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

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ СЕРВЕРІВ БАЗ ДАНИХ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»
спеціальність 125 «Кібербезпека»
Торколат Володимир Андрійович

Керівник: д.ф.-м.н., професор
Василенко Микола Дмитрович

Рецензент: к.ф.-м.н., доцент
Чепурна Олена Євгенівна

Одеса – 2024

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

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

З А В Д А Н Н Я
на кваліфікаційну (бакалаварську) роботу
здобувачу Торколат Володимиру Андрійовичу

1. Тема роботи: «**Організація захисту інформації серверів баз даних**»
Керівник роботи: д.ф.-м.н., професор Василенко Микола Дмитрович

затверджені наказом НУ ОЮА від *«_____»_____№ _____*
2. Строк подання здобувачем роботи *«20» травня 2024 року*
3. Дата видачі завдання *«15» вересня 2024 року*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Підготовчий	20.09 – 20.10.2023	
2	Вибірка теоретичних відомостей	22.10 – 20.11.2023	
3	Написання теоретичної частини	21.11 – 13.12.2023	
4	Збір відомостей про об’єкт дослідження	14.12.2023 – 22.03.2024	
5	Написання практичної частини	22.03 – 15.05.2024	

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Організація захисту серверів баз даних» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальності 125 «Кібербезпека».

Містить 4 малюнки, 15 таблиць, 10 літературних джерел за переліком посилань, 2 додаткових джерела. Робота виконана на 37 сторінках загального тексту і 32 сторінках основного тексту.

Метою даної роботи є оцінка та аналіз серверу баз даних та збереження файлів Господарського суду Одеської області, виявлення недоліків та розробка рекомендації для захисту сервера

У роботі розглянуто теоретичні відомості про інформацію т принципи інформаційної безпеки, види серверів, типи їх розміщення та призначення. Також розглянуто теоретичні відомості про види вразливостей серверів, види вторгнень та системи виявлення та запобігання вторгнень.

У роботі буде досліджено основні недоліки захисту та вразливості серверів баз даних. Дослідження основних вразливостей серверів баз даних зроблено на основі сервера баз даних Господарського суду Одеської області який був взламан восени 2023р.

ЗАХИСТ, СЕРВЕР, БАЗА ДАНИХ.

ABSTRACT

Qualification work on the topic "Organization of the protection of database servers" for obtaining the first (bachelor's) level of higher education in the specialty 125 "Cybersecurity".

Contains 4 figures, 15 tables, 10 references according to the list of references, 2 additional sources. The work was completed on 37 pages of the general text and 32 pages of the main text.

The purpose of this work is to evaluate and analyze the database server and save files of the Commercial Court of Odesa region, identify shortcomings and develop a recommendation for server protection

Theoretical information about information and principles of information security, types of servers, types of their placement and purpose are considered in the work. Theoretical information about types of server vulnerabilities, types of intrusions, and intrusion detection and prevention systems is also considered.

The work will investigate the main security flaws and vulnerabilities of database servers. The study of the main vulnerabilities of database servers was made on the basis of the database server of the Commercial Court of Odesa region, which was hacked in the fall of 2023y.

PROTECTION, SERVER, DATABASE

ЗМІСТ

ВСТУП

Актуальність теми. Дослідження захисту серверів баз даних залишається актуальним досі, зловмисники постійно шукають нові способи взламати сервера кампаній або державних підприємств, бо інформація та данні один з найцінніших ресурсів сучасності. Регулярні аудити захисту та дослідження причин уразнення серверів зловмисниками допомагають розробляти нові методи та системи захисту, й вдосконалювати існуючи.

Аналіз того як саме на сервери потрапляє шкідливе програмне забезпечення, до яких втрат воно призводить, які системи захисту були уникнуті та які системи захисту були наявні, займає ключову позицію у пошуку рішення проблеми.

Якщо відомо як шкідливе програмне забезпечення потрапило на сервер, які системи захисту зловмисник обійшов щоб його програма потрапила на сервер, разом із якими файлами був доставлен вірус, та які методи були використані для обходу захисту, чи відсутність яких мір захисту призвела до цього, допомагає зрозуміти з чим саме треба боротися та які методи захисту треба вдосконалювати.

Метою дослідження є аналіз захисту сервера який був уражений, вияснення які методи використав зловмисник для отримання доступу, та чого ураження серверу та всій мережі вірусним програмним забезпеченням було помічено лише через два тижня після того як вірус потрапив на сервер.

Завдання дослідження:

– зробити аналіз мір захисту сервера який було уражено

– оцінити рівень захисту сервера

– вияснити які саме міри захисту зловмисник обійшов

– скласти рекомендації до покращення захисту

Об’єкт дослідження – сервер Господарського суду Одеської області. Система включала до себе збереження бази даних для програми ДСС(Діловодство спеціалізованого суду), з’єднання однією мережею комп’ютера усіх працівників суду, збереження файлів рішень суду, ухвал, та збереження конфіденційних даних

учасників судових засідань, таких як:код ЄДРПОУ; РНКОПП(ІПН) учасників судового засідання та працівників; назви компаній та ПІБ учасників судового засідання; місця проживання та/або розташування учасників судового засідання та працівників; повні паспортні дані працівників суду (РНКОПП(ІПН), дата народження, місце проживання прописку та фактичне, номери телефонів).

Предмет дослідження є діючі законодавчі та міжнародні норми(методи CIA та ISO 27001), згідно до яких буде проведено аналіз та оцінено рівень захисту.

Методи дослідження: Аудит системи захисту відповідності нормам, перевірка програмного та технічного забезпечення.

Наукова новизна одержаних результатів: Визначення які методи обходу мір безпеки були використані зловмисником, складання рекомендації що то до усунення вразливості.

Визначення наскільки критичним у сфері захисту серверів баз даних є людський фактор та організація належного захисту.

Практичне значення отриманих результатів. Усвідомлення критичності людського фактору та поганої реалізації захисту серверів баз даних. Дослідження того, які методи безпеки зараз потребують вдосконалення, які нові методи використовуються зловмисниками, та які методи прикриття вірусного програмного забезпечення починають використовувати зловмисники.

1 ПОНЯТТЯ ІНФОРМАЦІЇ, СПОСОБИ РОЗМІЩЕННЯ ТА ВИДИ СЕРВЕРІВ(ОРГАНІЗАЦІЙНО-ПРОГРАМНА СТРУКТУРА) І ЇЇ ЗАХИСТ

1.1 Поняття про інформацію, що таке сервер та інформаційна безпека

Інформація - це сукупність знань про щось, якою одна людина ділиться з іншою. Вона може мати різну форму: текст, зображення, аудіо, відео та дані. Інформація може бути отримана з різних джерел, таких як книги, статті, веб-сайти, люди та досвід. Люди використовують інформацію для прийняття рішень, вирішення проблем, навчання та розваг. Інформація - це цінний ресурс, який може покращити наше життя багатьма способами.

Інформація - це не просто набір даних чи фактів. Це потужний ресурс, який може значно впливати на наше життя. Її цінність полягає в здатності:

Розширювати знання, завдяки інформації ми дізнаємося про світ, його закони, історію та культуру. Це допомагає нам краще розуміти себе та своє місце в ньому.

Приймати кращі рішення володіючи необхідною інформацією, ми можемо робити більш обґрунтовані та виважені вибори в різних сферах життя.

Вирішувати проблеми, тому що нформація дає нам ключ до вирішення проблем, з якими ми стикаємося щодня. Вона допомагає нам знаходити нові підходи та методи для досягнення цілей.

Розвиватися – інформація є рушієм прогресу. Завдяки їй ми можемо вчитися новому, розвивати свої навички та здібності, а також удосконалювати себе.

