ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захищеного обміну даними на базі протоколу SSL/TLS»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Андрій МАТВІЄНКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
МАТВІЄНКО Андрій
(прізвище, ім'я)

Керівник к.т.н., доцент БОРСУКОВСЬКИЙ ЮРІЙ
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
"___" жовтня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

МАТВІЄНКУ Андрію Анатолійовичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія захищеного обміну даними на базі протоколу SSL/TLS»

керівник кваліфікаційної роботи Борсуковський Юрій Володимирович, к.т.н., доц.
(прізвище, ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» жовтня 2024 року № ___.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
програмний код для демонстрації протоколу SSL/TLS;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми забезпечення захищеного обміну даними в організаціях.
2. Аналіз методів та засобів забезпечення захищеного обміну даними на базі

протоколу SSL/TLS.

3. Технологія забезпечення захищеного обміну даними на базі протоколу SSL/TLS.

5. Перелік графічного матеріалу

Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми забезпечення захищеного обміну даними в організації.	01.10.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	12.10.2024 р.	
3.	Аналіз методів та засобів забезпечення захищеного обміну даними на базі протоколу SSL/TLS.	27.10.2024 р.	
4.	Технологія забезпечення захищеного обміну даними на базі протоколу SSL/TLS.	03.11.2024 р.	
5.	Розроблення рекомендацій щодо застосування технології забезпечення захищеного обміну даними на базі протоколу SSL/TLS.	15.11.2024 р.	
6.	Оформлення результатів дослідження.	26.11.2024 р.	
7.	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Андрій МАТВІЄНКО

(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ

(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача МАТВІЄНКА Андрія
на тему: «Технологія захищеного обміну даними на базі протоколу SSL/TLS»

Актуальність: Сучасні компанії все більше приділяють увагу безпечному обміну даними в умовах зростаючих кіберзагроз. Надійність такого обміну є критичною для забезпечення конфіденційності та цілісності інформації, що передається між різними системами та користувачами. Незалежно від галузі та масштабу організації, питання захисту даних під час передачі залишається вкрай актуальним.

Необхідно зауважити, що впровадження та застосування технології забезпечення захищеного обміну даними на базі протоколу SSL/TLS є необхідною умовою для стійкості та ефективності бізнес-процесів організацій. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі було встановлено зміст проблеми забезпечення захищеного обміну даними в організації та визначено мету та завдання даного виду забезпечення, а також його складові частини.
2. Досліджено методи та засоби забезпечення захищеного обміну даними на базі протоколу SSL/TLS.
3. Розглянуто зміст технології забезпечення захищеного обміну даними на базі протоколу SSL/TLS та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз умов застосування технологій захищеного обміну даними та забезпечення безпеки передачі інформації на прикладі конкретної організації.
2. Запропонований порядок застосування технології забезпечення захищеного обміну даними на базі протоколу SSL/TLS бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач **МАТВІЄНКО Андрій** – присвоєння кваліфікації магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач МАТВІЄНКО Андірй до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія захищеного обміну даними на базі протоколу SSL/TLS».
Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач **МАТВІЄНКО Андрій** обрав тему роботи, метою якої було дослідити зміст технології забезпечення захищеного обміну даними на базі протоколу SSL/TLS та розробити рекомендації щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи **МАТВІЄНКО Андрій** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача **МАТВІЄНКА Андрія** на оцінку "**добре**" та присвоїти йому кваліфікацію магістра з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **Матвієнко Андрій** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)
_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 63 сторінки, 20 рисунків, 5 таблиць, 25 джерел.

Об'єкт дослідження – забезпечення захищеного обміну даними в організації.

Предмет дослідження – технологія забезпечення захищеного обміну даними на базі протоколу SSL/TLS.

Мета роботи – розробити порядок застосування технології забезпечення захищеного обміну даними в організації та рекомендації щодо її реалізації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Протокол SSL/TLS є стандартом для захисту даних, що передаються через мережу Інтернет. Він забезпечує шифрування даних, автентифікацію серверів та клієнтів, а також цілісність переданої інформації. Використання SSL/TLS дозволяє захистити комунікації між клієнтом та сервером, запобігаючи перехопленню та модифікації даних третіми особами.

В роботі проаналізовано проблему забезпечення захищеного обміну даними в організації, визначено його мету та завдання. Проведено аналіз існуючих технологій забезпечення захищеного обміну даними. Досліджено методи та засоби реалізації захищеного обміну даними на базі протоколу SSL/TLS. Визначено призначення, основні функції та склад технології SSL/TLS.

На основі досліджень, проведених в роботі, запропоновано порядок застосування технології забезпечення захищеного обміну даними в організації на базі протоколу SSL/TLS. Розроблено рекомендації фахівцям з кібербезпеки щодо застосування технології забезпечення захищеного обміну даними в організації.

Галузь використання – кібербезпека інформаційних ресурсів організації.

SSL/TLS, ЗАХИЩЕНИЙ ОБМІН ДАНИМИ, КІБЕРБЕЗПЕКА, ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ

ABSTRACT

Text part of the qualification work: 63 pages, 20 figures, 5 tables, 25 sources.

The object of research is to ensure secure data exchange in the organization.

The subject of research is the technology of providing secure data exchange based on the SSL/TLS protocol.

Purpose of the study - to develop a procedure for applying the technology of secure data exchange in the organization and recommendations for its implementation.

Research methods - studying the literature on this topic, analysis of operational documentation, international standards and their comparison.

The SSL/TLS protocol is a standard for protecting data transmitted over the Internet. It ensures data encryption, server and client authentication, and the integrity of transmitted information. The use of SSL/TLS allows you to protect communications between the client and the server, preventing the interception and modification of data by third parties.

The paper analyzes the problem of ensuring secure data exchange in an organization, defines its purpose and objectives. An analysis of existing technologies for secure data exchange is carried out. The methods and means of implementing secure data exchange based on the SSL/TLS protocol are investigated. The purpose, main functions and composition of SSL/TLS technology are determined.

Based on the research carried out in the work, the procedure for applying the technology for ensuring secure data exchange in an organization based on the SSL/TLS protocol is proposed. Recommendations for cybersecurity professionals on the use of technology to ensure secure data exchange in an organization have been developed.

Field of application - cybersecurity of information resources of the organization.

SSL/TLS, SECURE DATA EXCHANGE, CYBERSECURITY, TECHNOLOGY FOR SECURE DATA EXCHANGE

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

CA – Certification Authority

CRL – Certificate Revocation Lists

CSR – Certificate Signing Request

ECC – Elliptic Curve Cryptography

FTP – File Transfer Protocol

GDPR – General Data Protection Regulation

HIPAA – Health Insurance Portability and Accountability Act

HTTP – HyperText Transfer Protocol

IoT – Internet of Things

IP – Internet Protocol

MAC – Message Authentication Codes

MAC (у значенні адреси) – Media Access Control

PCI DSS – Payment Card Industry Data Security Standard

PKI – Public Key Infrastructure

PRF – Pseudo-Random Function

SIEM – Security Information and Event Management

SSL – Secure Sockets Layer

TLS – Transport Layer Security

ВСТУП

Актуальність дослідження. У сучасному світі інформаційні технології стали основою діяльності більшості організацій. Обмін даними між користувачами, серверами та додатками відбувається постійно, і безпека цього обміну є критично важливою. Збільшення кількості кіберзагроз, таких як перехоплення даних, атаки типу "людина посередині" (Man-in-the-Middle), вимагає впровадження надійних засобів захисту інформації під час її передачі.

Традиційні методи забезпечення безпеки, які базуються на периметральному захисті мережі, вже не є достатньо ефективними. З розвитком віддаленої роботи, хмарних сервісів та мобільних додатків, інформація часто передається поза межами корпоративної мережі. Це створює потребу в нових моделях захисту даних та протидії загрозам.

Протокол SSL/TLS (Secure Sockets Layer / Transport Layer Security) став стандартом для забезпечення захищеного обміну даними в мережі Інтернет. Він забезпечує шифрування інформації, автентифікацію сторін та цілісність даних, що передаються. Використання SSL/TLS дозволяє захистити комунікації між клієнтами та серверами, забезпечуючи безпечний доступ до веб-додатків, електронної пошти та інших сервісів.

