KAPITEL 6 / *CHAPTER 6* [6]
COMPREHENSIVE CORPORATE NETWORK PROTECTION: APPROACHES AND SOLUTIONS

DOI: 10.30890/2709-2313.2025-38-02-001

Вступ

Сучасний стан розвитку інформаційних технологій сприяє невпинному зростанню кількості загроз безпеці корпоративних мереж [1–3] і систем, що вони їх обслуговують [4–5]. Це зумовлює необхідність розроблення нових або вдосконалення існуючих методів та моделей комплексного захисту інформаційних систем [6–7]. Подана в монографії глава присвячена дослідженню та впровадженню методу комплексного захисту корпоративної мережі, який ґрунтується на виокремленні двох окремих стеків безпеки – мережевого (Network Stack) та вузлового (Host Stack) [8–11]. Такий підхід дає змогу системно розглядати й узгоджувати широкий спектр інженерно-технічних, програмних та криптографічно-стеганографічних заходів. У роботі спочатку подається узагальнений технологічний ланцюжок комплексного захисту корпоративної мережі, де окреслено правові, організаційно-адміністративні та інженерно-технічні аспекти. Далі детально аналізуються інженерно-технічні заходи, до яких належать фізичні, апаратні, програмні, криптографічні та стеганографічні засоби. На завершення пропонується власне метод комплексного захисту корпоративної мережі, а також формальна модель, що дає змогу кількісно оцінити ступінь захищеності на різних рівнях.

[6] ***Authors:*** *Korobeinikova Tetiana I.*
Number of characters: *36379*
Author's sheets: *0,91*

6.1. Узагальнений технологічний ланцюжок комплексного захисту корпоративної мережі

Для того щоб організувати надійний комплексний захист корпоративної мережі (КЗКМ) проводяться такі заходи [12]: правові; організаційно-адміністративні; інженерно-технічні. До міжнародних правових норм віднесемо: авторські права; угоди; ліцензії; патенти; договори. До національних правових норм віднесемо: Конституція; укази; нормативні акти; кодекси; керівні документи; інструкції. До організаційних заходів віднесемо: пропускний режим; зберігання документів; порядок обліку та знищення документів; облік захисних мір при проектуванні та будівництві КМ; навчання правилам роботи з таємною інформацією. До адміністративних заходів віднесемо: підтримка правильної конфігурації ОС; контроль журналів логів; контроль зміни паролів; виявлення «дірок» в системі захисту; проведення тестувань засобів захисту інформації.

Схематичне зображення узагальненого технологічного ланцюжка комплексного захисту корпоративної мережі наведено на рисунку 1. Почнемо з того, що будь-яка організація володіє певним набором активів. Активи – все, що представляє цінність для організації і повинно бути захищене в тому числі сервери, пристрої мережевої інфраструктури, кінцеві пристрої і найголовніший ресурс – дані [13–14]. Саме дані формують інформаційні активи і у свою без інформації немає інформаційних активів. Інформація може існувати у різних формах і видах, і мати різні прояви (акустична, сигнальна (аналогово-цифрова, об'ємно-видова)). Таким чином, з'являється необхідність у використанні різних засобів захисту цієї інформації у корпоративних мережах.

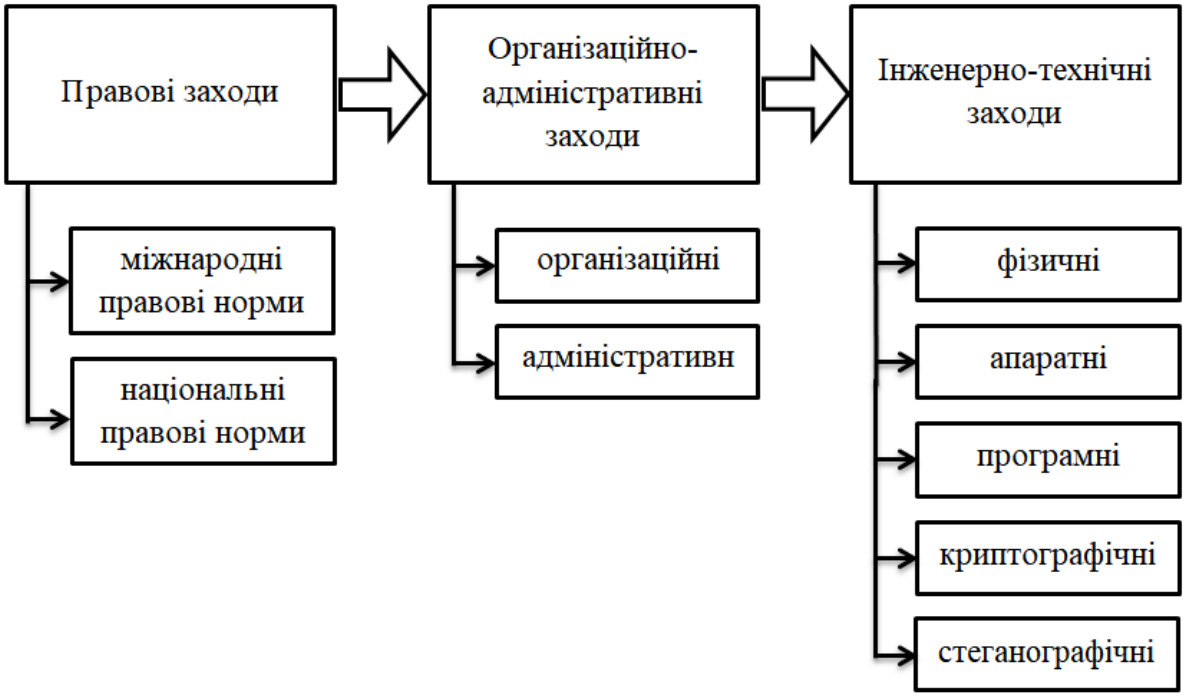

Рисунок 1 Схема узагальненого технологічного ланцюжка комплексного захисту корпоративної мережі