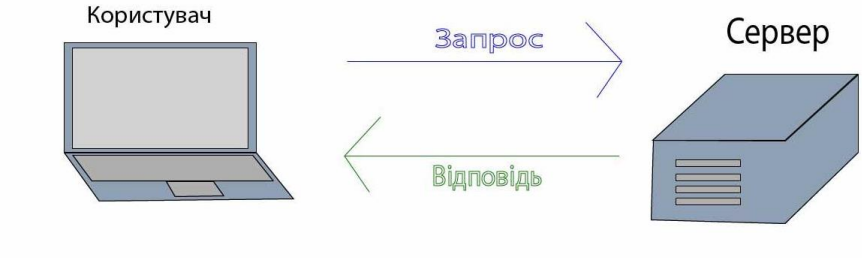
Цінність інформації складно переоцінити, вона є основою для розвитку особистості, суспільства та цивілізації в цілому.

Важливо пам'ятати, що не вся інформація є корисною й достовірною. Тому необхідно вміти критично її оцінювати, перевіряти джерела та використовувати лише надійні дані.

Сервери у свою чергу – це сукупність програмного та апаратного забезпечення для збереження великої кількості даних, найпоширеніші види серверів це файлові та

сервери баз даних. Обидва ці сервери призначені для збереження великих обсягів даних та забезпечення їх доступності, але конфіденційність даних та їх цілісність вони самі по собі не забезпечать, тому і потрібні фахівці кібербезпеки та фахівець з адміністрування комп'ютерних систем. Забезпечення захисту цілісності та конфіденційності даних від зовнішніх загроз це справа фахівців кібербезпеки, а забезпечення конфіденційності, цілісності та доступності від внутрішніх факторів та ненавмисних кіберінцидентів.

Сервери виступають хранилищами інформації та даних, роблячи їх доступними для клієнтів. Ця інформація може включати веб-сайти, електронні листи, файли та інші дані. Коли клієнт надсилає запит на сервер, сервер отримує його, знаходить запитувану інформацію та обробляє її, потім сервер надсилає відповідь клієнту, який може її використовувати (Малюнок 1). Сервери використовуються для надання різних послуг, таких як веб-хостинг, електронна пошта, хмарне зберігання та багато інших.



Малюнок 1.1 – Схематична робота веб-сервера/сервера

Сервер не володіє самостійною здатністю визначати, кому й яку інформацію надсилати. Саме тому необхідні системні адміністратори та фахівці з кібербезпеки. Їхня задача полягає в розробці правил доступу, які регулюють надання сервером користувачам доступу до даних. Ці правила можуть ґрунтуватися на таких факторах, як роль користувача в організації, його рівень доступу та тип даних, до яких він потребує доступу. Наявність чітких правил доступу допомагає захистити конфіденційні дані та запобігти несанкціонованому доступу до них.

Інформаційна безпека - це система заходів, що вживаються для захисту інформації від несанкціонованих дій, таких як несанкціонований доступ, використання, розкриття, зміна або знищення. До інформації, яка потребує захисту, належать конфіденційні дані, фінансова інформація, інтелектуальна власність та інші дані. Загрозами інформаційній безпеці можуть бути кібератаки, крадіжки даних, шпигунство та інші шкідливі дії. Забезпечення інформаційної безпеки є важливим для захисту даних від несанкціонованого доступу, а також для збереження конфіденційності, цілісності та доступності інформації.

Таблиця 1.1 – Принципи інформаційної безпеки

Принцип	Опис
Конфіденційність	інформація доступна лише авторизованим особам
Цілісність	інформація не може бути змінена несанкціоновано
Доступність	інформація доступна авторизованим особам, коли це необхідно

1.2 Способи розміщення та види серверів

Розберемося у тому які є види серверів, які є переваги та недоліки у різних типах розміщення сервера.

Три основних типу розміщення серверів це: Локальне розміщення; Хостинг на місці; Хмарний хостинг.

Локальне розміщення - це коли сервер знаходиться в безпосередній близькості до користувача або організації, що ним володіє. Це може бути офіс, дата-центр або навіть домашня мережа. окальне розміщення серверів часто використовується компаніями, яким потрібна висока продуктивність та безпека, а також тими, хто має чутливі дані, які не хочуть розміщувати в хмарі.

Хостинг в дата-центрі - це коли сервер розміщується в спеціально обладнаному приміщенні, що належить та обслуговується сторонньою компанією. Користувач або

організація орендує місце в цьому дата-центрі та отримує доступ до сервера через Інтернет. Хостинг в дата-центрі часто використовується компаніями, яким потрібна доступна та надійна платформа для розміщення своїх веб-сайтів та програм.

Хмарний хостинг - це коли сервер розміщується в "хмарі", тобто в віртуальному середовищі, яке надається сторонньою компанією. Користувач або організація має доступ до сервера через Інтернет і не несе відповідальності за фізичне обладнання або програмне забезпечення. Хмарний хостинг часто використовується компаніями, яким потрібна доступна та гнучка платформа для розміщення своїх веб-сайтів та програм.

Таблиця 1.2 – Переваги та недоліки різних типів розміщення

Тип розміщення	Переваги	Недоліки
Локальне	Повний контроль над сервером. Високий рівень безпеки. Низькі витрати на експлуатацію.	Високі початкові витрати. Потребує технічного обслуговування та підтримки. Обмежена масштабованість.
Хмарний в дата-центрі	Зниження початкових витрат. Зменшення навантаження на технічне обслуговування та підтримку. Можливість масштабування.	Менший контроль над сервером. Можливі проблеми з безпекою. Вищі витрати на експлуатацію, ніж у хмарному хостингу.
Хмарний хостинг	Низькі початкові витрати. Масштабованість за потребою. Відсутність необхідності в технічному обслуговуванні та підтримці.	Менший контроль над сервером. Можливі проблеми з безпекою. Залежність від стороннього постачальника послуг.

Вивчивши типи розміщення серверів, ми маємо уявлення про те, де вони можуть знаходитися. Тепер перейдемо до самих серверів, розглянемо їх види та особливості організації (організаційно-програмну структуру).

Таблиця 1.3 – Призначення серверу за видом(основні види)

Вид сервера	Призначення

Веб-сервер	хостинг веб-сайтів та веб-додатків
Файловий сервер	зберігання та спільний доступ до файлів
Поштовий	надсилання та отримання електронної пошти
Сервер Бази даних	зберігання та управління даними
Проксі-сервер	забезпечення анонімного доступу до Інтернету та кешування контенту
Ігровий сервер	хостинг онлайн-ігор
Сервер VoIP	хостинг телефонних дзвінків через Інтернет

Кожний вид серверу(Таблиця 1.3) може працювати окремо від інших але вони також можуть поєднуватися між собою (щоб сервер мав оптимальну працездатність), через те що у сучасному світі реалізовувати кожний тип серверу окремим комплексом апаратно-програмного забезпеченням буде ускладнювати роботу з захистом та обслуговуванням.

Розглянемо сервери баз даних, поштові, веб-сервери, файлові та проксі-сервери трішки детальніше, так як вони частіше використовуються:

1. Поштовий сервер – це програмне забезпечення, що відповідає за прийом, зберігання, обробку та надсилання електронних листів. Він є важливою частиною інфраструктури електронної пошти, що забезпечує зв'язок між користувачами. На ньому обов’язково є поштові агенти передачі (MTA), Поштові агенти користувацького інтерфейсу (MUA), Системи керування контентом (CMS) та Фільтри спаму.
2. Веб-сервер – це програмне забезпечення, яке зберігає веб-сайти та надає їх користувачам через Інтернет. Воно є важливою частиною інфраструктури Інтернету, що робить можливим доступ до мільярдів веб-сайтів у всьому світі. Основні його елементи, це HTTP-сервери такі як Apache чи Nginx, модулі веб-сервера(mod_rewrite, mod_security, mod_expires), системи керування контентом (CMS), інструменти моніторингу та інструменти резервного копіювання.