Враховуючи вищесказане, актуальність теми даної кваліфікаційної роботи визначається необхідністю дослідження технології забезпечення захищеного обміну даними на базі протоколу SSL/TLS та розробки рекомендацій щодо її ефективного впровадження в організаціях.

Об’єкт дослідження – забезпечення захищеного обміну даними в організації.

Предмет дослідження – технологія забезпечення захищеного обміну даними на базі протоколу SSL/TLS.

Мета роботи – розробити порядок застосування технології забезпечення захищеного обміну даними в організації та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми забезпечення захищеного обміну даними в організації;

проаналізувати підходи до забезпечення захищеного обміну даними в організації;

проаналізувати існуючі рішення із забезпечення захищеного обміну даними в організації;

проаналізувати методи та засоби забезпечення захищеного обміну даними на базі протоколу SSL/TLS;

розкрити порядок реалізації технології забезпечення захищеного обміну даними в організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології забезпечення захищеного обміну даними в організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ В ОРГАНІЗАЦІЇ

1.1. Дослідження проблеми забезпечення захищеного обміну даними в організації

Організація безпеки даних є головним пріоритетом для кожної організації, оскільки захист інформації стає все більш критичним у сучасному цифровому світі. Однак, як показує література, існує дефіцит глибокого розуміння переваг та недоліків існуючих технік захисту даних. Це ускладнює вибір оптимальних методів та створює потенційні вразливості в системах безпеки [17].

З появою терміну "великі дані" (Big Data) організації отримали безпрецедентні можливості для збору, обробки та аналізу величезних обсягів інформації, що генерується з різних джерел. Ці джерела включають цифрові пристрої, які фіксують дані під час операцій, машини, що автоматично створюють дані у промислових середовищах, та людей, які генерують мультимедійний контент, такий як аудіо, відео та текстові записи. Аналіз таких даних дозволяє компаніям отримувати важливі бізнес-інсайти, оптимізувати процеси, створювати нові продукти та покращувати взаємодію з клієнтами.

Проте, з іншого боку, масштаб і різноманітність даних створюють значні виклики щодо їх безпеки. Кожна додаткова точка збору даних стає потенційною вразливістю, яку можуть експлуатувати зловмисники. Обсяг даних настільки великий, що традиційні засоби захисту можуть виявитися недостатніми для ефективного запобігання загрозам. Крім того, специфіка великих даних — зокрема, швидкість і динаміка створення та обробки інформації — потребує постійного моніторингу та негайного реагування на потенційні атаки. У цих умовах критично важливим стає впровадження сучасних технологій захисту, таких як шифрування за допомогою SSL/TLS, які забезпечують безпечну передачу даних та знижують ризик їх перехоплення.

Соціальні платформи, такі як Facebook, Telegram, Twitter та LinkedIn, стали невід'ємною частиною сучасного інформаційного простору, пропонуючи зручні інструменти для спілкування, співпраці та обміну знаннями. Вони забезпечують безпрецедентну можливість об'єднувати людей по всьому світу, поширювати інформацію в реальному часі, підтримувати зв'язок з колегами, друзями та навіть спілкуватися з великими аудиторіями за допомогою одного повідомлення. Ця відкритість та доступність сприяють створенню нових бізнес-моделей, підвищенню продуктивності праці, швидшому обміну ідеями та можливостям для інновацій.

Проте, з іншого боку, така відкритість створює значні виклики у сфері безпеки та конфіденційності. Ці платформи дозволяють невідомим сторонам і навіть зловмисникам отримувати доступ до особистих даних користувачів, що може призводити до серйозних наслідків, таких як порушення приватності, шахрайство або витоки чутливої інформації. Дані, які публікуються або передаються через соціальні мережі, можуть бути використані для кіберзлочинів, зокрема фішингових атак, що ставлять під загрозу безпеку не лише окремих осіб, але й цілих організацій. Загроза стає ще більш серйозною, коли зловмисники експлуатують уразливості в системах або використовують соціальні платформи як середовище для запуску шкідливого програмного забезпечення.

У цьому контексті організаціям необхідно знайти баланс між використанням відкритих сервісів для бізнесу та ефективним захистом інформації. Це включає впровадження політик безпеки, використання сучасних технологій для шифрування даних, таких як SSL/TLS, а також постійне навчання співробітників з питань кібербезпеки. Організації повинні ретельно відстежувати, хто має доступ до їхніх даних, та забезпечувати контроль за тим, як ці дані використовуються. Лише комплексний підхід до захисту інформації дозволить скористатися перевагами соціальних платформ, не наражаючи при цьому себе на непотрібні ризики.

Згідно зі статистикою (рис. 1.1), найбільш поширеними причинами порушення безпеки та витоків даних є людський фактор і проблеми з обліковими даними. Зокрема, 85% порушень пов'язані з людськими помилками, що підкреслює

важливість навчання персоналу та запровадження надійних політик доступу. 61% інцидентів стосуються використання вкрадених або ненадійних облікових даних, що свідчить про необхідність посиленої автентифікації та шифрування переданих даних. У цьому контексті протокол SSL/TLS відіграє ключову роль, забезпечуючи захищений обмін інформацією між користувачами та серверами, що знижує ризик перехоплення облікових даних та захищає комунікації від атак.

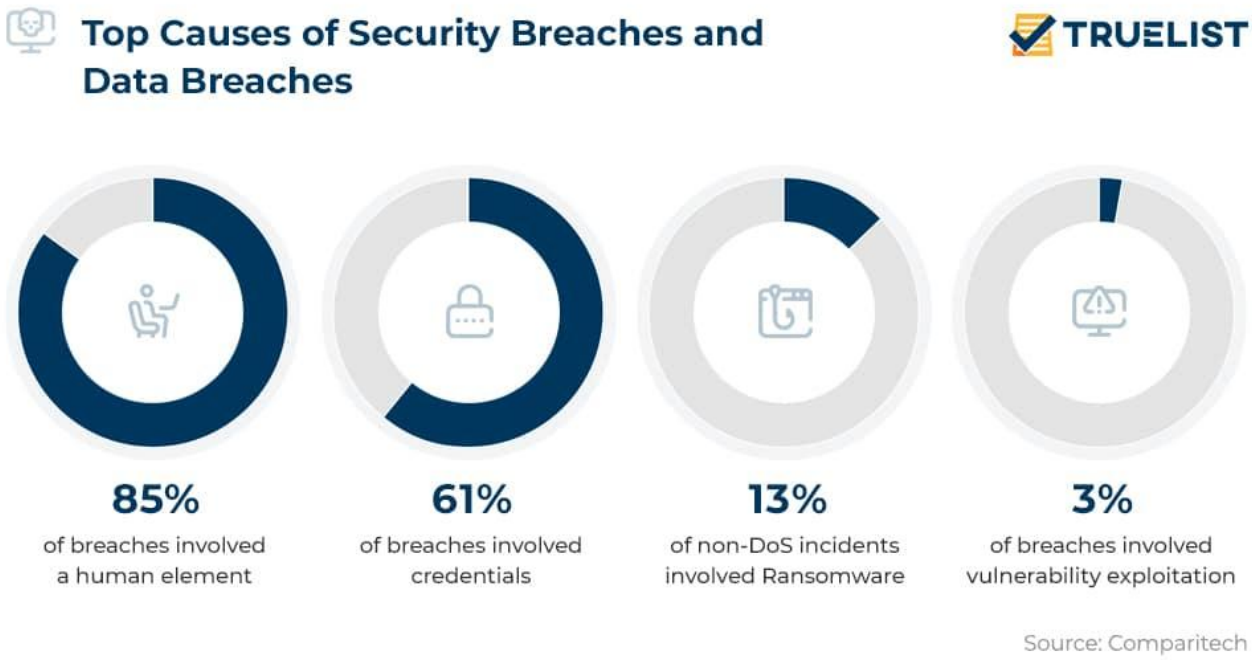

Рис. 1.1. Статистика причин витоків інформації [1]

Важливість впровадження SSL/TLS полягає у створенні надійного захисту під час передачі даних, що особливо актуально в умовах зростання загроз, таких як програми-вимагачі (13%) та експлуатація вразливостей (3%). Таким чином, використання SSL/TLS є одним із критичних засобів запобігання витокам даних та забезпечення цілісності інформації.