Авторська розробка на основі аналізу відкритих джерел

6.2. Розширений опис інженерно-технічних засобів моделі комплексного захисту корпоративної мережі

На рис. 1 зображено перелік інженерно-технічних заходів. До таких заходів відносять: фізичні; апаратні; програмні; криптографічні; стеганографічні. Використовуючи цей список, ми запропонуємо модель інженерно-технічного комплексного захисту корпоративної мережі.

6.2.1 Фізичні заходи

Фізичні заходи комплексного захисту корпоративної мережі необхідні для захисту персоналу, апаратних засобів, програмного забезпечення, мереж і даних від фізичних дій і подій, які можуть нашкодити підприємству чи установі. Впровадження фізичних заходів призначене для мінімізації витрат часу, грошей та ресурсів. Фізичні заходи комплексного захисту корпоративної мережі можна

умовно поділити на три категорії: контроль доступу, спостереження та тестування. Нижче опишемо кожну з них.

Контроль доступу. Активи підприємства можуть представляти цінність також і для зловмисників. Важливим є запобігання витоку інформації, що обробляється. Одним із способів уникнення цього є фізичне обмеження доступу до оброблюваної інформації, у тому числі розширення контрольованої зони. Контрольована зона – це територія, у якій виключена поява осіб і транспортних засобів, що не мають постійних чи тимчасових перепусток. На межі контрольованої зони та території, що не належить такій зоні можуть використовуватися фізичні бар'єри (огорожі, боларди, турнікети). Розглянемо деякі фізичні бар'єри.

Моделі управління доступом. До інформаційних активів, якими володіє підприємство, доступ має бути обмеженим. Це робиться для того, щоб відповідною інформацією могли користуватися лише працівники об'єкту. Процес застосування заходів контролю доступу може бути трудомістким, а також може потребувати фінансових витрат.

Суть контролю доступу полягає у тому, що ніхто не повинен мати більше привілеїв, ніж це необхідно для виконання його посадових обов'язків. Існує 4 основних моделі, де враховані як специфіки суб'єктів, так і ступінь важливості безпеки об'єктів або ресурсів. Моделі управління доступом поділяються на: дискреційне (виборче) управління (DAC); обов'язковий (мандатний) метод управління (MAC); рольова модель управління (RBA); управління доступом на основі правил (RBA).

Пункт контролю доступу (Access control vestibules, mantrap). Зазвичай, це невелике приміщення з вхідними дверима, що забезпечують доступ до цього приміщення, і внутрішніми дверима цього приміщення, які забезпечують доступ до об'єкту, ЦОД, наприклад. Можлива різна конфігурація механізмів замикання дверей пункту контролю доступу. Може бути так, що всі двері цього приміщення, зазвичай, відчинені, поки одна людина не відкриє двері. І як тільки ці двері відчиняються, всі інші двері в тамбурі замикаються автоматично. Або всі двері

зазвичай замкнені, і якщо відмикаються одні з цих дверей, це унеможливлює відмикання інших дверей в той самий час. Диктофон, відеокамери спостереження, металошукачі (для запобігання входу озброєних людей) можуть використовуватися у цьому приміщенні для того, щоб спеціально навчений працівник міг контролювати це приміщення з віддаленого місця. Існують різні способи ідентифікації для дверей, а також їхні комбінації. Наприклад, одні двері можна відчинити ключем, а інші – відчиняться після введення персонального ідентифікаційного. Також можуть використовуватися ключ-карти, біометричні пристрої, тощо.

Сигналізація. Основним призначенням охоронної сигналізації є виявлення спроб несанкціонованого подолання фізичних бар'єрів та оповіщення про такі спроби. Охоронна сигналізація може бути автономною, з автоматичним додзвоном та пультова.

Окрім охоронної сигналізації варто згадати і про систему пожежної сигналізації (СПС). Вона на ранній стадії виявляє ознаки пожежі, а також сповіщає пристрої передавання пожежної тривоги і попереджає про несправності, що можуть впливати на роботу самої СПС.

Біометрія. Біометрія – це сукупність автоматизованих методів ідентифікації й/або аутентифікації людей на основі їх фізіологічних і поведінкових характеристик. Біометричні дані, такі як відбиток пальця; сітківка ока; форма обличчя, долоні, вуха; рукописний/клавіатурний почерк; голос та інші є надійним та потужним фізичним заходом контролю. Це пов'язано з тим, що біометричні дані дуже важко змінити і скопіювати, а також вони пов'язані лише з конкретною людиною.

Блокувальник даних USB (USB data blocker). Блокувальник даних USB – це невеликий пристрій, який служить захистом від ризиків зараження вашого пристрою шкідливим програмним забезпеченням.