3. Файловий сервер – це програмне забезпечення, яке використовується для зберігання, керування та надання спільного доступу до файлів та папок на мережевому комп'ютері. Воно є важливою частиною інфраструктури мережі, що дозволяє користувачам ділитися файлами та співпрацювати над проектами. Складається з операційної системи, протоколів спільного доступу до файлів, системи керування доступом, програмне забезпечення резервного копіювання та антивірусного програмного забезпечення. Також на них часто додатково розгортають бази даних, для зменшення кількості об’єктів захисту до одного сервера замість двох, та зменшення затрат на розгортання серверів.
4. Сервер бази даних – це програмне забезпечення, яке використовується для зберігання, керування та надання доступу до даних. Воно є важливою частиною інфраструктури програмного забезпечення, що дозволяє веб-сайтам, мобільним додаткам та іншим програмам зберігати та отримувати доступ до даних, необхідних для їх роботи. Розгортається на сервері з операційною системою, але крім операційної системи на якій все розгортається також необхідними є системи керування базами даних (СКБД) та інструменти для того щоб зробити керування зручнішим, інструменти резервного копіювання та відновлення, інструменти моніторингу та безпеки.
5. Проксі-сервер - це програмне забезпечення, яке посередничає між комп'ютером та глобальною мережею(Інтернетом). Він приховує IP-адресу користувача та може використовуватися для покращення конфіденційності, безпеки та обходу обмежень. Основними елементами є програмне забезпечення проксі-сервера(HAProxy, Nginx, Squid, Privoxy).

При поєднанні різних типів серверів між собою збільшується їх функціонал, та зменшується необхідна площа для його встановлення, зменшуються затрати на обслуговування та кількість об’єктів які потребують індивідуального налаштування

та підходу до захисту, але збільшуються початкові затрати, так як необхідно встановлювати якісне апаратне забезпечення.

Один з прикладів змішаного сервера є сервер з яким я працюю, цей сервер реалізований як сервер бази-даних та файловий, що зменшує кількість проблем з обслуговуванням.

Не всі види серверів можуть поєднуватися з іншими типами, одним з таких є сервер VoIP, він не може поєднуватися з іншими типами серверів по причині того що у вимогах до його встановлення, він має бути підключений окремою лінією.

Програмна структура сервера – це програмне забезпечення, яке використовується для роботи сервера. Вона включає в себе операційну систем у, веб-сервер, програмне забезпечення бази даних та інші програми, необхідні для роботи сервера.

Таблиця 1.4 – Популярні конфігурацій серверів

Назва	Операційна система	Веб-сервер	База даних	Мова програмування
LAMP	Linux	Apache	MySQL	PHP
LEMP	Linux	Nginx	MySQL	PHP
WAMP	Windows	Apache	MySQL	PHP
Windows server з IIS	Windows Server	IIS	Microsoft SQL Server	.NET

LAMP – це популярна конфігурація програмного забезпечення сервера.

LEMP – це ще одна популярна конфігурація програмного забезпечення сервера, яка схожа на LAMP, але використовує Nginx замість Apache.

WAMP – це конфігурація програмного забезпечення сервера для Windows.

Windows Server з IIS – це популярна конфігурація програмного забезпечення сервера для Windows.

1.3 Системи та методи захисту серверів

Захист серверів є критично важливим завданням для будь-якої організації, яка володіє інформацією або даними які є критичними чи життєво важливими. Сервери зберігають цінні дані, які можуть бути використані зловмисниками для нанесення шкоди вашому бізнесу. Тому важливо вжити заходів для захисту серверів від кібератак.

Існує багато різних систем та методів захисту серверів, які можна використовувати. Найкращий підхід для вас залежатиме від ваших конкретних потреб та ризиків. Деякі з найпоширеніших систем та методів захисту включають в себе фізичний та мережевий захист, захист програмного забезпечення яке використовується у компанії, захист даних компанії, навчання та обізнаність персоналу у кібергігієні(що ці методи включають у себе дивиться таблицю 5). Важливо зазначити, що це лише деякі з багатьох систем та методів захисту серверів, які можна використовувати.

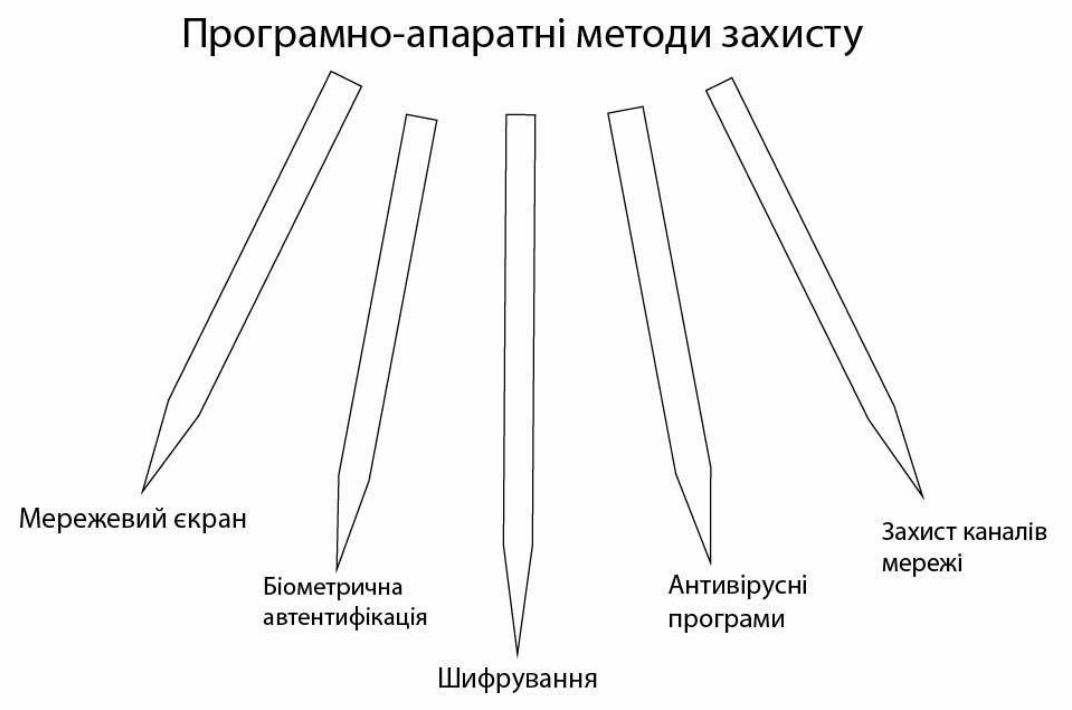
Таблиця 1.5 – Основні методи захисту

Метод захисту	Опис
Фізичний	Захист серверів від несанкціонованого доступу за допомогою фізичних засобів, таких як замки, камери та охорона.
Мережевий	Використання брандмауерів, систем виявлення вторгнення (IDS) та систем запобігання вторгненням (IPS) для захисту серверів від кібератак.
Програмного забезпечення	Установка та оновлення антивірусного та антишпигунського програмного забезпечення, а також використання брандмауерів та контролю доступу для захисту серверів від шкідливого програмного забезпечення.
Даних	Резервне копіювання даних, шифрування даних та контроль доступу до даних.
Навчання та обізнаність	Навчання співробітників основам кібербезпеки та тому, як розпізнавати та уникати фішингових атак та інших соціальних інженерних атак.