Різні методи захисту даних, такі як контроль доступу, автентифікація, резервне копіювання та відновлення, маскування даних та забезпечення стійкості даних, пропонують рішення для підвищення безпеки. Наприклад, контроль доступу встановлює політики для обмеження несанкціонованого доступу, а автентифікація гарантує, що тільки авторизовані користувачі можуть отримати

доступ до інформації. Проте, впровадження цих методів може бути складним та вимагати значних ресурсів.

Згідно з дослідженням компанії IBM, 75% зростання середніх витрат на порушення безпеки в цьому році було зумовлено втратою бізнесу та витратами на постінцидентні заходи реагування [9]. Це свідчить про те, що інвестування в підготовку до реагування на інциденти може значно знизити витрати, пов'язані з порушеннями безпеки. Однак багато організацій недооцінюють важливість попередньої підготовки та не впроваджують ефективні стратегії захисту даних. Це підкреслює необхідність інвестування в сучасні технології забезпечення безпеки, такі як протокол SSL/TLS, для мінімізації ризиків та фінансових втрат.

Незалежно від того, які технічні рішення в кінцевому підсумку будуть використані в компанії, вони повинні бути обрані та впроваджені центральним органом. У більшості випадків IT-відділ є правильним підрозділом, який може оцінити та впровадити рішення з технічної точки зору. Мінімальною технічною вимогою тут має бути шифрування передачі даних за допомогою SSL або TLS, а також шифрування даних на відповідному сервері за допомогою AES-256.

Інтеграція такого принципу безпечного обміну даними з технологією SSL/TLS дозволяє забезпечити комплексний підхід до захисту інформації в організації.

Обмін даними в бізнес-процесах охоплює різні сценарії захищеного обміну інформацією, зокрема надсилання повідомлень з вкладеннями через зашифровані електронні листи, а також розміщення файлів у захищених хмарних папках для доступу зовнішніх користувачів. SSL/TLS тут виступає основним механізмом захисту під час передачі даних, запобігаючи перехопленню та несанкціонованому доступу. Завдяки цьому навіть при обміні файлами через загальні папки чи хмарні сервіси можна забезпечити високий рівень безпеки.

Ще один важливий аспект — доступ для всіх працівників. За даними досліджень, 70% співробітників мають доступ до чутливих даних, що підкреслює необхідність поширення рішень для захищеного обміну інформацією на всіх працівників. Технології SSL/TLS мають бути легко доступними та інтегрованими

в робочі інструменти (наприклад, через плагіни для Outlook), щоб усі співробітники могли безпечно обмінюватися даними без необхідності додаткового навчання. Цей підхід мінімізує ризик людських помилок і підвищує загальну ефективність системи безпеки.

Простота використання та інтеграція також відіграють вирішальну роль. Для того щоб рішення для захищеного обміну даними були ефективно прийняті всіма працівниками, інтерфейс має бути інтуїтивно зрозумілим. SSL/TLS-технології повинні бути інтегровані у вже звичні для співробітників платформи, що знижує рівень складності та підвищує їх прийняття. Наприклад, інтеграція SSL/TLS у поштові клієнти або корпоративні портали дозволяє співробітникам обмінюватися даними без зайвих зусиль, що значно підвищує безпеку.

Додатковий важливий аспект — відстеження та документування передачі даних. Використання SSL/TLS дозволяє створити прозору систему, в якій можна відслідковувати, які дані передаються зовнішнім сторонам і з яким рівнем захисту. Ця функція необхідна для створення аудиторських звітів і забезпечення відповідності правовим вимогам. Системи повинні мати можливість у будь-який момент визначити, яка інформація залишила організацію і з якими правами доступу. Розділення внутрішнього та зовнішнього обміну даними також спрощує управління інформацією та додає додатковий рівень захисту.

Автоматизація процесів передачі даних є ще одним важливим аспектом. Завдяки впровадженню автоматизованих робочих процесів можна гарантувати, що певна інформація, як-от контракти чи рахунки, завжди передається з визначеним рівнем безпеки, використовуючи SSL/TLS. Це не тільки підвищує ефективність, а й мінімізує ризики людських помилок. Автоматизація таких процесів дозволяє зменшити ручну працю та скоротити час обробки, забезпечуючи при цьому найвищий рівень захисту даних.

Інтеграція SSL/TLS у всі аспекти обміну даними в організації, від централізованого шифрування до автоматизації, дозволяє створити всебічну систему безпеки, яка забезпечує захист інформації на кожному етапі її життєвого циклу.

З іншого боку, незважаючи на існування цих методів, організації все ще стикаються з викликами у забезпеченні повної безпеки даних, особливо враховуючи швидкий розвиток технологій та появу нових загроз. Це підкреслює необхідність постійного дослідження та вдосконалення технік захисту, а також розробки інноваційних підходів для забезпечення цілісності та конфіденційності даних.

Отже, забезпечення захищеного обміну даними в сучасних організаціях є вкрай важливим завданням, яке вимагає інтеграції передових технологій, таких як SSL/TLS, у всі процеси передачі інформації. Сучасний ландшафт кіберзагроз постійно змінюється, і традиційні методи захисту вже не можуть забезпечити належний рівень безпеки. Тому організаціям необхідно впроваджувати комплексний підхід, що охоплює як технічні рішення для шифрування та захисту даних, так і навчання персоналу з питань кібербезпеки, а також постійний моніторинг і вдосконалення захисних механізмів.

Впровадження SSL/TLS як основи для безпечної передачі даних дозволяє мінімізувати ризики витоків інформації та значно підвищити стійкість організації до потенційних загроз. Однак, зважаючи на динамічний розвиток цифрових технологій, важливо продовжувати інвестувати у нові інструменти та методики захисту, підтримуючи їх актуальність у відповідності до найкращих практик і стандартів кібербезпеки. Лише так можна забезпечити надійний захист даних та зберегти довіру клієнтів і партнерів у довгостроковій перспективі.

1.2 Аналіз підходів до забезпечення захищеного обміну даними в організації

Захист інформації у сучасному цифровому середовищі набуває все більшої ваги, адже обсяги переданих даних продовжують зростати, і з ними збільшується кількість потенційних загроз. Кіберзлочинці стають дедалі витонченішими у своїх методах, що ставить перед організаціями нові виклики у сфері інформаційної безпеки. Забезпечення надійного обміну даними є важливим завданням, яке

потребує впровадження ефективних технологій і постійного вдосконалення підходів до захисту.

Захист даних є важливим пріоритетом для окремих осіб, бізнесу та організацій будь-якого розміру. У сучасну цифрову епоху, коли технології стали основою для зберігання та передачі чутливої інформації, загроза порушень безпеки та викрадення даних стала серйозною проблемою. Зокрема, зростання кількості кібератак, таких як хакерські зломи, підкреслює необхідність впровадження ефективних засобів захисту. Цей розділ присвячений аналізу підходів, які використовуються для забезпечення безпеки даних, включаючи різні методи захисту, які дозволяють зменшити ризики та забезпечити конфіденційність інформації.

Щоб зменшити ризики пов'язані з витоками даних, існує декілька методів захисту, зокрема спрямованих на захист даних від несанкціонованого доступу та маніпуляцій. Розглянемо 5 найкращих методів захисту.

Шифрування є фундаментальним компонентом захисту персональних даних (рис. 1.2). Воно передбачає перетворення конфіденційної інформації в закодовану форму, що робить її нечитабельною [24] для будь-кого, хто не має відповідного ключа розшифрування. Лише авторизований користувач, який володіє ключем розшифрування, може розшифрувати та пере глянути інформацію. Цей метод широко використовується для захисту конфіденційних даних під час передачі через Інтернет, а також для захисту даних, що зберігаються на пристроях, таких як ноутбуки та мобільні телефони. Крім того, алгоритми шифрування, такі як AES і RSA, використовуються для шифрування даних, що практично унеможливлює доступ до них несанкціонованих користувачів.