Кабельний замок (Cable lock). Це невеликий отвір у корпусі ноутбука чи монітору, у який вставляється спеціальний замок із металевим тросом, який у свою чергу кріпиться або обмотується навколо нерухомих предметів.

Спостереження. Спостереження виступає важливою складовою фізичної безпеки. Воно потрібне для моніторингу ситуації у різних місцях одночасно. Також цей компонент фізичної безпеки відіграє важливу роль у запобіганні різного роду інцидентів і відновленні після їх виникнення.

Камери спостереження. Призначенням системи відеоспостереження є централізоване спостереженні за об'єктом у режимі реального часу, а також створення записів (архівів). Така система повинна бути реалізована на надійному обладнанні, яке має бути сертифікованим, тобто мати документи, що підтверджують якість такого обладнання. Для системи відеоспостереження можуть бути інтегровані засоби фільтрації трафіку (міжмережеві) та антивірусне ПЗ (якщо використовуються IP-камери.

Сенсори і датчики. Деяку інформацію про стан об'єкта, який захищають отримують сенсорів. Сенсором називають пристрій, який безпосередньо сприймає інформацію про стан об'єкта, що охороняється і перетворює її на таку, яку зручно передавати каналом зв'язку. Зазвичай, сенсори реєструють неелектричні величини. Опишемо деякі поширені сенсори: сенсори розбиття скла: інфрачервоні (ІЧ) сенсори; магнітоконтактні сенсори; улектроконтактні сенсори; ємнісні сенсори.

Захищена система розподілу (protective distribution system (PDS)). Основною метою захищеної системи розподілу є запобігання або утруднення фізичного доступу до мережевої кабельної інфраструктури. Така система робить майже неможливим фізичний доступ до мережевих кабелів. При використанні PDS, кабелі надзвичайно важко пошкодити (розрізати чи розірвати).

Охоронне освітлення. Охоронне освітлення передбачається у випадку потреби охорони об'єкта захисту у темний час доби. Таке освітлення встановлюється по периметру об'єкта захисту.

Дрони. Використовуються для контролю чи спостереження за великими територіями, особливо якщо вони розташовані у такій місцевості, куди важко дістатися. Перевагою дронів є те, що вони можуть швидко «покрити» відносно велику територію за досить короткий час. Вони можуть виконувати складні

задачі у небезпечних умовах без ризику для здоров'я і життя людини.

Тестування систем безпеки. Впровадження заходів фізичної безпеки потрібне для запобігання інцидентам інформаційної безпеки, а також для реагування на них. Одним із способів реагування на певні події є виконання плану аварійного відновлення. Тестування дозволяє зрозуміти на скільки ефективним є такий план. Саме завдяки тестуванню можна виявити його недоліки, а також координувати персонал і відпрацьовувати методи реагування на ті, чи інші події безпеки.

6.2.2 Апаратні заходи

Завдання заходів, котрі забезпечують апаратну безпеку, полягає у захисті фізичних пристроїв від загроз, що можуть сприяти несанкціонованому доступу до систем організації. Апаратні заходи захисту інформації комп'ютерних мереж охоплюють розробку апаратного забезпечення, контроль доступу, безпечні багатосторонні обчислення, безпечне зберігання ключів, а також забезпечення автентичності коду. Дозволяємо собі не наводити класифікацію апаратних заходів. Оскільки, на фізичному рівні працюють стандартизовані специфікації.

Апаратний модуль безпеки (Hardware security module, HSM) є фізичним пристроєм, який призначений для генерації, захисту ключів та їхнім управлінням. Такі ключі використовуються для шифрування та розшифрування даних, а також генерації цифрових підписів. Серед переваг апаратних модулів безпеки можна віднести: підтримка стандартних криптографічних алгоритмів; генерування ключів, управління ними; виконання функцій шифрування та створення цифрового підпису; вбудоване сховище криптографічних ключів; можливість безпечного резервного копіювання ключів; висока продуктивність; розвантаження серверів додатків; стійкість до несанкціонованого доступу (двофакторна аутентифікація).

Trusted platform module, TPM. TMP – це криптографічний модуль, реалізований у вигляді спеціалізованого чіпа. Сам чіп TMP припаюють до материнської плати ноутбука чи настільного комп'ютера. Дискретна реалізація

TMP є досить популярною, хоча можуть виникати проблеми для інтегрованих пристроїв, особливо, якщо вони невеликих розмірів і низьким енергоспоживанням. Також існують реалізації TMP, у яких функції модуля вбудовуються в той самий чіпсет, що й деякі інші компоненти і при цьому, використовують логічне розділення.

TMP призначений для захисту апаратного обладнання за допомогою вбудованих криптографічних ключів. Окрім цього, модуль допомагає підтвердити особу користувача та аутентифікувати його пристрій. Кожен чіп має ключ підтримки (Endorsement Key, EK). EK є ключем RSA. Має відкриту і закриту частини. Закрита частина ключа не повинна бути доступною за межами чіпу TPM. Використовується у процесі генерації ключів підтвердження справжності, а також для встановлення власника TPM.