Найкращий підхід залежатиме від конкретних потреб та ризиків. Як фахівці з кібербезпеки, ми повинні визначити, які системи та методи захисту найкраще підходять для нашої організації, також треба проконсультуватися з головою організації для визначення необхідного рівня захисту(наскільки втрата даних буде критичною).

Захист серверів – це неперервний процес, який потребує постійної адаптації до нових загроз та вразливостей, це комплексне завдання, яке потребує поєднання технологічних та організаційних заходів.. Оновлення систем та методів захисту – це невід'ємний елемент кібербезпеки серверів, який допомагає їм протистояти кібератакам.

До систем захисту серверів відносять брендмауєри(міжмережеві єкрани), системи виявлення вторгнень, системи запобігання вторгнень, антивірусне та антишпигунське програмне забезпечення, системи захисту даних(шифрування, контроль доступу, резервні копії), фізичний захист (захист від несанкціонованого доступу фізичних осіб).



Малюнок 1.2 – Програмно-апаратні методи захисту

Біометричні технології автентифікації – це системи які підверджують особу корисувача завдяки його біометричних даних, таких як відбитки пальців, сітчатка ока, розпізнавання обличя, розпізнавання голосу та геометрія руки.

Системи виявлення вторгнень або IDS – це системи, які моніторять мережевий трафік і шукають підозрілу активність. Вони можуть попередити вас про можливі атаки, щоб ви могли вжити заходів. Також використовують системи запобігання вторгнення (IPS), вони схожі на системи IDS, але на відмінну від них можуть вживати заходи для блокування, а не лише попереджати.

Брандмауери(FireWall) – це бар'єри, які контролюють трафік, що надходить і виходить із сервера. Вони можуть бути програмними або апаратними і можуть бути налаштовані для блокування трафіку з певних IP-адрес, портів або типів трафіку.

Системи запобігання вторгненням (IPS) – це тип програмного або апаратного забезпечення для кібербезпеки, яке виявляє та запобігає несанкціонованому доступу до комп’ютерних систем і мереж. Вони працюють шляхом аналізу мережевого трафіку та активності на комп’ютері на предмет підозрілих дій. Якщо IPS виявляє потенційну загрозу, він може вжити заходів для її блокування, наприклад, закрити з’єднання або заблокувати IP-адресу.

Система захисту даних через шифрування – це процес перетворення інформації на секретний код, роблячи її незрозумілою для сторонніх осіб, які не мають спеціального ключа. Це як секретна мова, яку можуть зрозуміти лише ті, хто володіє "шифром". Шифрування є важливим інструментом для захисту конфіденційності даних, особливо в таких випадках:

2 ВИДИ ВРАЗЛИВОСТЕЙ СЕРВЕРІВ, ВИДИ ВТОРГНЕНЬ, ІНСТРУМЕНТИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ

2.1 Основні види вразливостей серверів

Сервери, як і будь-які інші комп'ютерні системи, схильні до різних видів вразливостей, які можуть бути використані зловмисниками для отримання несанкціонованого доступу, крадіжки даних або заподіяння шкоди. Є декілька основних вразливостей: вразливості програмного забезпечення; вразливості мережі; вразливості апаратного забезпечення; вразливості користувачів(для подробного усвідомлення, таблиця 2.1).

Таблиця 2.1 – Види вразливості

Вид вразливості	Опис	Приклад
Вразливості програмного забезпечення	Помилки в програмному забезпеченні, які можуть бути використані зловмисниками.	Програмні помилки, незахищені конфігурації, застаріле програмне забезпечення.
Вразливості мережі	Атаки, які спрямовані на те, щоб отримати доступ до сервера або перешкодити його роботі.	Атаки типу "людина в середині", атаки типу "відмова в обслуговуванні" (DoS), сканування портів.
Вразливості апаратного забезпечення	Вразливості, пов'язані з фізичним доступом до сервера або його апаратними компонентами.	Фізичний доступ, апаратні збої.
Вразливості користувачів	Слабкі паролі, фішинг, соціальна інженерія.	Використання слабких паролів, розкриття особистої інформації зловмисникам.

Звісно всі види вразливостей які існують важко буде описати, так як при гарно розробленому захисті від кібератак залишаються лише кіберінциденти ненавмисного характеру(природні явища, збої електро мережі, черезвичаїні ситуації, помилка користувача), але захист серверу від внутрішніх та ненавмисних загроз.

Також коротко розглянемо вразливість майже всіх серверів – це SQL-ін’єкції. Вони є найшкідливішими. Причина цього полягає в тому, що SQL-ін’єкції можуть бути введені через пакет даних які отримує сервер, SQL-ін’єкції не потребують авторизації, так як потрапляють безпосередньо з вхідними даними, витягують необхідні дані, або змінює їх, в залежності від того як це запланував зловмисник.

Таблиця 2.2 – Принцип роботи SQL-ін’єкції

Етап	Опис
Створення запиту	Створюємо SQL-ін’єкцією та вшиваємо її до запиту який надсилається до сервера
Надсилання запиту	Надсилаємо запит з SQL-ін’єкцією на сервер, так як веб-застосунки не перевіряють дані що надсилаються до сервера
Виконання запиту	Веб-застосунок виконує запит, а SQL-ін’єкція свою роботу
Результат	SQL-ін’єкція виконує те на що була запрограмована

Також велику частку усіх можливих уразнень сервера складає низький рівень обізнаності у сфері кібергігієни серед рядових працівників різних компаній. Мало хто з роботодавців хвилюється за рівень обізнаності у працівників в кібергігієні та навичках роботи з комп’ютерами, коли у штаті є системний адміністратор чи фахівець з кібербезпеки, це призводить до того що у більшості випадків системний адміністратор та фахівець з кібербезпеки вирішують проблеми що трапляються на комп’ютерах працівників, через що не можуть приділяти достатньо уваги для моніторингу мережі, та перевірки звітів від систем захисту.

2.2 Види вторгнень

Вторгнення в комп'ютерні системи – це несанкціонований доступ, використання або модифікація даних, систем або ресурсів. Зловмисники можуть здійснювати вторгнення з різних причин, наприклад, для крадіжки конфіденційних даних, порушення роботи системи або встановлення програм-вимагачів. Існує декілька основних типів вторгнень, які варто розрізняти: (Таблиця 2.3).

Таблиця 2.3 – Описи видів вторгнення

Вид вторгнення	Методи	Опис методу
Вторгнення на рівні мережі	Сканування мережі	Використання спеціальних програм для пошуку вразливих місць у мережі
	Атаки типу DoS(DDoS)	Перевантаження трафіку великою кількістю запитів, щоб призвести до вимкнення
	Сніфінг(Sniffing)	Перехоплення пакетів даних у мережі за допомогою спеціалізованих програм
	Людина посередені(MitM)	Перехоплення пакетів даних між двома
Вторгнення на рівні операційної системи(ОС)	Вразливості ОС	Використання відомих вразливосте у ОС
	Bruteforce(Груба сила)	Підбір пароля та логіну шляхом їх перебору
	Соціальна інженерія	Маніпулювання користувачами
	Фішинг	Відправках листів чи повідомлень під виглядом представника компанії для отримання логіну та пароля
Вторгнення на рівні додатків	Вторгнення до веб-додатку	SQL-ін'єкція
	Вторгнення з використанням шкідливого програмного забезпечення	Вторгнення завдяки необачному встановленню на сервер чи пристрій користувача програми зі шкідливим кодом

Вторгнення на рівні мережі – це тип кібератаки, при якій зловмисник отримує несанкціонований доступ до комп'ютерної мережі. Це може призвести до серйозних наслідків, таких як крадіжка даних або порушення роботи системи. Важливо пам’ятати що за відсутності належного захисту від вторгнення на рівні мережі може призвести до того, що зловмисник може відключити один чи декілька мережевих комутаторів, щоб поки адміністратор відійшов розбиратися чого на у працівників зник інтернет, зловмисник міг спокійно витягнути дані з сервера знаючи що адміністратор мережі не побачить ознак вторгнення на сервер.