Однією з ключових переваг шифрування є те, що воно забезпечує високий рівень безпеки, навіть у випадку витоку даних. Якщо зашифровані дані будуть викрадені або іншим чином отримані несанкціонованою стороною, вони будуть нечитабельними, а отже, марними для зловмисника. Крім того, шифрування також допомагає організаціям дотримуватися правил і стандартів конфіденційності, таких як Загальний регламент про захист даних (GDPR) і Стандарт безпеки даних

індустрії платіжних карток (PCI DSS).

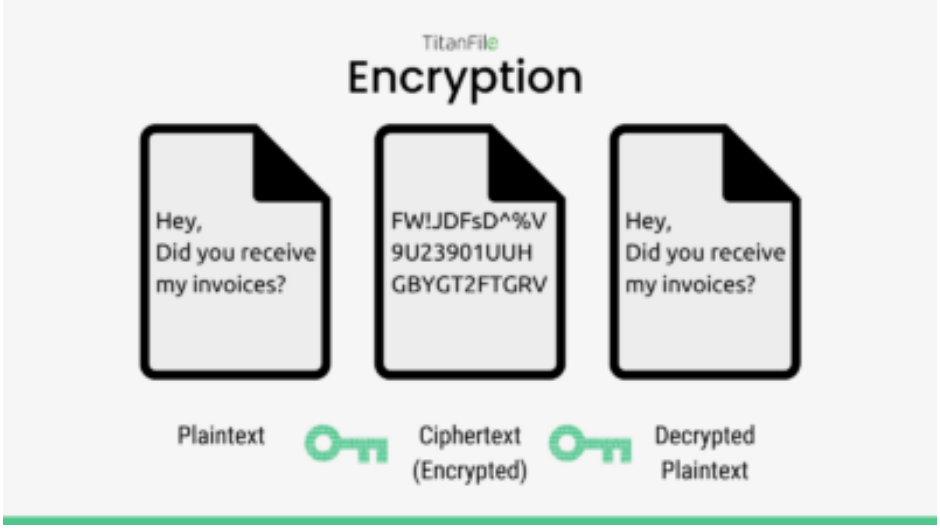

Рис. 1.2. Процес шифрування [24]

Однією з ключових переваг шифрування є те, що воно забезпечує високий рівень безпеки, навіть у випадку витоку даних. Якщо зашифровані дані будуть викрадені або іншим чином отримані несанкціонованою стороною, вони будуть нечитабельними, а отже, марними для зловмисника. Крім того, шифрування також допомагає організаціям дотримуватися правил і стандартів конфіденційності, таких як Загальний регламент про захист даних (GDPR) і Стандарт безпеки даних індустрії платіжних карток (PCI DSS).

Однак шифрування не є надійним, і для того, щоб бути ефективним, його потрібно правильно впроваджувати. Наприклад, якщо ключ шифрування втрачено або викрадено, зашифровані дані будуть недоступні навіть для законного власника. Крім того, алгоритми шифрування можуть бути зламані, особливо якщо вони не оновлюються відповідно до технологічного прогресу та атак зловмисників.

Регулярне резервне копіювання даних є важливим аспектом захисту даних, оскільки воно гарантує збереження даних у разі їх втрати або пошкодження. Створюючи копії даних і зберігаючи їх у безпечному місці, організації можуть швидко відновити свої дані в разі катастрофи. Багато компаній використовують хмарні сервіси зберігання даних, такі як TitanFile, оскільки вони забезпечують безпечний і надійний спосіб зберігання та відновлення даних. Також експерти

рекомендують використовувати метод 3-2-1 для резервного копіювання даних. Метод резервного копіювання даних 3-2-1 передбачає резервне копіювання трьох копій даних на двох локальних пристроях (тобто на оригінальному пристрої, зовнішньому жорсткому диску) і на одному зовнішньому (тобто в хмарному сховищі).

Однією з ключових переваг резервного копіювання та відновлення є те, що воно дозволяє організаціям швидко відновлюватися після втрати даних, мінімізуючи час простою і знижуючи ризик безповоротної втрати даних. Крім того, рішення для резервного копіювання та відновлення можуть забезпечити додатковий рівень безпеки, оскільки їх можна використовувати для відновлення даних до більш раннього моменту часу, ефективно скасовуючи будь-які несанкціоновані зміни або видалення.

Резервне копіювання та відновлення даних, незважаючи на їхню користь, є настільки успішним, наскільки успішним є середовище, в якому вони зберігаються. Резервні копії повинні зберігатися в безпечному місці, наприклад, за межами офісу, щоб захистити їх від крадіжок, стихійних лих та інших ризиків. Крім того, резервні копії необхідно регулярно тестувати, щоб гарантувати, що їх можна буде успішно відновити в разі критичного інциденту.

Контроль доступу - це метод обмеження доступу до конфіденційної інформації лише авторизованим користувачам. Цього можна досягти за допомогою паролів, багатофакторної автентифікації та контролю доступу на основі ролей. Ці методи гарантують, що лише ті, хто має відповідні повноваження, можуть отримати доступ до конфіденційних даних, зменшуючи ризик витоку даних та несанкціонованого доступу.

Однією з ключових переваг контролю доступу є те, що він допомагає встановити підзвітність в організаціях, дозволяючи їм відстежувати і контролювати, хто має доступ до яких ресурсів і хто виконував які дії, знижуючи ризик внутрішніх загроз. Крім того, контроль доступу підвищує ефективність, спрощуючи управління дозволами на доступ, зменшуючи час і ресурси, необхідні для управління доступом для великої кількості користувачів.

Як і всі методи захисту даних, контроль доступу повинен бути реалізований належним чином, щоб бути ефективним. Наприклад, паролі повинні бути надійними та унікальними, а для забезпечення додаткового рівня безпеки необхідно використовувати багатофакторну автентифікацію. Крім того, системи контролю доступу повинні регулярно оновлюватися і тестуватися, щоб переконатися, що вони функціонують належним чином і захищають конфіденційні дані від несанкціонованого доступу.

Іншим методом є організація безпеки мережі. Мережева безпека - це заходи, які використовуються для захисту інформації та активів, що зберігаються в комп'ютерних мережах, від несанкціонованого доступу, крадіжки або пошкодження. Це може включати використання брандмауерів для блокування несанкціонованого доступу, впровадження систем виявлення вторгнень для моніторингу та запобігання кібератакам, а також використання шифрування для захисту конфіденційної інформації, що передається мережею. Регулярне оновлення програмного забезпечення та навчання співробітників також можуть відігравати важливу роль у зниженні ризику кібератак.

Однією з ключових переваг мережевої безпеки є її роль у забезпеченні конфіденційності. Мережева безпека допомагає забезпечити конфіденційність конфіденційної інформації, запобігаючи несанкціонованому доступу та витоку даних. Вона також дозволяє організаціям відповідати нормативним вимогам і галузевим стандартам, таким як HIPAA і PCI DSS. Найважливіше те, що мережева безпека відіграє величезну роль в управлінні ризиками. Вона допомагає організаціям виявляти і зменшувати потенційні ризики безпеки, знижуючи ймовірність порушень безпеки та інших інцидентів.

Важливо зазначити, що успішна інфраструктура мережевої безпеки вимагає освіченої IT-команди. Системи мережевої безпеки можуть бути складними і важкими в управлінні, що вимагає спеціальних знань і досвіду для їх ефективного налаштування та обслуговування. Крім того, з розвитком загроз заходи мережевої безпеки повинні постійно оновлюватися і вдосконалюватися, щоб йти в ногу з новими загрозами.

Нарешті, фізична безпека є ще одним важливим компонентом захисту даних, оскільки вона включає в себе заходи, спрямовані на захист фізичних пристроїв і приміщень, в яких зберігається конфіденційна інформація. Це може включати блокування пристроїв у захищених шафах або сховищах, впровадження систем контролю доступу з біометричною автентифікацією або ключовими картками, а також встановлення камер спостереження та сигналізації у вразливих зонах. Портативні пристрої, такі як ноутбуки та мобільні телефони, також вразливі до крадіжки або втрати, і їх можна захистити за допомогою шифрування, надійних паролів та можливості віддаленого стирання даних.