Кореневий ключ сховища (Storage Root Key, SRK) створюється, коли користувач стає власником системи. Він генерується на основі EK та вказаного власником пароля (якщо зміниться користувач, зміниться і SRK). Цей ключ використовується для створення криптографічних ключів та їх шифрування так, що створені ключі може розшифрувати лише той TMP, на якому вони були згенеровані. Такий процес носить назву «обгортання» або «зв'язування» ключа. Простішими словами, усі ключі, що використовуються власником TPM для підписання та шифрування, фактично, є дочірніми для SRK.

Генератори випадкових чисел (ГВЧ). Такі пристрої створені для генерації послідовності випадкових чисел, тобто таких, послідовність яких не відповідає ніякому шаблону.

Апаратне повне шифрування диску (Hardware Full disk encryption, FDE). Головним завданням є захист інформації, яка зберігається на жорсткому диску, шляхом перетворення її у нечитабильний код, який буде дуже важко розшифрувати неавторизованим користувачам. Шифрується кожен біт даних диску.

Проксі-сервери. Виступає «посередником» між клієнтом і мережевими сервісами, запити до яких робить клієнт. Сам процес, у якому задіяний проксі

сервер можна описати наступним чином. Клієнт звертається до проксі-сервера і запитує в нього потрібний йому ресурс, який знаходиться на іншому сервері, наприклад, на сервері електронної пошти. Далі проксі-сервер підключається до вищезгаданого сервера і отримує потрібний користувачу ресурс і надсилає йому цей ресурс.

6.2.3 Програмні заходи

На програмні заходи покладають багато важливих завдань. Їх впроваджують для захисту інформації у БД, від несанкціонованого доступу до мережевих ресурсів, під час передачі каналами зв'язку, тощо. Також програмні заходи використовуються для розмежування та контролю доступу до активів, ідентифікації й аутентифікації користувачів. У мережевій безпеці такі заходи потрібні для фільтрації мережевого трафіку, контролю і розмежування доступу до мережевих ресурсів і т.д.

Міжмережеві екрани (МЕ). Міжмережевий екран реалізує політику управління доступом між мережами. Використовується для контролю або фільтрації повідомлень, яким дозволено входити/виходити до/з пристрою або мережі. Кожен МЕ повинен відповідати певним вимогам, при його впровадженні в мережу, а саме:

- стійкість до мережевих атак;
- беручи до уваги те, що мережевий трафік проходить із зовнішніх мереж через міжмережевий екран у внутрішню корпоративну мережу, брандмауер повинен бути єдиною транзитною точною між вхідним і вихідним трафіком;
- застосування політики управління доступом.

Зважаючи на те, що мережеві та комп'ютерні атаки постійно вдосконалюються і стаються складнішими і серйознішими, постійно розробляються нові та вдосконалюються вже наявні міжмережеві екрани для забезпеченні надійного захисту інформації у мережі. Опишемо деякі з поширених брандмауерів.

МЕ з фільтрацією пакетів. Працює на мережевому і транспортному рівнях моделі OSI. Є частиною МЕ маршрутизатора. Без контролю стану, використовує простий пошук в таблиці політик

МЕ зі збереженням стану. Працює на мережевому, транспортному та сеансовому рівнях моделі OSI. Є найпоширенішим. ВонВіни використовує інформацію про активні підключення, що зберігається у таблиці станів.

МЕ шлюзу додатків (на проксі-сервері). Працює на мережевому, транспортному, сеансовому, та прикладному рівнях моделі OSI. Велика частина функцій керувань і фільтрації виконується на програмному рівні. Проксі-сервер підключається до віддаленого сервера від імені клієнта. Таким чином, цей сервер бачить тільки підключенні проксі-сервера.

МЕ на зворотному проксі-сервері. Такий брандмауер розміщується перед веб-сервером. Він може захищати, приховувати, розвантажувати та розподіляти доступ до веб-серверів.

МЕ на основі хоста. ПК або сервер з запущеним на ньому спеціальним ПЗ Такі фаєрволи фільтрують порти та виклики системних служб на одному комп'ютері.

Прозорий МЕ. Фільтрує IP-трафік між парою інтерфейсів з мостовим з'єднанням.

Гібридний МЕ. Є поєднанням МЕ різних типів. Міжмережеві екрани нового покоління. Міжмережеві екрани нового покоління, окрім можливостей стандартних брандмауерів мають такі вдосконалення:

- вбудована IPS;
- дані про додатки і керування ними для пошуку і блокування небезпечних додатків;
- варіанти оновлення для включення майбутніх інформаційних каналів;
- забезпечення захисту від постійного виникнення нових загроз безпеки.

Список контролю доступу (Access Control List, ACL). Списки контролю доступу – це списки правил, які визначають легітимність мережевого трафіку до

об'єкту. Тобто, використовуючи їх можна визначити хто може отримувати доступ до певного об'єкту і що йому дозволено або заборонено робити з цим об'єктом. ACL складають відповідно до раніше визначених критеріїв. Такі критерії мають порядок важливості, адже дозвіл чи відмова у доступі до об'єкту залежить саме від них.

Перетворення мережевих адрес (network Address Translation, NAT). За допомогою NAT можна замінювати IP-адреси пристроїв приватної мережі на публічні IP-адреси. Застосування NAT потрібне для економії IP-адрес, які використовуються в організації, а також у цілях безпеки.