Вторгнення на рівні операційної системи (ОС) – це тип кібератаки, при якій зловмисник отримує несанкціонований доступ до ОС сервера чи персонального комп'ютера. Це може призвести до серйозних наслідків, таких як крадіжка даних, порушення роботи системи або встановлення шкідливого програмного забезпечення. Частіше вторгнення на рівні ОС трапляються коли користувач необачно завантажує програму в яку вшито вірус, чи необачно переходить по посиланню яке замасковано під офіційне чи достовірне джерело, завдяки чому зловмисник отримує доступ до комп'ютера працівника, якщо у мережі не реалізовано жодної системи контролю доступу, вірусне програмне забезпечення може бути встановленим через метод тихого встановлення, без відома користувача, та розповсюдитись по всій мережі.

Вторгнення на рівні додатків - це тип кібератаки, при якій зловмисник отримує несанкціонований доступ до веб-сайту або іншого програмного забезпечення, яке працює на сервері. Це може призвести до серйозних наслідків, таких як крадіжка даних, порушення роботи системи або поширення шкідливого програмного забезпечення. Якщо на сервері не реалізовано перевірку вхідних пакетів, до бази даних сервера, чи до його програмного забезпечення може потрапити пакет даних зі шкідливим кодом, що призведе до втрати конфіденційності, цілісності чи доступності даних на сервері.

Також треба розрізняти види кібератак, які призводять до вторгненя зловмисника у мережу, розглянемо ті які нам потім будуть необхідні в нашому дослідженні.

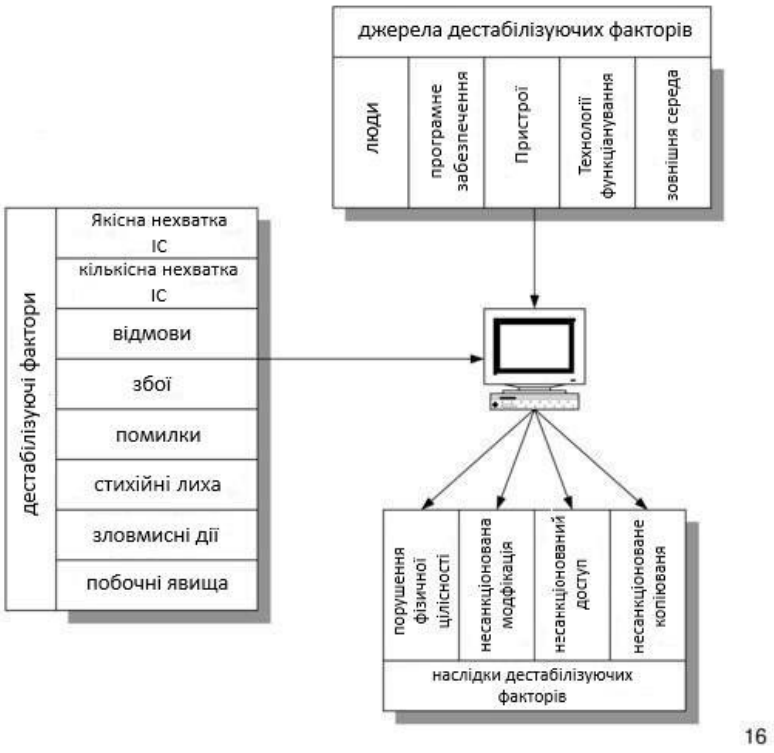
Один з найпоширеніших типів кібератак – це Фішинг, інтернет просякнут їм наскрізь й всюди. Немає такого закуточку інтернету де фішинг вас не дістане, він приходить з електронними листами на електрону пошту, зловмисник підроблюють різні сайти з ціллю отримати конфіденційні дані необачного користувача.

Атаки за допомогою вірусного програмного забезпечення – тип атаки під час якої на комп'ютері користувача з'являються вірусні програми, прикладом є KeyLogger(також використовується в ОС для роботи з клавіатурами, у випадку вірусу,

перехоплює дані о нажатих клавіш під час введення паролю, чи логіну), вірус-майнер(використовує обчислювальні потужності комп’ютера користувача для майнингу), вірусне програмне забезпечення віддаленого керування(рідко використовуються, так як його легко помітити), вірусне програмне забезпечення для копіюваннння та надсилання файлів та інші.

Також це можна назвати дестабілізуючими факторами комп’ютерної мережі та інформаційних систем.

Джерела дестабілізуючих факторів – це те що впливає на ймовірність їх з’явлення у мережі та комп’ютерних пристроях. Частіше джерелом є самі користувачі(люди) через низьку свідомість багатьох у кібергігієні. Програмне забезпечення теж може бути джерелом, якщо вірус був вшити до програмного коду, чи схован до файлів програми окремим додатком. Пристрої що можуть нанести шкоди системі, наприклад USB Killer. Технології функціонування – фактор який може призвести до системних збоїв, такі як непередбачуване вимкнення системи. Фактори зовнішньої середи – це фізичні втручання до роботи обчислювальної техніки.