Очевидною перевагою фізичної безпеки є впевненість, яку вона надає організаціям. Заходи фізичної безпеки можуть дати організаціям впевненість у цілісності та доступності їхніх резервних копій даних, зменшуючи ризик втрати або пошкодження даних. Організації також можуть зменшити витрати, захищаючи носії резервних копій, оскільки вони уникають витрат і часу, пов'язаних з відновленням даних, наприклад, відновленням даних зі стрічок або жорстких дисків.

Однак основним недоліком фізичної безпеки є людський фактор. 95% порушень кібербезпеки даних є наслідком людської помилки - незважаючи на заходи фізичної безпеки, людські помилки все ще можуть мати місце, наприклад, неправильне розміщення носія резервної копії або залишення його незахищеним. Важливо відстежувати місцезнаходження носіїв резервних копій і забезпечувати їхню безпеку перед тим, як зберігати їх.

Попри те, що існує безліч методів захисту даних, кожен з яких відіграє важливу роль у комплексній стратегії безпеки, шифрування залишається одним із найнадійніших і найефективніших засобів захисту. Воно забезпечує конфіденційність інформації, перетворюючи її в недоступну для читання форму, яку неможливо розшифрувати без відповідного ключа. Ця властивість робить шифрування критично важливим компонентом безпеки даних, особливо у випадках, коли дані передаються через Інтернет або зберігаються на пристроях, що можуть бути вразливими до фізичного чи цифрового викрадення.

Інші методи захисту, такі як резервне копіювання, контроль доступу, мережева і фізична безпека, також є важливими складовими загальної системи захисту даних. Вони забезпечують багаторівневий підхід до мінімізації ризиків, запобігаючи втраті або маніпуляціям з інформацією. Наприклад, регулярне резервне копіювання дозволяє швидко відновити дані після аварійних ситуацій, а контроль доступу обмежує можливість несанкціонованого доступу до конфіденційної інформації. Проте жоден з цих методів не забезпечує такого високого рівня конфіденційності та стійкості до перехоплення даних, як шифрування.

У цій роботі основна увага буде приділена технологіям шифрування, зокрема протоколам SSL/TLS, які використовуються для захисту даних під час їх передачі в мережі. SSL/TLS забезпечує надійне шифрування інформації, запобігаючи її перехопленню або модифікації зловмисниками. Завдяки цьому протоколу передані дані залишаються конфіденційними та захищеними від несанкціонованого доступу, що є надзвичайно важливим в умовах сучасного кіберпростору, де загрози стають дедалі витонченішими. У подальших розділах розглядатимуться деталі впровадження SSL/TLS, його принципи роботи та переваги у забезпеченні захищеного обміну інформацією.

Захист даних у сучасному цифровому середовищі вимагає комплексного підходу, який поєднує різні методи безпеки. Хоча резервне копіювання, контроль доступу, мережева та фізична безпека забезпечують важливі рівні захисту, шифрування залишається ключовим засобом для забезпечення конфіденційності і цілісності даних, особливо під час їх передачі. Використання протоколів SSL/TLS є критичним у цьому контексті, адже вони гарантують, що навіть у разі перехоплення дані залишатимуться недоступними для зловмисників. Підсумовуючи, можна сказати, що надійний захист інформації вимагає як ефективних технологічних рішень, так і правильної їх інтеграції в усі аспекти роботи організації, і саме шифрування відіграє вирішальну роль у забезпеченні безпеки у цифрову епоху.

1.3 Аналіз існуючих рішень із забезпечення захищеного обміну даними в організації

У сучасних умовах зростаючих кіберзагроз та збільшення обсягу даних, що передаються в мережах, забезпечення захищеного обміну інформацією стає критично важливим для будь-якої організації. Вибір ефективного рішення для реалізації шифрування та захисту переданих даних може суттєво вплинути на загальну безпеку інформаційної системи. Цей розділ присвячено аналізу існуючих рішень, таких як WolfSSL, BoringSSL і LibreSSL, які пропонують різні підходи до впровадження SSL/TLS. Особливу увагу буде приділено їх перевагам, недолікам та можливостям застосування в організаційному середовищі, з акцентом на LibreSSL як потенційне рішення для вибору.

WolfSSL, раніше відома як CyaSSL, є легкою, високопродуктивною бібліотекою SSL/TLS, розробленою спеціально для вбудованих систем та середовищ з обмеженими ресурсами, таких як IoT-пристрої, мобільні пристрої та вбудовані платформи. Вона була створена з акцентом на мінімізацію використання пам’яті та підвищення швидкості, при цьому забезпечуючи підтримку сучасних криптографічних алгоритмів і стандартів, включаючи TLS 1.3. Завдяки своїм властивостям, WolfSSL ідеально підходить для випадків, коли критично важлива продуктивність та ефективність, а обмеження апаратних ресурсів не дозволяють використовувати громіздкі рішення [3].

Однією з головних переваг WolfSSL є її малий розмір і оптимізована архітектура. Бібліотека займає мінімум пам’яті, що робить її ідеальною для використання на пристроях з обмеженими ресурсами, таких як мікроконтролери або IoT-системи. Крім того, завдяки оптимізованому коду WolfSSL може забезпечувати високу продуктивність, що особливо важливо для пристроїв, де кожен байт і кожен мілісекунда мають значення. Це дозволяє виконувати операції шифрування та розшифрування швидко і з мінімальним впливом на загальну продуктивність системи.

Ще однією важливою перевагою WolfSSL є підтримка сучасних стандартів і

алгоритмів. Бібліотека підтримує протокол TLS 1.3, що забезпечує кращу продуктивність і вищий рівень безпеки у порівнянні з попередніми версіями. Крім того, вона має вбудовану підтримку сучасних криптографічних алгоритмів, таких як AES, ChaCha20, Poly1305, а також Elliptic Curve Cryptography (ECC). Це означає, що WolfSSL забезпечує захист від сучасних загроз і відповідає високим вимогам до безпеки у світі, де постійно зростає кількість кібератак.

WolfSSL також має сертифікацію FIPS 140-2, що є важливим фактором для багатьох організацій, які працюють у галузях з підвищеними вимогами до безпеки. Ця сертифікація свідчить про відповідність строгим вимогам до криптографічних модулів, що робить WolfSSL відповідним рішенням для використання в урядових установах або в проектах, які підпадають під дію нормативних актів. Бібліотека також пропонує інструменти для інтеграції з іншими системами безпеки, що полегшує її впровадження у вже існуючі інфраструктури.

Проте, незважаючи на численні переваги, WolfSSL має і деякі обмеження. Вона може не бути найкращим вибором для великих корпоративних систем або серверних додатків, де потрібна більша функціональність і гнучкість, що властива таким бібліотекам, як OpenSSL. Крім того, хоча WolfSSL ідеально підходить для вбудованих і IoT-систем, її можливості можуть бути недостатніми для комплексних середовищ, де потрібна підтримка широкого спектру криптографічних функцій та розширена інтеграція.

BoringSSL — це бібліотека SSL/TLS, розроблена і підтримувана компанією Google. Вона є форком OpenSSL, створеним для задоволення специфічних потреб Google. BoringSSL була створена з метою забезпечити більшу безпеку та спрощення коду, зокрема шляхом видалення непотрібних або застарілих функцій, які не використовуються у проектах Google [6]. Це робить BoringSSL легшою і простішою у використанні бібліотекою, яка зосереджується на потребах сучасних додатків, таких як Google Chrome і серверна інфраструктура Google.

Однією з ключових особливостей BoringSSL є її фокус на безпеці та оптимізації для масштабованих веб-додатків. Розробники Google регулярно оновлюють і вдосконалюють код бібліотеки, щоб підтримувати її в актуальному

стані. Це означає, що BoringSSL постійно отримує оновлення безпеки і покращення продуктивності, що робить її надійним вибором для великомасштабних додатків. Однак ця бібліотека не орієнтована на загальне використання і призначена в першу чергу для потреб Google, що може обмежувати її корисність для сторонніх розробників.

BoringSSL має деякі переваги у порівнянні з іншими SSL/TLS бібліотеками. Наприклад, вона спрощує інтеграцію для проектів, де використовується велика кількість одночасних підключень і потрібно забезпечити високу продуктивність. Завдяки своїй оптимізації BoringSSL може впоратися з великими обсягами трафіку, не жертвуючи безпекою. Також, завдяки регулярним перевіркам коду та зосередженості на сучасних криптографічних алгоритмах, ця бібліотека може захистити від багатьох поширених уразливостей, таких як ті, що були виявлені у старих версіях OpenSSL.