Active Directory (AD). Active Directory – це набір служб і база даних (каталог), які призначені для об'єднання користувачів із необхідними їм мережевими ресурсами. Мережі AD можуть містити від кількох сотень до кількох мільйонів об'єктів. AD призначена для полегшення і прискорення розгортання ПЗ, встановлення його оновлень на великій кількості комп'ютерів мережі, а також для зберігання даних у централізованій базі даних. У цій базі даних міститься важлива інформація про те, які користувачі та комп'ютери є у середовищі та що й кому дозволено робити. Сюди вносять детальні відомості про користувачів та їхні дозволи. Набір служб призначений для контролю того, що відбувається у середовищі. Служби відповідають за аутентифікацію та авторизацію.

SSH, Telnet. Завданням цих протоколів полягає у забезпеченні віддаленого управління операційною системою і тунелювання TCP-з'єднань для передачі файлів. Ці два протоколи функціонально схожі, але на відміну від Telnet, SSH шифрує весь трафік, а також дає можливість вибрати алгоритми шифрування. Тут описуватиметься лише протокол SSH, оскільки, він виконує ті ж задачі що і Telnet, але є безпечнішим, популярнішим і новішим. SSH – Secure Shell – безпечна оболонка.

6.2.4 Криптографічні заходи

Криптографію використовують для передачі важливої інформації надійним

чином. Використовуючи шифри, інформація захищається так, щоб тільки той, кому призначена ця інформація міг її обробити і зрозуміти. У криптографії математичні методи (зокрема інструменти абстрактної алгебру та теорії ймовірностей) необхідні для забезпечення тріади CIA.

Зараз існує три типи криптографії: симетрична криптографія, асиметрична криптографія та криптографічні хеш-функції.

У симетричні криптографії відправник та одержувач повідомлення використовують один ключ для шифрування і розшифрування. У асиметричні криптографії використовується пара ключів. Один з них є відкритим, його можна вільно розповсюджувати і він використовується для шифрування, а інший є секретним, такий ключ тримають у таємниці і застосовують для дешифрування.

Важливе місце у криптографії посідають хеш-функції. Такі функції призначені для обчислення коротких чисел фіксованого розміру – хешу. На вхід може подаватися рядок довільної довжини. Показником якості хеш-функцій служить складність знаходження двох різних відкритих повідомлень, які мають однакові значення хешу. Таке явище називається колізією. Якщо два повідомлення мають однакові хеші, можна бути впевненим, що це одне і те саме повідомлення.

6.2.5 Стеганографічні заходи

Стеганографією називають техніку приховування повідомлень так, щоб вони не виглядали як повідомлення, тобто приховується факт їхнього існування. Стеганографію можна застосовувати і для захисту інформації при передачі комп'ютерними мережами. Таку стеганографію називають мережевою. В основі її методів лежать певні особливості роботи мережевих протоколів, а також взаємозв'язки між цими протоколами. Мережева стенографія має багато методів, такими є WLAN стеганографія, LACK стеганографія, DAB- і DVB стеганографія.

WLAN стеганографія. Система HICCUPS. Використовується у бездротових локальних мережах. Прикладом використання такого методу стеганографії є система HICCUPS – Hidden Communication System for Corrupted Networks.

LACK стеганографія (Lost Audio Packets Sreganography). Використовується для приховування повідомлень під час розмов з використанням IP-телефонії. Основною метою використання IP-телефонії є перетворення аналогового звукового сигналу у цифрове представлення від одного абонента і передача цього сигналу цифровими каналами зв'язку до іншого абонента, де проводяться зворотні перетворення. Важливу роль відіграють протоколи RTP (Real-Time Transport Protocol). У мультимедійних комунікаційних протоколах, в тому числі і у протоколах RTP, надто затримані пакети відкидаються, оскільки, вважаються помилковими.

Сам процес роботи LACK стеганографії можна описати так. Відправник обирає пакет з голосового потоку і замість корисного навантаження цього пакету вбудовує секретне повідомлення. Такий пакет затримується навмисно. Одержувач, котрий знає про наявність секретного повідомлення не відкидає RTP-пакет, а приймає його і вилучає секретну інформацію. Якщо одержувач не знає факту наявності секретного повідомлення, то RTP-пакети, які надто затримані, просто відкидаються.

DAB- і DVB стеганографія. Методи DAB- і DVB стеганографії використовуються для обробки інформації у мережах цифрового звукового та телевізійного мовлення.

Зформовано розширений опис складових інженерно-технічних засобів комплексного захисту корпоративної мережі і відображено у таблиці 1.

Таблиця 1 Розширений опис інженерно-технічних засобів комплексного захисту корпоративної мережі

№	Стек мережі	Стек вузлів	Реалізація/Імплементація	Результат
1	**Фізичні заходи**			
1.1	**Контроль доступу**			
	Огорожа	Замкнута серверна кімната	Фізичний бар'єр	Контроль та розмежування доступу
	Боларди			
	Моделі управління доступом	Ідентифікаційні бейджі	Смарт-карта	

