізації принципу найменших привілеїв, який полягає в наданні доступу лише тим хостам або службам, яким це дійсно необхідно.

3. Централізована безпека: Брандмауери економічно вигідні для організацій, оскільки більшість оновлень програмного забезпечення та додаткових засобів безпеки можна встановити та централізовано керувати на брандмауері, а не розподіляти їх по великій кількості окремих хостів. Це особливо стосується рішень для надійної автентифікації, таких як системи одноразових паролів або багатофакторна автентифікація (*MFA*), які можна розгорнути на брандмауері, а не

на кожній системі, що потребує доступу до мережі. Хоча деякі методи безпеки (наприклад, *Kerberos*) вимагають модифікації на кожній системі, брандмауери, як правило, легше впроваджувати та масштабувати.

4. Покращена конфіденційність: Брандмауери відіграють важливу роль у підвищенні конфіденційності, блокуючи служби, які можуть надавати інформацію, корисну для зловмисників. Наприклад, вони можуть блокувати застарілі сервіси *Finger* (який надає інформацію про користувачів) або обмежувати *DNS*-запити ззовні, щоб приховати внутрішні імена хостів та *IP*-адреси. Це ускладнює розвідку для потенційних атак.

5. Журнали та статистика використання мережі: Оскільки весь мережевий доступ проходить через брандмауер, він може реєструвати доступ та надавати детальну статистику використання мережі. Завдяки правильно налаштованій системі сповіщень, брандмауер може надавати цінну інформацію про спроби атак, зондування або інші інциденти безпеки. Збір та аналіз цих даних є критично важливим для:

- Оцінки стійкості брандмауера до атак.
- Визначення ефективності існуючих заходів безпеки.
- Формування вимог до мережевого обладнання та програмного забезпечення.
- Проведення досліджень та аналізу ризиків.

6. Інтеграція політики в життя: Брандмауери є головним засобом для впровадження та забезпечення дотримання політик мережевого доступу. Вони надають технічний контроль доступу для користувачів та служб, що гарантує виконання політик незалежно від волі окремих користувачів. Це життєво важливо, оскільки організація не може покладатися на свідомість усіх користувачів

мережі. Обмеження та недоліки брандмауерів:

Хоча брандмауери є потужним інструментом, вони не є панацеєю від усіх проблем мережевої безпеки та мають певні недоліки:

1. Блокування корисних служб: Найбільш очевидний недолік полягає в тому, що брандмауер може блокувати багато служб, які потрібні користувачам

(наприклад, застарілі *TELNET, FTP, X Windows*). Однак це не є унікальним для брандмауерів; будь-який захист на рівні хоста також обмежує доступ відповідно до політик безпеки. Добре продумана політика безпеки, що балансує потреби безпеки з потребами користувачів, може значною мірою вирішити ці проблеми.

Іноді топологія мережі або використання певних служб (як *NFS*) може створювати значні обмеження для роботи брандмауера. У таких випадках необхідно провести ретельний аналіз ризиків, щоб зважити витрати на встановлення брандмауера проти потенційних збитків від атак. Можливо, інші рішення (наприклад, *Kerberos* або інші системи централізованої автентифікації) будуть більш підходящими, хоча й вони мають свої недоліки.

2. Не захищають від "бекдорів" та інсайдерських загроз: Брандмауери не захищають від усіх типів загроз. Наприклад, якщо зловмисник має несанкціонований доступ до мережі (наприклад, через скомпрометований модем або віддалений доступ), він може ефективно обійти брандмауер. Брандмауери також, як правило, не захищають від внутрішніх загроз (інсайдерських атак). Хоча брандмауер може запобігти несанкціонованому зовнішньому доступу до критичних даних, він не може перешкодити співробітнику скопіювати дані на зовнішній носій (наприклад, *USB*-флешку) і винести їх з мережі. Тому помилково вважати, що брандмауер повністю захищає від внутрішніх атак або що він є єдиним необхідним засобом захисту. Якщо існують інші шляхи витоку даних, інвестування всіх ресурсів лише в брандмауер може бути невиправданим.

Ключові компоненти брандмауера:

Основні компоненти сучасного брандмауера включають:

- Політика доступу до мережі: Визначає дозволений та заборонений трафік. - Механізми надійної автентифікації: Перевірка справжності користувачів та систем.

- Фільтрація пакетів: Контроль мережевого трафіку на основі різних критеріїв.

- Шлюзи прикладного рівня (*Application Layer Gateways*/*Proxies*): Деталізований контроль трафіку на рівні конкретних застосунків.