Водночас BoringSSL має свої недоліки. Бібліотека не підтримує стабільний API, оскільки її розробники постійно оновлюють і модифікують код. Це означає, що сторонні розробники, які бажають використовувати BoringSSL, можуть зіткнутися з труднощами при підтримці сумісності з майбутніми версіями. Крім того, оскільки BoringSSL створена для внутрішніх потреб Google, вона не має такої ж кількості функцій, як OpenSSL, і може бути менш зручною для проектів, які вимагають специфічних криптографічних функцій.

Ще одним важливим аспектом є відсутність офіційної документації та підтримки для широкого загалу. Оскільки BoringSSL не розроблена для загального використання, вона не має тієї ж підтримки спільноти, що OpenSSL чи інші більш поширені бібліотеки. Розробники, які планують використовувати BoringSSL, повинні бути готові до того, що їм доведеться витратити більше часу на інтеграцію та підтримку.

LibreSSL — це бібліотека SSL/TLS, яка була створена командою OpenBSD як форк OpenSSL у відповідь на відомі проблеми безпеки та складності коду, які проявилися після виявлення вразливості Heartbleed [13]. Основна мета розробників LibreSSL полягала у спрощенні, очищенні та вдосконаленні кодової бази OpenSSL

для забезпечення більш надійного та безпечного функціонування. LibreSSL отримала значну підтримку від спільноти через акцент на стабільності та безпеці.

Однією з головних переваг LibreSSL є її зосередженість на чистоті та простоті коду. Розробники витратили значні зусилля на видалення застарілих і небезпечних функцій, що значно знизило ризик вразливостей, викликаних надмірно складним або незахищеним кодом. Крім того, LibreSSL регулярно оновлюється для того, щоб відповідати сучасним стандартам безпеки, забезпечуючи підтримку нових протоколів і алгоритмів шифрування. Завдяки цьому бібліотека є більш безпечною та стійкою до поширених атак у порівнянні з деякими іншими рішеннями.

LibreSSL також має репутацію надійного і стабільного рішення, яке чудово підходить для використання в системах, де безпека має першорядне значення. Завдяки активній підтримці з боку OpenBSD, яка відома своєю прихильністю до безпеки, LibreSSL є гарним вибором для критично важливих додатків. Крім того, бібліотека добре інтегрується в екосистему OpenBSD, що робить її природним вибором для проектів, які базуються на цьому операційному середовищі.

Однак LibreSSL також має деякі недоліки. Одним із них є те, що вона не є повною заміною OpenSSL для всіх можливих випадків використання, оскільки деякі функції були навмисно видалені. Це може стати проблемою для додатків, які залежать від специфічних можливостей або API OpenSSL. Крім того, хоча LibreSSL підходить для багатьох сценаріїв, вона не завжди отримує настільки ж швидкі оновлення та підтримку нових функцій, як OpenSSL, оскільки акцент зроблено на стабільності та безпеці, а не на додаванні нових можливостей.

Ще одним аспектом, який слід враховувати, є обмежена підтримка в деяких системах та проектах. Через зміни, внесені в кодову базу LibreSSL, деякі програми можуть вимагати адаптації для забезпечення повної сумісності з цією бібліотекою. Крім того, хоча LibreSSL є відмінним вибором для проектів, орієнтованих на безпеку, розробники можуть зіткнутися з певними труднощами при інтеграції у випадках, коли потрібна максимальна гнучкість або підтримка рідкісних криптографічних функцій.

Порівняння трьох рішень для забезпечення захищеного обміну даними —

WolfSSL, BoringSSL та LibreSSL — можна здійснити за кількома основними параметрами: продуктивність, простота використання, стабільність, фокус на безпеці, підтримка та цільове призначення. Розглянемо ці параметри більш детально у таблиці 1.1.

Таблиця 1.1.

Порівняння рішень для забезпечення захищеного обміну даними

Параметр	**WolfSSL**	**BoringSSL**	**LibreSSL**
Продуктивність	Висока продуктивність, оптимізована для IoT та вбудованих систем	Оптимізована для великомасштабних проектів, висока швидкодія	Стабільна продуктивність, акцент на надійність
Простота використання	Легкий API, добре документована для вбудованих пристроїв	Складна інтеграція, нестабільний API для сторонніх розробників	Спрощений та очищений код, легка інтеграція
Стабільність	Добра стабільність для вбудованих рішень, сертифікація FIPS 140-2	Стабільна, але нестабільний API через часті зміни	Висока стабільність, регулярні аудити від OpenBSD
Фокус на безпеку	Підтримка сучасних стандартів безпеки, орієнтація на сертифікацію	Відмінна безпека для масштабних систем Google, регулярні оновлення	Очищений код, акцент на безпеку та захист від уразливостей

Продовження таблиці 1.1.

Порівняння рішень для забезпечення захищеного обміну даними

Цільове призначення	Вбудовані системи, IoT, обмежені ресурси	Великомасштабні корпоративні додатки (специфічні потреби Google)	Загальне використання, серверні додатки, критичні системи
Підтримка	Сильна підтримка для IoT-платформ, документація	Відсутність офіційної підтримки для сторонніх проектів	Підтримка від OpenBSD, регулярні оновлення
Гнучкість	Обмежена для великих систем, більше для вбудованих рішень	Низька гнучкість для загального використання	Гнучка для серверних середовищ, але без деяких функцій OpenSSL

Отже, вибір падає на бібліотеку LibreSSL через її акцент на безпеку, стабільність та простоту. Ця бібліотека була створена з метою виправити недоліки OpenSSL і забезпечити більш чистий і захищений код. Для організацій, які цінують надійність і не хочуть мати справу з нестабільними API, LibreSSL є ідеальним рішенням. Вона добре підходить для звичайних серверних середовищ та критично важливих додатків, де безпека стоїть на першому місці. Крім того, постійна підтримка та аудит від команди OpenBSD гарантують, що бібліотека буде відповідати сучасним вимогам безпеки. У порівнянні з BoringSSL, яка орієнтована на специфічні корпоративні потреби Google, і WolfSSL, яка спеціалізується на вбудованих системах, LibreSSL є більш універсальним і безпечним вибором.

У сучасних умовах, коли загрози в сфері інформаційної безпеки стають дедалі серйознішими, організації змушені шукати ефективні та надійні рішення для захисту даних. Порівняння WolfSSL, BoringSSL та LibreSSL показує, що кожна з цих бібліотек має свої унікальні переваги та обмеження, залежно від цілей і потреб

конкретного проекту. WolfSSL відзначається своєю високою продуктивністю у вбудованих системах та IoT, проте її можливості можуть бути недостатніми для комплексних корпоративних рішень. BoringSSL, незважаючи на свою надійність і швидкодію, є складною для інтеграції та орієнтованою насамперед на внутрішні потреби Google. Натомість LibreSSL пропонує оптимальне поєднання безпеки, простоти та стабільності, що робить її чудовим вибором для більшості серверних додатків. Очищений код і постійна підтримка від команди OpenBSD гарантують високу якість та захист від поширених загроз. Таким чином, для забезпечення захищеного обміну даними у більшості випадків саме LibreSSL може стати найкращим рішенням, що забезпечує надійний рівень безпеки та відповідає сучасним вимогам.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ НА БАЗІ ПРОТОКОЛУ SSL/TLS

2.1 Призначення та основні функції протоколу SSL/TLS

Протокол SSL/TLS є основою сучасної безпеки передачі даних в Інтернеті. Його призначення полягає в забезпеченні конфіденційності, цілісності та автентичності інформації, яка передається між клієнтами та серверами [25]. SSL/TLS використовується для шифрування даних, запобігання їх перехопленню та несанкціонованому доступу з боку зловмисників, що особливо важливо в умовах постійно зростаючих кіберзагроз.

Використання симетричних та асиметричних алгоритмів шифрування у цьому протоколі гарантує, що лише отримувач із відповідним ключем зможе розшифрувати та прочитати передану інформацію. У сучасному світі, де обмін даними відбувається в режимі реального часу, важливість захисту конфіденційності важко переоцінити [8].