№	Стек мережі	Стек вузлів	Реалізація/Імплементація	Результат
	Пункт контролю доступу		Персонал та спеціально обладнана кімната	Контроль доступу до об'єкту
	Сигналізація		Сенсори, датчики та інше спеціалізоване обладнання	Оповіщення про спроби несанкціонованого подолання фізичних бар'єрів
	Біометрія		Сукупність відповідних методів та засобів	Надійна ідентифікація та аутентифікація персоналу
		Кабельний замок	Спеціальний отвір у корпусі пристрою та металевий трос	Фактор стримування для запобігання крадіжки
		Блокувальник даних USB	USB-пристрій	Захист від ризиків зараження пристрою ШПЗ через електромережу
	Захищена система розподілу		Комплекс засобів захисту	Фізичний захист ліній зв'язку, якими передається незашифрована інформація
1.2	**Спостереження**			
	Камери спостереження			Спостереженні за об'єктом створення архівів
	Сенсори і датчики		Спеціальний пристрій	Перетворюють неелектричні сигнали на такі, що зручно обробляти та передавати каналами зв'язку
	Дрони		Безпілотний літальний апарат	Допоміжний захід спостереження
	Охоронне освітлення		Світильники, лампи, прожектори, тощо	
1.3	**Тестування**			
	План аварійного відновлення		Документ	Послідовність кроків мінімізації наслідків подій, яких повинна вжити організація

№	Стек мережі	Стек вузлів	Реалізація/Імплементація	Результат
2	**Апаратні заходи**			
	HSM		Плат плагінів, смарт-карт або самостійних зовнішніх пристроїв, кілька захищених криптопроцесорів	Генерація, захист та управління криптографічними ключами для шифрування, розшифрування та цифрових підписів
	TPM		Захищений криптопроцесор	Генерація, захист та управління криптографічними ключами для аутентифікації
	ГВЧ		Схема, вбудована у слот системної шини PCI / мікросхема	Генерація послідовностей для криптографічних цілей
	FDE		Жорсткий диск із самошифруванням / мікросхема	Захист інформації шляхом шифрування кожного біту даних на жорсткому диску
	PUF		Мікроконтролер ChipDNA	Ідентифікації мікропроцесорів, захист від несанкціонованого доступу
	Проксі-сервер		На основі ARP	Захист внутрішньої структури мережі
3	**Програмні заходи**			
	ME		Спеціальне ПЗ	Фільтрація мережевого трафіку
	ACL		Набір команд	
	NAT			Захист хостів внутрішньої мережі
	AD		Набір служб та база даних	Об'єднання користувачів із необхідними їм мережевими ресурсами
	SSH, Telnet		Клієнт-серверне ПЗ	Віддалене управління доступом
4	**Криптографічні заходи**			
	Симетрична криптографія		Блочні (TDES, Rijndael) та потокові (RC4)шифри	Захист інформації шляхом її шифрування
	Асиметрична криптографія		RSA, ЕЦП	
	Хеш-функції		SHA-1, MD5	Перевірка цілісності, а також ідентифікація інформації

№	Стек мережі	Стек вузлів	Реалізація/Імплементація	Результат
5	**Стеганографічні заходи**			
	WLAN-стеганографія		Система HICCUPS	Приховування інформації у бездротових локальних мережах
	LACK-стеганографія		На основі RTP	Приховування інформації з використанням IP-телефонії
	DAB- і DVB-стеганографія			Приховування інформації у мережах цифрового звукового та телевізійного мовлення

Авторська розробка

6.3. Метод комплексного захисту корпоративної мережі

Наведений розширений опис інженерно-технічних засобів комплексного захисту корпоративної мережі покладено в основу методу комплексного захисту корпоративної мережі (КЗКМ) виокремлення і формування автором двох стеків КЗКМ – стек мережі (Network Stack) стек вузлів (Host Stack), що знайшли своє відображення у запропонованому методі КЗКМ під назвою «Безпекова модель» (табл. 2).

Обидва стеки – Network Stack (NS) та Host Stack – працюють у парадигмі та взаємозв'язку із протокольним стеком TCP/IP і мають такі рівні:

1) Криптографічно-стеганографічний NSL_1 та HSL_1 – покривають прикладний рівень стеку TCP/IP;
2) Програмно-апаратний NSL_2 та HSL_2 покривають частину мережевого та транспортний рівні стеку TCP/IP;
3) Апаратний NSL_3 та HSL_3 покривають частину мережевого та рівень доступу до мережі стеку TCP/IP.

Нехай обидва стеки – *NS* та *HS* – мають по три рівні відповідно «Безпековій моделі».