Існує два типи політик доступу до мережі, що впливають на проєктування, встановлення та використання системи брандмауера:

- Концептуальна політика (високорівнева): Визначає, яким службам буде дозволено або явно заборонено доступ, як їх можна використовувати, та за яких

обставин робляться винятки. Це відображає загальну стратегію безпеки організації.

- Політика проєкту брандмауера (низькорівнева): Описує, як брандмауер фактично обмежуватиме доступ та фільтруватиме служби. Вона розробляється з урахуванням можливостей та обмежень конкретного брандмауера, а також загроз, пов'язаних з *TCP/IP*.

Зазвичай реалізується одна з двох основних спеціальних політик: 1. "Дозволяти все, що не заборонено" (*Permissive by default*): Дозволяє весь трафік, якщо служба явно не заборонена в політиці контролю доступу. Цей підхід є менш безпечним.

2. "Заборонити все, що не дозволено" (*Restrictive by default* / *Deny by default*): Забороняє весь трафік, крім того, що явно вказаний у списку дозволених служб. Ця політика відповідає класичній моделі доступу, що є найбільш безпечною та широко використовуваною в усіх сферах інформаційної безпеки.

Політика доступу до послуг є найважливішим компонентом, а інші три використовуються для її реалізації. Ефективність брандмауера залежить від його типу реалізації, правильності налаштування та відповідності обраній політиці доступу.

Подолання вразливостей традиційних паролів за допомогою надійної автентифікації:

Протягом багатьох років користувачам радили вибирати складні паролі та нікому їх не розголошувати. Проте, навіть якщо користувачі дотримуються цих порад, факт того, що зловмисники можуть контролювати мережевий трафік, перехоплювати паролі та використовувати різні атаки (наприклад, *Brute-Force*, *Credential Stuffing*, *Phishing*), робить традиційні паролі недостатньо надійними.

Для боротьби з цими вразливостями розроблено багато засобів надійної автентифікації, таких як:

- Смарт-картки
- Біометрія (відбитки пальців, розпізнавання обличчя)
- Програмні токени (*Authenticator apps*)

- Апаратні ключі безпеки (наприклад, *FIDO U2F*/*WebAuthn*)

Спільним для всіх цих заходів є те, що згенеровані ними одноразові паролі (*OTP*) або криптографічні відповіді не можуть бути повторно використані зловмисниками у разі перехоплення. Оскільки проблема з паролями в Інтернеті залишається актуальною, критично важливо захистити мережеві з'єднання, які не використовують надійні методи автентифікації, за допомогою брандмауера.

Системи одноразових паролів є одними з найпопулярніших рішень для надійної автентифікації. Наприклад, смарт-картка або програмний токен генерує унікальну відповідь для кожного сеансу, замінюючи традиційний статичний пароль.

Оскільки брандмауери централізовано контролюють доступ до мережі, вони є логічним місцем для інтеграції засобів надійної автентифікації. Хоча надійну автентифікацію можна використовувати на будь-якому хості, практичніше розміщувати її на брандмауері.

Рисунок 3.5: "Схема, що порівнює автентифікацію без брандмауера та з брандмауером, що використовує сильну автентифікацію. У першому випадку, неавтентифікований трафік (наприклад, *TELNET*, *FTP*) надходить безпосередньо в мережу, створюючи ризик перехоплення паролів. У другому – весь трафік з Інтернету (включаючи *TELNET*, *FTP*) спочатку проходить сильну автентифікацію на брандмауері, що унеможливлює використання перехоплених внутрішніх паролів для обходу захисту."

Навіть якщо внутрішні системи все ще вимагають статичних паролів, інтеграція сильної автентифікації на брандмауері гарантує, що зловмисники не зможуть проникнути або обійти брандмауер, використовуючи скомпрометовані паролі.

Рисунок 3.5 - "Схема, що порівнює автентифікацію без брандмауера та з брандмауером

Фільтрація пакетів:

Фільтрація *IP*-пакетів є базовою функцією більшості маршрутизаторів та брандмауерів. Вона виконується під час проходження пакетів між мережевими інтерфейсами маршрутизатора/брандмауера. Сучасні маршрутизатори з фільтрацією можуть фільтрувати *IP*-пакети на основі комбінації таких полів:

- *IP*-адреса відправника: Запобігає трафіку з певних джерел.
- *IP*-адреса одержувача: Контролює доступ до певних цілей.
- *TCP*/*UDP*-порт відправника: Дозволяє фільтрувати трафік за вихідним портом.
- *TCP*/*UDP*-порт одержувача: Дозволяє фільтрувати трафік за цільовим портом (наприклад, блокувати доступ до веб-серверів на порту 80, або дозволяти лише *HTTPS* на порту 443).

Більшість сучасних фільтруючих маршрутизаторів підтримують фільтрацію за *TCP*/*UDP*-портами. Деякі маршрутизатори також перевіряють мережевий інтерфейс, з якого надійшов пакет, і використовують цю інформацію як додатковий критерій фільтрації.