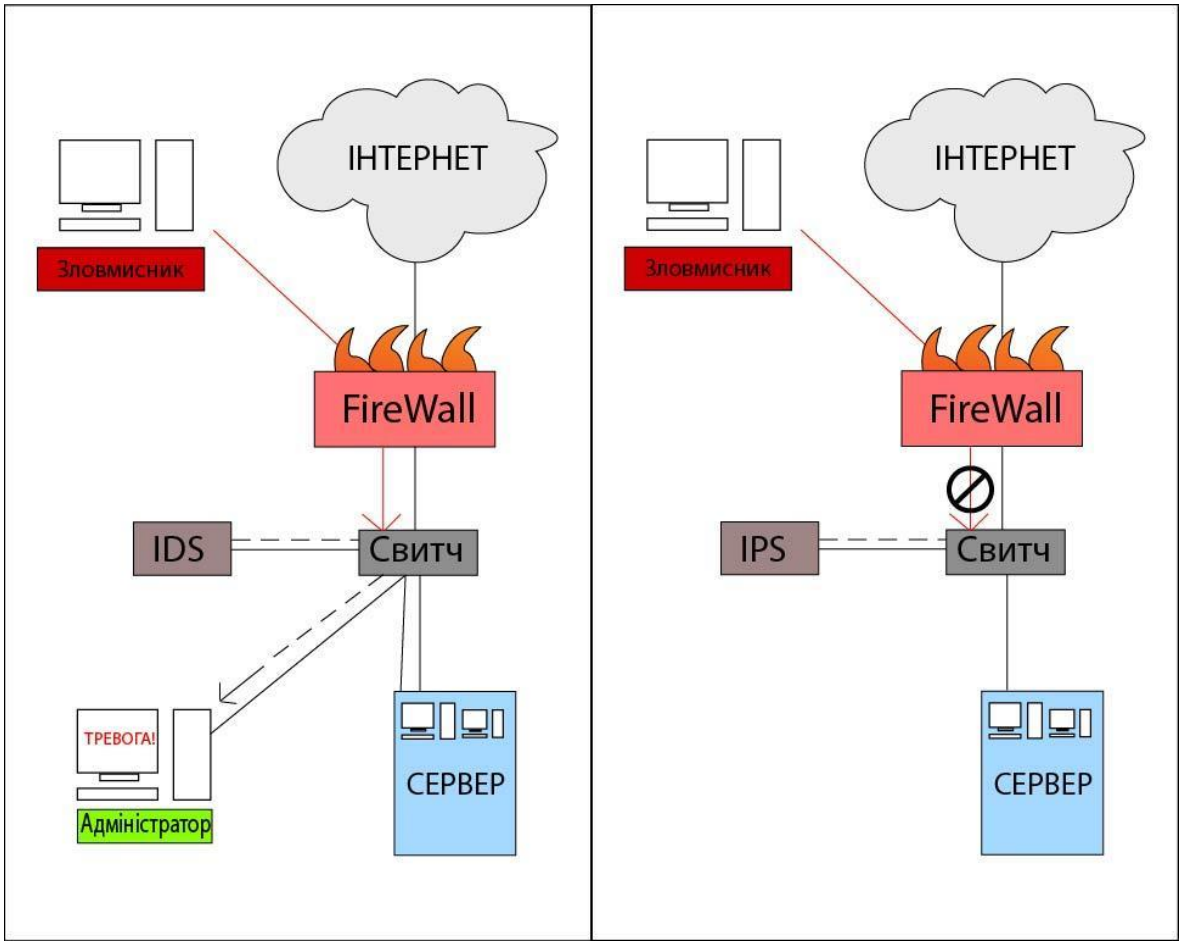
Малюнок 2.1 – Дестабілізуючі фактори

Дестабілізуючі фактори – це то що призводить до того, що обчислювальна техніка припинила свою роботу, або працює некоректно. Якісною нехваткою, можно назвати застарілість техніки, або нехватку обчислювального потенціалу для виконання певних завдань. Кількісна нехватка – нехватка обчислювальної техніки на підприємстві (працівників більше ніж техніки) для виконання завдань, та спроможності забезпечити її для всіх працівників. Відмови – коли техніка не може виконати певну задачу через відсутність необхідних дозволів чи ситемних файлів. Збої – це фактор який виникає при некоректній роботі з технікою, некоректній роботі самої техніки, чи певних файлів системи. Помилки – фактор що виникає при некоректній роботі програми, чи засобів керування обчислювальної техніки. Стихійні лиха – це фактор який не залежіть від людини, він є ненавмисним, але може призвести до критичних несправностей. Зловмисні дії – втручання до роботи обчислювальної техніки особ що не мають доступу до системи та її даних. До побочних явищ як

фактора можно віднести перегрузку мережі(інтернет та електромережі) через велику кількість підключеної техніки, фізичний знос елементів обчислювальної техніки.

2.3Інструменти виявлення та запобігання вторгнень

Інструменти виявлення та запобігання вторгненням (IDS/IPS) – це програмне забезпечення або апаратні пристрої, які використовуються для виявлення та запобігання несанкціонованому доступу до комп'ютерних систем. Вони відіграють важливу роль у кібербезпеці, допомагаючи захищати мережі, сервери та дані від атак.



Малюнок 2.2 – Схематичне представлення того як працює IDS та IPS

Системи виявлення вторгнень або IDS – це системи які моніторять мережевий трафік на наявність аномальних активностей, у випадку виявлення повідомляють про це адміністратору системи. До систем IDS відноситься Cisco Secure IDS одна з

найпопулярніших й найнадійніших серед своїх аналогів. Cisco Secure IDS – це комплекс апаратно-програмного забезпечення який підключається до світчів для контролю трафіку всередині мережі, також підключається до сервера й контролює увесь вхідний та вихідний трафік.

Системи запобігання вторгнень або IPS – це системи які моніторять трафік мережі й при виявлені аномальних активностей блокує їх джерело. До систем IPS які часто використовують при захисті серверів та персональних комп'ютерів від вторгнень є система Fail2Ban, вона є вшитою до деяких антивірусних програм й іноді використовується як окрема програма. Її принцип роботи достатньо простий, при виявлені аномалії які можно віднести до атак типу DoS, які використовують для перевантаження сервера, або для отримання доступу методом підбору логінів та паролів Bruteforce, коли система Fail2Ban це бачить вона спочатку блокує зв'язок з тим від кого це їде на короткий час, і поступово збільшує час блоку кожного разу, до поки цей користувач не буде повністю заблокован.

Один з найкращих засобів запобігання та виявлення вторгнень для персональних комп'ютерів та серверів – це комплекс програмного забезпечення Symantec Endpoint Protection від компанії Symantec, яка займається розробкою антивірусного та антишпигунського програмного забезпечення, а також системами запобігання та виявлення вторгнень, завдяки чому при організації захисту не треба шукати окремо антивірусне, окремо антишпигунське та інше програмне забезпечення, достатньо встановити комплекс Symantec Endpoint Protection, та зайнятися системами контролю доступу, системою шифрування, та системами виявлення вторгнень на рівні мережі(Symantec Endpoint Protection виявляє вторгнення на рівні програмного забезпечення та операційних систем).

3 ДОСЛІДЖЕННЯ ВИПАДКУ У ГОСПОДАРСЬКОМУ СУДІ ОДЕСЬКОЇ ОБЛАСТІ

3.1 Об’єкт дослідження та джерела інформації

Об’єктом дослідження є сервер бази даних Господарського суду, на якому зберігалась велика кількість даних по судових справах, учасниках справ та усіх працівників. Ці дані є конфіденціальним, а дані по судовим справам мають статус документів з обмеженим рівнем допуску, окрім документів які видаються учасниками справ(ухвала, повідомлення про виклик до суду, повідомлення про розгляд, рішення).

Згідно з законодавством України що до кібербезпеки та державних документів, ці данні мають бути захищенні по високим стандартам, але все ж таки сервер господарського суду був взламаний.

Джерелами інформації про те що трапилося та рівень захисту який на той момент був є ДП ІІТ ІСС, та адміністратор господарського суду, документи про стан захисту та документи з повним описом того що сталося я нажаль не можу додати до своєї роботи так як вони мають статус державної таємниці.

Дані про стан захисту сервера та організацію мережі були надані мені одним з адміністраторів, а інформацію про то, що це був за вірус та до яких наслідків це він привів надали працівники ДП ІІТ ІСС.

На основі цих даних ми розглянемо як саме вірус потрапив у мережу суду, заразив усю мережу ї витягнув майже всі дані.

3.2 Організація захисту та внутрішньої системи об’єкту

Перше що треба розглянути це як був розгорнут сервер у Господарському суді, нажаль надати інформацію про апаратне забезпечення я не можу так як не маю доступу до даних про цей сервер, тому уся інформація яка відома була надана молодшим адміністратором(Таблия 3.1).

Таблиця 3.1 – Відомості реалізація сервера

Операційна система	Неліцензована Windows Server 2012
Антивірусне та антишпигунське програмне забезпечення	ESET Endpoint Antivirus
Система виявлення вторгнень	Устарівша без ліцензованого програмного забезпечення Cisco Secure IDS
Система контролю доступу	Не була реалізована, усі користувачі відправляли запит як адміністратор

Розглянемо тепер побудову мережі та реалізацію на комп'ютерах працівників суду.

На кожному комп'ютері був власний користувач з правами адміністратора, через відсутність централізованої системи контролю доступу у домені, на кожному комп'ютері були різні версії антивірусного програмного забезпечення від різних розробників (Avast/ESET/McAfee) через це була відсутня централізована система управління та збору звітів антивірусного програмного забезпечення.