Таблиця 2 Узагальнена безпекова модель корпоративної мережі

<table>
<tr><th>Модель OSI</th><th>Стек протоколів TCP/IP</th><th>Безпекова модель</th><th>Стек мережі</th><th>Стек хостів</th></tr>
<tr><td rowspan="3">Прикладний</td><td rowspan="6">Прикладний</td><td rowspan="6">Криптографічний / Стеганографічний</td><td>WLAN-стеганографія</td><td></td></tr>
<tr><td>LACK-стеганографія</td><td></td></tr>
<tr><td>DAB- і DVB-стеганографія</td><td></td></tr>
<tr><td rowspan="3">Представлення</td><td colspan="2">Симетрична</td></tr>
<tr><td colspan="2">Асиметрична</td></tr>
<tr><td colspan="2">Хеш-функції</td></tr>
<tr><td>Сеансовий</td><td colspan="2">SSH, Telnet</td></tr>
<tr><td rowspan="2">Транспортний</td><td rowspan="2">Транспортний</td><td rowspan="3">Програмний</td><td>AD</td><td></td></tr>
<tr><td colspan="2">ACL</td></tr>
<tr><td rowspan="2">Мережевий</td><td rowspan="2">Мережевий</td><td>NAT</td><td></td></tr>
<tr><td rowspan="6">Апаратний</td><td colspan="2">ME / HSM</td></tr>
<tr><td>Проксі-сервер</td><td></td></tr>
<tr><td rowspan="4">Канальний</td><td rowspan="6">Доступу до мережі</td><td colspan="2">TPM</td></tr>
<tr><td colspan="2">ГВЧ</td></tr>
<tr><td colspan="2">FDE</td></tr>
<tr><td colspan="2">PUF</td></tr>
<tr><td rowspan="7">Фізичний</td><td rowspan="7">Фізичний</td><td></td><td>Блокувальник даних USB</td></tr>
<tr><td>Огорожа, боларди</td><td>Кабельний замок</td></tr>
<tr><td>Пункт контролю доступу</td><td></td></tr>
<tr><td>Біометрія</td><td></td></tr>
<tr><td>Сигналізація</td><td></td></tr>
<tr><td>Сенсори і датчики</td><td></td></tr>
<tr><td>Камери спостереження</td><td></td></tr>
<tr><td>Захищена система розподілу</td><td></td></tr>
</table>

Авторська розробка

Тоді *NSL* (Network Security Level) міститиме:

- NSL_1,
- NSL_2,

– NSL_3

А *HSL* (Host Security Level) міститиме:

– HSL_1,

– HSL_2,

– HSL_3.

І на кожному з них є кілька опцій мережевого захисту *Def*.

Подамо аналітичний опис моделі комплексного захисту корпоративної мережі.

6.4. Модель комплексного захисту корпоративної мережі

Нехай на рівні NSL_1 є деяка кількість *A* засобів захисту корпоративної мережі (ЗЗКМ) і становить деяку множину $A = \{a_1, a_2, \dots, a_a,\}$; на рівні NSL_2 є деяка кількість *B* ЗЗКМ і становить деяку множину $B = \{b_1, b_2, \dots, b_b,\}$; на рівні NSL_3 є деяка кількість *C* ЗЗКМ і становить деяку множину $C = \{c_1, c_2, \dots, c_c,\}$ (табл. 3).

Кількість ЗЗКМ на рівнях стеків визначається потужність відповідних множин і може варіюватися згідно потреб підприємства.

І нехай на рівні HSL_1 є деяка кількість *F* засобів захисту корпоративної мережі (ЗЗКМ) і становить деяку множину $F = \{f_1, f, \dots, f_f,\}$; на рівні HSL_2 є деяка кількість *G* ЗЗКМ і становить деяку множину $G = \{g_1, g_2, \dots, g_g,\}$; на рівні HSL_3 є деяка кількість ЗЗКМ і становить деяку множину $H = \{h_1, h_2, \dots, h_h,\}$.

Кожен ЗЗКМ у обох стеках має свою вагу *W*, вага ЗЗКМ визначається засобами експертних оцінок аудиторів і регулюється потребами та специфікою роботи підприємства в мережі.

Оцінимо ступінь захисту *SL* (Security Level) на кожному з рівнів по обидвом стекам сумою ваг усіх ЗЗКМ на відповідному рівні. Тоді для стеку *NS* ступінь захисту SL_{NS} буде сумою сум ваг по кожному рівню і для стеку хостів *HS* ступінь захисту SL_{HS} буде теж сумою сум ваг (1).

Таблиця 3 Візуальне відображення Безпекової моделі

	Стек мережі *NS*	Стек хостів *HS*	
NSL_1	a_1 a_2 … a_a $\sum_1^a W_{A_a}$	f_1 f_2 … f_f $\sum_1^f W_{F_f}$	HSL_1
NSL_2	b_1 b_2 … b_b $\sum_1^b W_{B_b}$	g_1 g_2 … g_g $\sum_1^g W_{G_g}$	HSL_2
NSL_3	c_1 c_2 … c_c $\sum_1^c W_{C_c}$	h_1 h_2 … h_h $\sum_1^h W_{H_h}$	HSL_3
	$\sum_1^3 NSL_i$	$\sum_1^3 HSL_k$	

Авторська розробка

$$SL_{NS} = \sum_1^3 NSL_i \text{ і } SL_{HS} = \sum_1^3 HSL_k \quad (1)$$

Ступінь захисту SL_1 на криптографічно-стеганографічному рівні (2):

$$NSL_1 = \sum_1^a W_{A_a} \text{ і } HSL_1 = \sum_1^f W_{F_f} \quad (2)$$

Ступінь захисту SL_2 на програмно-апаратному рівні (3):

$$NSL_2 = \sum_1^b W_{B_b} \text{ і } NSL_2 = \sum_1^g W_{G_g} \quad (3)$$

Ступінь захисту SL_3 на апаратному рівні (4):

$$NSL_3 = \sum_{1}^{c} W_{C_c} \text{ і } NSL_3 = \sum_{1}^{h} W_{H_h} \quad (4)$$