Використання фільтрації пакетів:

- Блокування з'єднань з певних джерел/до певних цілей: Організація може блокувати з'єднання з відомих шкідливих *IP*-адрес або мереж, або ж дозволяти лише винятковий доступ до певних внутрішніх систем (наприклад, *SMTP*-серверу для пошти).

- Контроль доступу за службами (портами): Додавання фільтрації портів *TCP* та *UDP* до фільтрації *IP*-адрес забезпечує величезну гнучкість. Оскільки сервіси (наприклад, веб-сервер на порту 80/443, *SSH* на порту 22) прив'язані до певних портів, брандмауер може дозволяти лише певні типи з'єднань з певними хостами. Наприклад, організація може блокувати всі вхідні з'єднання, за винятком декількох систем у межах брандмауера, які можуть дозволяти лише визначені служби (наприклад, *SMTP* на одній системі та захищений *SSH* на іншій).

Рисунок 3.6: "Схема мережі з брандмауером, що демонструє функцію фільтрації пакетів. На ній показано, як брандмауер перевіряє *IP*-адреси джерела/призначення та порти *TCP*/*UDP*, приймаючи рішення про дозвіл чи заборону пакетів."

Рисунок 3.6 - "Схема мережі з брандмауером, що демонструє функцію фільтрації пакетів

Завдяки фільтрації портів *TCP* та *UDP,* цю стратегію можна легко реалізувати за допомогою брандмауера або маршрутизатора з можливостями фільтрації пакетів, значно підвищуючи гранулярність контролю доступу.

ВИСНОВКИ

Підсумовуючи проведену роботу, можна зробити низку ключових висновків щодо сучасних підходів до безпеки програмного забезпечення та мережевого захисту:

1. Еволюція загроз: Зі зростанням складності інформаційних систем, загрози

безпеці також еволюціонують. Від простих "електронних закладок" до високоінтелектуального шкідливого програмного забезпечення (ШПЗ) та прихованих алгоритмічних/програмних закладок – атаки стають все більш витонченими. Це вимагає постійного оновлення методів захисту та проактивного підходу.

2. Критичність захисту КІІ: Захист критичних інформаційних інфраструктур (КІІ) є життєво важливим для національної безпеки, економічної стабільності та суспільного функціонування. Компрометація таких систем може мати катастрофічні наслідки, підкреслюючи необхідність застосування найсучасніших та найнадійніших засобів безпеки.

3. Безпека на всіх етапах життєвого циклу ПЗ: Загрози виникають не лише під час експлуатації, а й на етапах проєктування, розробки та тестування програмного забезпечення. Принципи *Security by Design* та *DevSecOps* стають обов'язковими, вимагаючи інтеграції безпеки в кожен етап життєвого циклу програмного продукту, а також безперервного контролю діяльності розробників та користувачів.

4. Комплексний підхід до безпеки ПЗ: Забезпечення технічної та операційної безпеки програмного забезпечення вимагає застосування багатовекторних методів аналізу — від лексичного та синтаксичного до глибокого семантичного аналізу. Поєднання цих методів, а також інспекцій, тестування та контролю, дозволяє ефективно виявляти як відомі, так і потенційно невідомі вразливості та шкідливі закладки.

5. Роль брандмауерів: Брандмауери (*Firewalls*), зокрема брандмауери наступного покоління (*NGFW*), залишаються центральним елементом мережевої безпеки. Вони забезпечують багаторівневий контроль доступу, сегментацію мережі

та ефективне фільтрування трафіку. Розгортання демілітаризованих зон (*DMZ*) та використання брандмауерів для реалізації політики "заборонити все, що не дозволено" є ключовими для побудови захищеної мережевої архітектури.

6. Важливість надійної автентифікації: Традиційні паролі є вразливими до

сучасних кібератак. Впровадження багатофакторної автентифікації (*MFA*) та систем одноразових паролів, централізовано керованих на брандмауерах або окремих сервісах автентифікації, є критично важливим для захисту доступу до мережевих ресурсів.

7. Обмеження та баланс: Хоча брандмауери значно підвищують безпеку, вони не є універсальним рішенням. Вони не можуть захистити від внутрішніх загроз або обходу через несанкціоновані точки доступу. Тому успішна стратегія кібербезпеки вимагає комплексного підходу, що поєднує технічні засоби (брандмауери, *IDS*/*IPS*,
антивірусне ПЗ) з організаційними заходами, політиками безпеки, аналізом ризиків та навчанням користувачів.