Іншим важливим аспектом роботи SSL/TLS є забезпечення цілісності інформації. Цілісність означає, що дані, які передаються між клієнтом і сервером, не можуть бути змінені або пошкоджені без виявлення. Протокол досягає цього завдяки використанню кодів автентифікації повідомлень (MAC), які обчислюються на основі переданих даних і включаються в кожне повідомлення. Якщо зловмисник спробує змінити дані в процесі передачі, MAC-код після перевірки не відповідатиме, і отримувач знатиме, що інформація була скомпрометована. Таким чином, SSL/TLS забезпечує захист від атак, спрямованих на модифікацію переданих даних.

SSL/TLS також відповідає за автентифікацію сторін з'єднання, що є ще однією важливою функцією для безпеки зв'язку. Під час процесу рукостискання (рис. 2.1) сервер надсилає клієнту сертифікат, виданий довіреним центром сертифікації, який підтверджує автентичність сервера. У деяких випадках також може виконуватися автентифікація клієнта, що додає ще один рівень захисту. Цей

механізм дозволяє переконатися, що клієнт дійсно з'єднується з легітимним сервером, а не з підставним ресурсом, створеним зловмисником. Автентифікація забезпечує довіру до з'єднання і запобігає атакам типу "людина посередині" (Man-in-the-Middle).

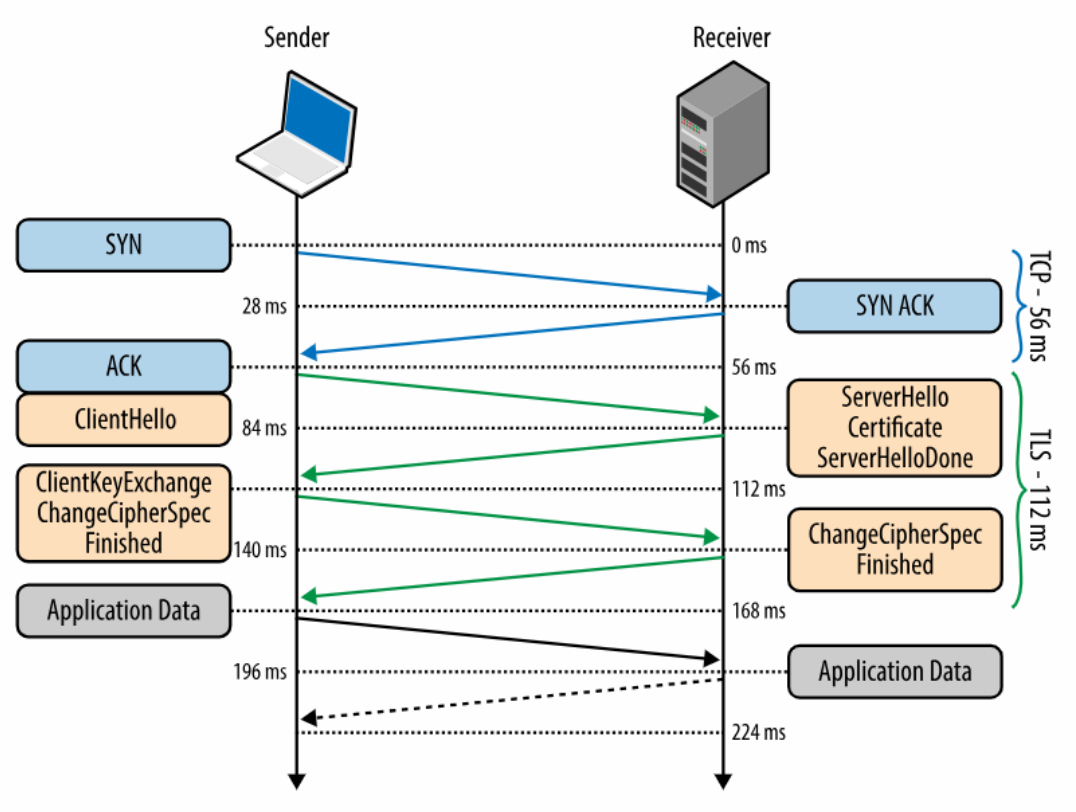

Рис. 2.1. TLS рукостискання

Одним із ключових етапів встановлення захищеного з'єднання є рукостискання SSL/TLS. Під час цього процесу узгоджуються параметри шифрування, автентифікуються сторони та генерується спільний секретний ключ, який буде використовуватися для шифрування подальших даних. Клієнт і сервер обмінюються повідомленнями "Client Hello" і "Server Hello", де визначаються криптографічні алгоритми, які будуть використовуватись. Результатом рукостискання є створення спільного секрету, який гарантує, що дані між клієнтом і сервером будуть надійно захищені. Цей процес є критично важливим для забезпечення захищеної комунікації у мережі.

Порівняння між SSL і TLS показує, наскільки суттєво вдосконалений

протокол TLS у порівнянні зі своїм попередником (таблиця 2.1.). TLS пропонує покращене обчислення MAC, використання псевдовипадкових функцій для генерування ключів і підтримку нових, більш захищених алгоритмів шифрування. Наприклад, TLS впроваджує Elliptic Curve Cryptography (ECC), яка є ефективнішою та безпечнішою в порівнянні з традиційними методами. Крім того, TLS усунув багато вразливостей, властивих SSL, що зробило його надійнішим для захисту даних у сучасних мережах.

Таблиця 2.1.

Порівняння SSL та TLS

Аспект	SSL	TLS
Безпека	Менш безпечний, вразливий до атак, таких як POODLE	Більш безпечний, з покращеними алгоритмами шифрування та механізмами захисту
Алгоритми шифрування	Підтримка старих алгоритмів, наприклад, RC4	Підтримка сучасних алгоритмів, таких як AES
Обчислення MAC	Обчислення MAC до шифрування	Обчислення MAC після шифрування
Псевдовипадкова функція (PRF)	Відсутня	Введено для покращення безпеки
Стиснення даних	Включає опцію стиснення даних	Стиснення даних за замовчуванням вимкнено
Рукостискання	Вразливе до певних типів атак	Покращене рукостискання з додатковими перевірками безпеки
Сертифікати	Обмежена підтримка нових типів сертифікатів	Підтримка нових сертифікатів та розширених параметрів автентифікації

Ще однією перевагою TLS є поліпшена структура обробки помилок. Протокол включає нові повідомлення про помилки, що дозволяють краще реагувати на потенційні загрози. Це важливо для своєчасного виявлення та запобігання спробам зловмисників зірвати з'єднання або скомпрометувати дані. Завдяки цим змінам TLS став основним вибором для захищених з'єднань у всесвітній павутині. Правильне впровадження та використання протоколу дозволяє організаціям захищати свої дані та зменшувати ризики витоку інформації.

В умовах зростаючих загроз кібератак та підвищених вимог до захисту даних знання та розуміння основних функцій SSL/TLS є необхідними. Протокол став стандартом для безпеки у веб-комунікаціях і використовується повсюдно — від банківських операцій до захисту особистих даних користувачів у соціальних мережах. Використання надійного протоколу шифрування дозволяє не тільки захистити інформацію, але й забезпечити безперервність бізнес-процесів, підвищуючи довіру з боку користувачів. Усі ці аспекти роблять SSL/TLS невід'ємною частиною сучасної цифрової безпеки.

Протокол SSL/TLS є ключовою технологією для забезпечення безпечної передачі даних у сучасних цифрових мережах. Завдяки своїй архітектурі, що дозволяє забезпечити конфіденційність, цілісність та автентичність інформації, SSL/TLS став невід'ємною частиною багатьох веб-сервісів і додатків (рис. 2.2).

Основними компонентами, які роблять цей протокол таким ефективним, є процес рукостискання, узгодження параметрів шифрування та механізми захисту від перехоплення даних. Порівняння SSL з його покращеною версією TLS показало значні переваги TLS у сфері безпеки, включаючи вдосконалене обчислення MAC, використання псевдовипадкових функцій та підтримку нових алгоритмів шифрування.