Умовою проходження **мінімального рівня аудиту** AUD_{min} на кожному окремому рівні запропонованої Безпекової моделі є наявність принаймні одного впровадженого ЗЗКМ на цьому рівні (незалежно від того, чи це стек мережі, чи хостів). Умови проходження мінімального аудиту $AUD1_{min}$ на криптографічно-стеганографічному рівні (5):

$$AUD1_{min} = \begin{cases} 1, \text{якщо } \left(\sum_{1}^{a} W_{A_a} + \sum_{1}^{f} W_{F_f} \right) > 0 \\ 0, \text{якщо } \left(\sum_{1}^{a} W_{A_a} + \sum_{1}^{f} W_{F_f} \right) = 0 \end{cases} \quad (5)$$

Умови проходження мінімального аудиту $AUD2_{min}$ на програмно-апаратному рівні (6):

$$AUD2_{min} = \begin{cases} 1, \text{якщо } \left(\sum_{1}^{b} W_{B_b} + \sum_{1}^{g} W_{G_g} \right) > 0 \\ 0, \text{якщо } \left(\sum_{1}^{b} W_{B_b} + \sum_{1}^{g} W_{G_g} \right) = 0 \end{cases} \quad (6)$$

Умови проходження мінімального аудиту $AUD3_{min}$ на апаратному рівні (7):

$$AUD3_{min} = \begin{cases} 1, \text{якщо } \left(\sum_{1}^{c} W_{C_c} + \sum_{1}^{h} W_{H_h} \right) > 0 \\ 0, \text{якщо } \left(\sum_{1}^{c} W_{C_c} + \sum_{1}^{h} W_{H_h} \right) = 0 \end{cases} \quad (7)$$

Умовою проходження **оптимального рівня аудиту** AUD_{min} на кожному окремому рівні запропонованої Безпекової моделі є наявність одночасно по однму впровадженого ЗЗКМ на цьому рівні – один у стеці мережі і один у стеці хостів. Умови проходження оптимального аудиту $AUD1_{opt}$ на криптографічно-

стеганографічному рівні (8) за наявності мінімального аудиту:

$$AUD1_{opt} = \begin{cases} 1, \text{якщо } \sum_{1}^{a} W_{A_a} > 0 \text{ і } \sum_{1}^{f} W_{F_f} > 0 \\ 0, \text{якщо } \begin{cases} \sum_{1}^{a} W_{A_a} > 0 \text{ і } \sum_{1}^{f} W_{F_f} = 0 \\ \sum_{1}^{a} W_{A_a} = 0 \text{ і } \sum_{1}^{f} W_{F_f} > 0 \end{cases} \end{cases} \quad (8)$$

Умови проходження оптимального аудиту $AUD2_{opt}$ на програмно-апаратному рівні (9) за наявності мінімального аудиту:

$$AUD2_{opt} = \begin{cases} 1, \text{якщо } \sum_{1}^{b} W_{B_b} > 0 \text{ і } \sum_{1}^{g} W_{G_g} > 0 \\ 0, \text{якщо } \begin{cases} \sum_{1}^{b} W_{B_b} > 0 \text{ і } \sum_{1}^{g} W_{G_g} = 0 \\ \sum_{1}^{b} W_{B_b} = 0 \text{ і } \sum_{1}^{g} W_{G_g} > 0 \end{cases} \end{cases} \quad (2.9)$$

Умови проходження оптимального аудиту $AUD3_{opt}$ на апаратному рівні (10) за наявності мінімального аудиту:

$$AUD3_{opt} = \begin{cases} 1, \text{якщо } \sum_{1}^{c} W_{C_c} > 0 \text{ і } \sum_{1}^{h} W_{H_h} > 0 \\ 0, \text{якщо } \begin{cases} \sum_{1}^{c} W_{C_c} > 0 \text{ і } \sum_{1}^{h} W_{H_h} = 0 \\ \sum_{1}^{c} W_{C_c} = 0 \text{ і } \sum_{1}^{h} W_{H_h} > 0 \end{cases} \end{cases} \quad (10)$$

Висновки

У даному науковому дослідженні виконано аналіз та впровадження методу комплексного захисту корпоративної мережі, що враховує інженерно-технічний, криптографічний, стеганографічний, організаційний та правовий аспекти, а також забезпечує гнучке оцінювання рівня безпеки на різних рівнях мережевої та вузлової інфраструктури. Зокрема:

1) Обґрунтовано важливість комплексного підходу. Поєднання правових, організаційно-адміністративних та інженерно-технічних заходів є критично важливим для забезпечення надійного захисту мережі.
2) Запропоновано розширений опис інженерно-технічних засобів. Розглянуто та систематизовано фізичні, апаратні, програмні, криптографічні й стеганографічні заходи, що дають змогу протидіяти широкому спектру загроз.
3) Розроблено метод комплексного захисту корпоративної мережі. Суть є у виокремленні двох стеків (мережевого та вузлового) з відповідними рівнями, які віддзеркалюють технології забезпечення безпеки.
4) Сформовано формальну модель для оцінювання захищеності. Запропоновано розрахункові співвідношення, які дають можливість визначати ступінь захисту на кожному рівні обох стеків, а також порівнювати отримані результати з мінімальними та оптимальними критеріями аудиту.

Таким чином, використання методів і моделей, описаних у розділі колективної монографії, дає змогу забезпечити системну та гнучку реалізацію захисту корпоративної мережі відповідно до сучасних вимог інформаційної безпеки.