Загалом, ефективна кібербезпека в сучасному світі полягає у постійній адаптації, інтеграції безпеки на всіх етапах розробки та експлуатації систем, а також у розумінні обмежень окремих інструментів для створення справді стійких та захищених інформаційних екосистем.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *ISO*/*IEC* 27001:2022. *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*. – Женева : *ISO,* 2022. – 50 с.

2. *ISO*/*IEC* 27701:2019. *Security techniques – Extension to ISO*/*IEC* 27001 *and ISO*/*IEC* 27002 *for privacy information management – Requirements and guidelines*. – Женева : *ISO,* 2019. – 76 с.

3. *NIST SP* 800-122. *Guide to Protecting the Confidentiality of Personally Identifiable Information* (*PII*) / *National Institute of Standards and Technology*. – Гейтерсберг : *NIST,* 2010. – 59 с.

4. *General Data Protection Regulation* (*GDPR*). *Regulation* (*EU*) 2016/679 *of the European Parliament and of the Council*. – Брюссель, 2016. – 88 с. 5. *OWASP*: *Privacy Risks and Security Controls*. – [Електронний ресурс]. – Режим доступу: *https*://*owasp.org* (дата звернення: 30.05.2025).

6. *Cisco*: *Data Privacy and Protection*. – [Електронний ресурс]. – Режим доступу: *https://www.cisco.com* (дата звернення: 30.05.2025).

7. *Microsoft*: *Protecting Personal Data in the Cloud*. – [Електронний ресурс]. – Режим доступу: *https://learn.microsoft.com* (дата звернення: 30.05.2025). 8. *ISO/IEC* 29100:2011. *Information technology – Security techniques – Privacy framework*. – Женева : *ISO*, 2011. – 36 с.

9. *ISO/IEC* 27018:2019. *Code of practice for protection of personally identifiable information* (*PII*) *in public clouds*. – Женева : *ISO*, 2019. – 44 с.

10. ДСТУ *ISO/IEC* 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. – К. : Мінекономрозвитку України, 2016. – 44 с.

11. Закон України «Про захист персональних даних» №2297-*VI* від 01.06.2010 р. – [Електронний ресурс]. – Режим доступу: *https://zakon.rada.gov.ua* (дата звернення: 30.05.2025).

12. Копець С.В. Основи інформаційної безпеки в мережах. – К. : Ліра-К, 2021. – 248 с.

13. Михайленко В.О. Захист персональних даних в інформаційних системах. – Львів : Новий Світ – 2000, 2022. – 204 с.

14. Савчук І.М. Системи захисту інформації: навчальний посібник. – Київ : КНЕУ, 2020. – 312 с.

15. Білоус О.В. Криптографічні методи захисту персональних даних. – Системи управління та автоматики. – 2023. – №3. – С. 28–35.

16. Теслюк В.М., Базильчук Я.Ю. Захист інформації в комп'ютерних системах. – Львів : Видавництво Львівської політехніки, 2019. – 296 с. 17. Марченко І.О. Організаційні аспекти безпеки персональних даних у корпоративному середовищі. – Вісник ХНУРЕ. – 2022. – №2. – С. 38–45. 18. Наказ Уповноваженого ВРУ з прав людини №1/02-14 від 08.01.2014 «Про затвердження Методичних рекомендацій щодо обробки персональних даних». – [Електронний ресурс]. – Режим доступу: *https://ombudsman.gov.ua* (дата звернення: 30.05.2025).

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

РЕЦЕНЗІЯ

на кваліфікаційну роботу

випускника спеціальності: 123 «Комп'ютерна інженерія»

відділення: комп'ютерної та програмної інженерії

циклова комісія: комп'ютерних систем та мереж

Анатолій БАЛАБАНОВ
(ім'я, прізвище)

1. Актуальність теми: Обрана тема кваліфікаційної роботи «Безпека персональних даних на підприємстві» є актуальною.

2. Кваліфікаційна робота відповідає темі, затвердженій наказом.

3. Завдання на виконання кваліфікаційної роботи виконано у повному обсязі.

4. В результаті виконання кваліфікаційної роботи були поставлені і успішно вирішені завдання розробки систем захисту інформації комп'ютерних мереж від спаму.

5. Якість виконання пояснювальної записки та ілюстративного (графічного) матеріалу відповідає вимогам Державних стандартів.

6. В кваліфікаційній роботі зроблений акцент на дані отримані на практиці («живі» експерименти).

7. Кваліфікаційна робота заслуговує оцінку «добре».

Рецензент _____
(науковий ступінь, посада)

«____»_____ 2025 р. _____ Андрій КРАВЧАТИЙ
(підпис) (ім'я, прізвище)

З рецензією ознайомлений _____ Анатолій БАЛАБАНОВ
(підпис) (ім'я, прізвище)