Мережа була реалізована через свитчі, а комплекс програмно-апартного забезпечення Cisco Secure IDS яка включає в себе FirewWall та систему виявлення вторгнень, була лише при сервері для контролю вхідного та вихідного трафіку (через це система виявлення вторгнень не могла працювати належним чином та помітити вірус всередині мережі), свитчів на будівлю суду було три, для першого поверху, другого, третього й при сервері для підключення четвертого поверху та свитчів інших поверхів.

Як ми бачимо рівень захисту був не дуже високий, але щоб вірусне програмне забезпечення потрапило на сервер ї у мережу все одно треба обійти антивірусне програмне забезпечення, та зробити так щоб вірус пройшов FireWall, ї шоб вірус був встановлен, так як він був замаскован під частину програми.

3.3 Аудит захисту, причини потрапляння вірусу у мережу

Зараз ми проведемо більш глибокий аналіз захисту, розберемо причину через яку вірус потрапив у мережу та у кінці розробимо рекомендації який мав бути захист та що треба покращити.

Почнемо з причин які призвели до зараження мережі та серверу. Головна причина це відсутність у працівників розуміння кібергігієни, та належного відношення до безпеки. Точкою відліку при уражені мережі суду став секретар судового засідання, він мав виходити у відпустку але не встигав доробити декілько документів, тому вирішив встановити програму для віддаленого керування яка здалася йому надійною. Після встановлення програми комп'ютер та мережеве з'єднання на ньому почали працювати повільніше, але працівник не звернув на це уваги та вирішив не повідомляти про це адміністратору.

Таблиця 3.2 – дерево атаки вірусу

Вид шахрайства	Етап 1	Етап 2	Етап 3	Етап 4	Результат
Фішинг	Доставка вірусу	Отримання доступу	розповсюдження	Копіювання даних та маскування дій	Копіювання даних з серверу та комп’ютерів працівників, знищення серверу

Як наведено у таблиці 3.2, це план по якому зловмисник діяв. Розберемо все більш детально.

То що зловмисник використовува фішинг для отримання доступу відомо з того що програма була завантажена та встановлена з невідомого ресурсу у глобальній мережі, зловмисник міг і не планувати атаку саме на суд, але необачність та відсутність у працівника свідомості у кібергігієні дозволили шахраю отримати багато конфіденціальної інформації та державної інформації з обмеженим доступом.

Доставка вірусу до системи відбулася разом з програмою віддаленого доступу, файли вірусу були замасковані під життєво необхідні файли програми, тому застарілий антивірусний захист їх не помітив, інакше програма була би заблокована антивірусом ще на етапі встановлення, або при спробі експлуатації.

Отримання доступу відбулося через те, що після встановлення з комп'ютеру працівника було надіслано файл MSI(Microsoft Soft Installer) тихого інсталювання, що дозволило вірусу встановитися на сервері без відома адміністраторів системи.

На етапі розповсюдження вірус з сервера робив розсилку файлів інсталювання та встановлювался разом із программою віддаленого доступу як прикриття.

На останньому етапі коли зловмисник скопіював данні для прикриття своїх дії вірусне програмне забезпечення перехватило доступ до поштового клієнта та поставило маркер на пересилку електронів лістів які надходять на інший поштовий адрес, яким опинився поштовий адрес Окружного адміністративного суду, коли я це помітив я зателефонував до адміністратора Господарського суду та спитав у чому справа, чого всі листи адресовані на їх поштову адресу, та поштові адреси залів приходять до нас. Адміністратор відповів що усе з'єднання з їх сервером, на їх комп'ютерах заблоковано і вони не можуть нічого вдіяти.

Коли зловмисник отримав те що хотів, усі данні на сервері було знищенно.

Вірус копіював усі дані з сервера на протязі двох тижнів, помічено наявність вірусу у системі було в останній момент, що й призвело до таких втрат.

Тепер розглянемо які міри захисту зловмисник зміг уникнути та де були основні вразливості у захисті.

Перша головна вразливість яка кидається у очі, це відсутність системи контролю доступу до даних. Друга це відсутність централізованої системи управління антивірусним та антишпигунським програмним забезпеченням. Останнє, це відсутність у працівників свідомості про кібергігієну та байдуже ставлення до власної безпеки.

Таблиця 3.3 – Системи захисту що були уникнуті

Система захисту	Уникнена/Немає належної реалізації
FirewWal	Уникнена
Система виявлення вторгнень на рівні мережі	Немає належної реалізації
Система запобігання вторгнень	Немає належної реалізації
Антивірусне програмне забезпечення	Немає належної реалізації
Система контролю доступу	Немає належної реалізації
Свідомість працівників у кібергігієні	Немає належної реалізації(майже ніхто з працівників не мав уявлення що таке кібергігієна)

Виходячи з усіх відомих даних, та проведеня аудити систем захисту, була побудована таблиця 3.3, у якій чітко вказано які системи захисту були уникнуті, або не мали належної реалізації. Також треба пам’ятати що значну частку у захисті складає свідомість працівників у кібергігієні, та людський фактор, цього можно було уникнути й ніхто би не став проводити аудит систем захисту Господарського суду, але через відсутність спеціальних тренінгів з кібергігієни, в нас є явний доказ того що це є невід’ємною часткою безпеки.

3.4 Аналіз впливу людського фактору на основі недоліків захисту

Переїдемо до розробки рекомендацій що до покращення захисту та розглянемо як саме вони мали бути реалізовані для забезпечення захисту.

Для цього спочатку побудуємо таблицю у якій розглянемо як міри захисту мали бути реалізовані. Програмно-апаратне забезпечення для шифрування каналу зв’язку не буде розглядатися, так як вона працює з спеціалізованим каналом зв’язку який

відокремлено від глобальної мережі, та необхідний для зв’язку з серверами у києві, також ми її не будемо брати у розрахунки так як вона була реалізована на системі Unix подібних й вірус не зміг на неї встановитися, так як був розрахований на системи Windows.

Таблиця 3.4 – Як мали бути реалізовані методи захисту

Метод захисту	Реалізація
Система контролю доступу	Створення домену з розподіленням на ролі в залежності від посади працівника
Система виявлення вторгнень	Комплекси програмно-апаратного забезпечення IDS мали бути встановлені на кожному свтчі для моніторингу підозрілої активності пакетів у трафіку мережі
Система запобігання вторгнень	Комплекси програмного забезпечення мали бути встановлені на комп'ютерах працівників, такох програмно-апаратний комплекс IPS мав бути встановлений для контролю вхідного та вихідного трафіку, для змоги перервати зв’язок по якому їде підозріла активність
Антивірусне та антишпигунське програмне забепечення	Кмоплекси програмно забезпечення мали бути централізованими, з програмою керування на сервері для збору звітів, та при виявленні підозрілого файлу направляти дані про нього на інші пристрої
Firewall	Мав бути встановлений разом із комплексами IDS для аналізу пакетів, та їх блокування з глобальної мережі, та у внутрешній мережі
Свідомість працівників у кібергігієні	Мали проводитися певні регулярні тренінги з кібергігієни для підвищення захисту системи від людського фактору

Розберемо детальніше як саме мала бути реалізована система контролю доступу у домені(Таблиця 3.5), та як це допомогло би захистити систему.

Таблиця 3.6 – Розподілення ролей та їх доступу й прав

Ролі	Права доступу до сервера	Права на комп’ютері
Адміністратори	Повний доступ	Повний доступ
Молодший/помічник адміністратора	Має обмежений доступ до систем серверу, та файлів користувачів	Має обмеження на своєму комп'ютері які встановив головний адміністратор
Судді	Доступ лише до файлів та даних які відносяться до них, без прав на керування сервером прав на доступ до файлів інших	Права на створення, редагування та читання файлів, обмеження прав на встановлення програм та доступу до диску С
Помічники	Доступ лише до файлів та даних які відносяться до них та їх судді, без прав на керування сервером й прав на доступ до файлів інших	Права на створення, редагування та читання файлів, обмеження прав на встановлення програм та доступу до диску С
Серкретарі	Доступ лише до файлів та даних які відносяться до них та їх судді, без прав на керування сервером й прав на доступ до файлів інших	Права на створення, редагування та читання файлів, обмеження до прав на встановлення програм та доступу до диску С
Відділ кадрів/матеріально-технічного забезпечення/Керування апаратом	Доступ лише до файлів та даних які відносяться до них, без прав на керування сервером й прав на доступ до файлів інших	Права на створення, редагування та читання файлів, обмеження прав на встановлення програм та доступу до диску С

Якщо система контролю доступ реалізована як наведено у таблиці 12, то ймовірність того що буде встановлено вірусне програмне забезпечення зводиться до нуля, так як навіть файл тихого встановлення не зможе встановити програму без дозволу на це від адмінсатратора системи.

Також треба взяти до уваги відсутність належної реалізації системи виявлення вторгнень, принципи її роботи доволі прості(таблиця 3.7), але дуже ефективні, коли система виявлення вторгнень проаналізувала мережу та зберігла дані про те, які взаємодії є стандартиними, вона постійно перевіряє мережу на признак аномалій. В нашому випадку аномалією було розповсюдженя файлу по мережі з комп'ютера користувача, система виявлення вторгнень при виявленні файлу тихого встановлення

що гуляє по мережі одразу повідомила би про це, що дозволило би виявити та вирішити проблему.

Таблиця 37. – Принцип роботи системи виявлення вторгнень

Дія	Опис
Аналіз	Система аналізує взаємодії у мережі та зберігає дані про те які взаємодії у мережі є стандартними
Виявлення	На основі даних про те які взаємодії є стандартними система шукає у мережі признаки аномальних взаємодій
Попередження	Система надсилає на комп'ютер адміністратора повідомлення про аномальнії у мережі

Зараз коли ми закінчили розбір недоліків у системі захисту, тож можемо зробити розрахунок на основі якого розглянемо як людський фактор впливає на захист серверу та мережі підприємств.

Для визначення того як людський фактор впливає на захищеність серверу та мережі використуємо формулу оцінки надійності людини HRA(Human Reliability Assessment) та складемо таблицю з наглядним уявленням розрахунків.

Формула має вигляд:

$$R\ P_a * Q \tag{3.1}$$

де P_a– людський фактор який матиме значення 5(по шкалі від 1 до 10, 10 – максимальне значення, 1 – мінімальне);

Q – критичність наслідків, так як будь який наслідок є критичним Q буде дорівнювати 10(по шкалі від 1 до 10, 10 – максимальне значення, 1 – мінімальне);

R – ризик по шкалі від 1 до 100, де 100 це максимальний ризик.

Додамо до формули показник рівня реалізації безпеки C (10 – надійний захист, 1 – ненадійний захист), так як рівень безпеки знижує ризик, ми будемо ділити $P_a * Q$ на C, після чого отримаємо такий вигляд формули:

$$R = \frac{P_a * Q}{C}$$

(3.2)

До таблиці та формули рівень свідомості працівників не був додан, так як за це відповідає організація, а не системний адміністратор та фахівець кібербезпеки.

Таблиця 3.8 – Аналіз впливу людського фактору на ризик за формулою HRA

Метод	C_1 захисту серверу Господарському. суді	C_2 який має бути(мінімально)	$P_a * Q$	R_1	R_2
Система контролю доступу	1	9	50	50	5,5
Антивірусне ПЗ	5	8	50	10	6,25
IDS	4	6	50	12,5	8,33
IPS	2	7	50	25	7,1

Після закінчення розрахунків, ми бачимо який ризик для серверу несе неналежне налаштування методів, щоб отримати загальний відсоток небезпеки який мав сервер Господарського суду складемо всі значення R_1 так як у таблиці 3.8 вони залежать від C_1, ми отримуємо значення у 97,5% ймовірність уразнення серверу та мережі, у той час як при мінімальному значені відповідності захисту до стандартів ймовірність уразнення серверу та мережі усього 27.18%.

Тож моя головна рекомендація для підвищення захисту серверів, це робити захист хоча б мінімально відповідаючий вимогам, та проведення регулярних тренінгів з кібергігієни для працівників. Виходячи з власної практики, відомої мені інформації та виходячи з випадку у Господарському суді Одеської області, людський фактор є важливою складовою при розробці захисту.

ВИСНОВКИ

У дипломній роботі було досліджено випадок що трапився восени 2023 року у Господарському суді Одеської області. Було проведено аудит систем захисту, виявлено недоліки, складано рекомендації що до покращення мір захисту, та було засвоєно що значну частину у захисті відіграє свідомість працівників у кібергігієні,

Також було усвідомлено що при організації сервера та його захисту, обов’язково треба використовувати програмне забезпечення яке ліцензоване і має останні оновлення, та треба регулярно перевіряти наявність нових оновлень, це покращить по перше роботу програмного забезпечення, по друге підвищить рівень захисту, але треба пам’ятати що для того щоб використовувати останні версії деяких програм треба мати нове апаратне забезпечення.

Системи контролю доступу є невід’ємною частиною захисту корпоративних серверів та мереж, особливо при використанні домену, розмеження по ролям, та обмеженням доступу та прав в залежності від ролі працівника, допоможуть підняти рівень захисту від несанкціонованого встановлення невідомого програмного забезпечення.

Зроблені мною дослідження підвищили мій рівень знань в організації корпоративних мереж, організації серверів та їх захисту. Було усвідомлено наскільки кібербезпека є важливою у сучасному світі, та як свідомість працівників у кібергігієні разом із людським фактором можуть вплинути на роботу організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Information. URL: https://en.wikipedia.org/wiki/Information
2. Server. URL: https://en.wikipedia.org/wiki/Server_(computing)
3. Сервер – що це таке, як працює і навіщо потрібен. Види, функції та приклади. URL: https://termin.in.ua/server/
4. Офіційний веб-сайт Symantec Endpoint Protection. URL: https://www.broadcom.com/support/security-center/definitions?pid=sep14
5. Документація Symantec Endpoint Protection. URL: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all.html
6. Microsoft corporation. What is database security?. URL: https://azure.microsoft.com/en-gb/resources/cloud-computing-dictionary/what-is-database-security
7. Верховна Рада України. Закон Уркаїни «Про інформацію URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
8. Верховна Рада України. Закон Уркаїни «Про державну таємницю. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
9. Захист інформації. URL: https://uk.wikipedia.org/wiki/Захист_інформації
10. Microsoft corporation. Що таке інформаційна безпека. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-information-security-infosec
11. Веб-сервер. URL: https://uk.wikipedia.org/wiki/Вебсервер
12. Surfshark . Проксі-сервер: що це таке і чи потрібен він вам?. URL: https://surfshark.com/uk/blog/proxy-server
13. База даних. URL: https://uk.wikipedia.org/wiki/База_даних
14. Сервер даних. URL:https://uk.wikipedia.org/wiki/Сервер_даних
15. Як запустити поштовий сервер на VPS. URL: https://cityhost.ua/uk/blog/Yak-zapustiti-poshtoviy-server-na-vps.html

16. Врахування людського фактору в оцінці ризиків в охороні праці. URL: https://www.khadi.kharkov.ua/fileadmin/P_vcheniy_secretar/ОХОРОНА_ПРАЦІ/R_Human.pdf С.15–18.