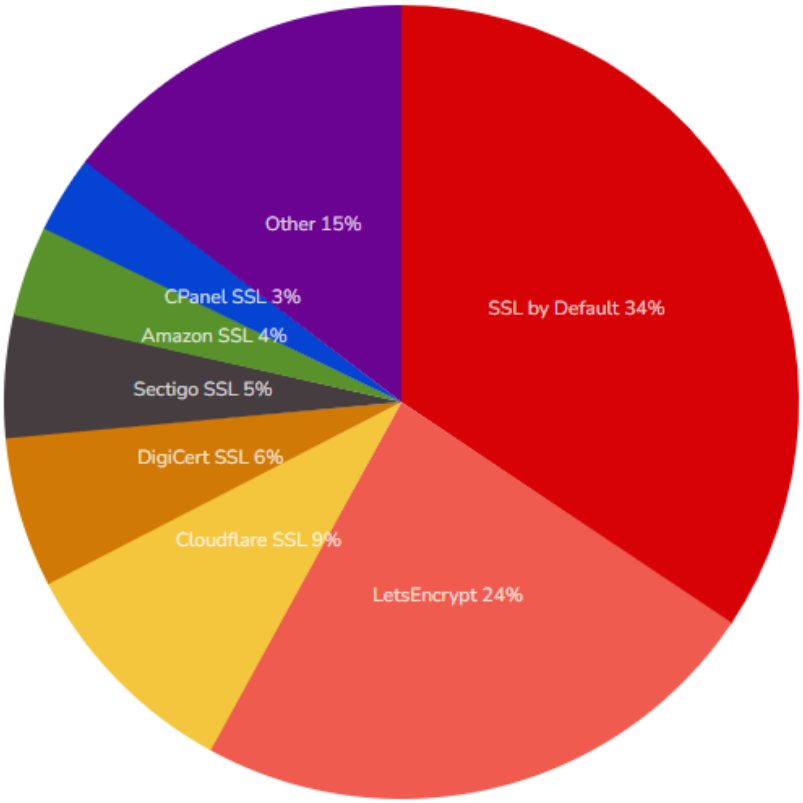

Рис. 2.2. Загальна кількість веб-сайтів, що використовують SSL [2]

Завдяки описаним поліпшенням TLS став основним вибором для забезпечення безпеки в інтернет-комунікаціях. Важливість протоколу зростає в умовах сучасного світу, де кібератаки стають все більш складними та поширеними. Знання та правильне використання можливостей SSL/TLS є необхідним для захисту конфіденційної інформації та запобігання можливим загрозам. Таким чином, SSL/TLS залишається основою для безпечного обміну даними, що забезпечує надійність і довіру в сучасному цифровому середовищі.

2.2 Основні компоненти загальної архітектури SSL/TLS

Архітектура протоколу SSL/TLS складається з декількох ключових компонентів, які працюють разом для забезпечення безпечного обміну даними в мережі. Ця архітектура забезпечує конфіденційність, цілісність і автентичність переданої інформації, що має критичне значення в умовах постійно зростаючих кіберзагроз. Основні компоненти архітектури, такі як протокол запису, протокол

рукостискання, алгоритми шифрування, хешування і методи перевірки сертифікатів, створюють комплексний захист, що гарантує надійність переданих даних. У цьому розділі буде розглянуто деталі кожного з цих компонентів, їхню роль і важливість у забезпеченні надійної та захищеної комунікації в сучасному цифровому середовищі.

SSL - це суміш чотирьох протоколів, які забезпечують безпеку протоколів верхнього рівня, таких як HTTP, FTP і будь-яких протоколів прикладного рівня. Вони розподілені на два рівні (рис. 2.3).

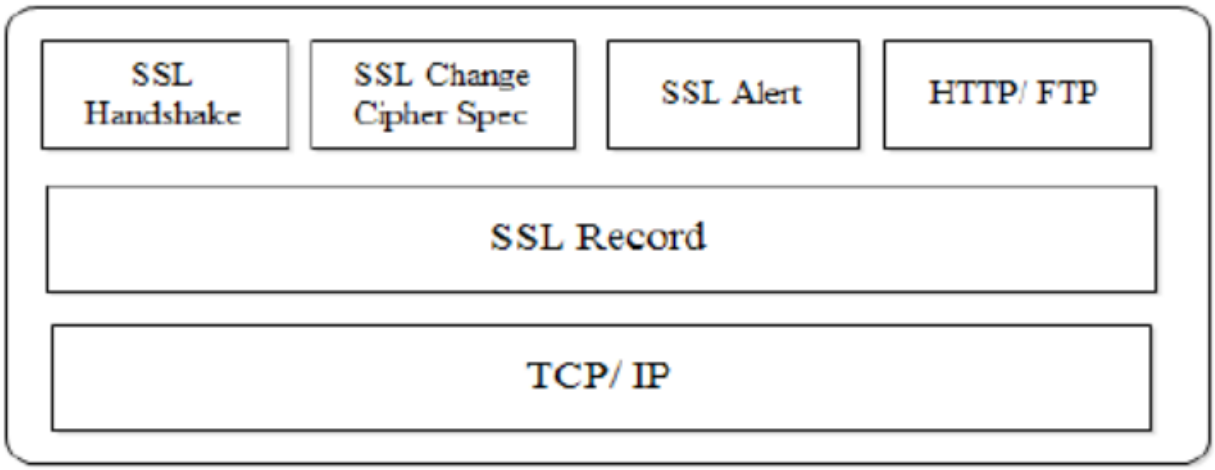

Рис. 2.3. Структура протоколу SSL [18]

SSL працює як основа для інших трьох протоколів і забезпечує конфіденційність і цілісність повідомлень верхнього рівня. На стороні відправника він сегментує інформацію на кілька частин, стискає їх, обчислює MAC-адреси і шифрує частини з відповідними MAC-адресами разом. На стороні одержувача ці процеси виконуються у зворотному напрямку до того, як оригінальні повідомлення будуть доставлені одержувачу. За замовчуванням стиснення вимкнено в SSLv3.0 і всіх версіях TLS.

SSL/TLS рукостискання — це процес встановлення захищеного з'єднання між клієнтом і сервером, під час якого узгоджуються параметри шифрування, автентифікуються обидві сторони (якщо потрібно) і генерується спільний секретний ключ для шифрування даних. Це один із найважливіших етапів роботи

протоколу SSL/TLS, адже саме завдяки йому забезпечується конфіденційність і цілісність інформації, що передається через мережу.

Рукостискання починається, коли клієнт надсилає серверу повідомлення "Client Hello" (рис. 2.4). Це повідомлення містить випадкове число, список підтримуваних криптографічних алгоритмів (CipherSuites), а також інформацію про версію протоколу. Сервер відповідає своїм повідомленням "Server Hello", в якому обирає конкретний алгоритм шифрування, який буде використовуватись для цього з'єднання, і надсилає клієнту свій сертифікат. Сертифікат містить відкритий ключ сервера і служить для підтвердження його ідентичності. На цьому етапі сервер може також запросити сертифікат від клієнта, якщо необхідна двостороння автентифікація.

Після отримання сертифіката сервера клієнт перевіряє його на відповідність певним вимогам і автентичність. Якщо сертифікат серверу довірений, клієнт продовжує процес, генеруючи секретний ключ (Pre-Master Secret) і зашифровуючи його за допомогою відкритого ключа сервера. Цей зашифрований секретний ключ клієнт надсилає серверу, і лише сервер може його розшифрувати, використовуючи свій приватний ключ. Таким чином, обидві сторони отримують однаковий спільний секретний ключ, який використовується для шифрування даних упродовж сесії.

Заключні етапи рукостискання включають повідомлення "Finished" від обох сторін. Це підтверджує, що шифрування налаштоване і обидві сторони готові до захищеного обміну даними. З цього моменту всі передані дані шифруються за допомогою симетричного шифрування, використовуючи узгоджений спільний секретний ключ. Завдяки цьому процесу клієнт і сервер можуть впевнено обмінюватися інформацією, знаючи, що їхні дані залишаються захищеними від перехоплення або несанкціонованої модифікації.

SSL/TLS рукостискання є досить складним процесом, однак забезпечує критично важливий рівень захисту для комунікацій у сучасних мережах. Завдяки йому можна запобігти численним кіберзагрозам, таким як атаки "людина посередині" (Man-in-the-Middle), і гарантувати безпечну передачу конфіденційної інформації.

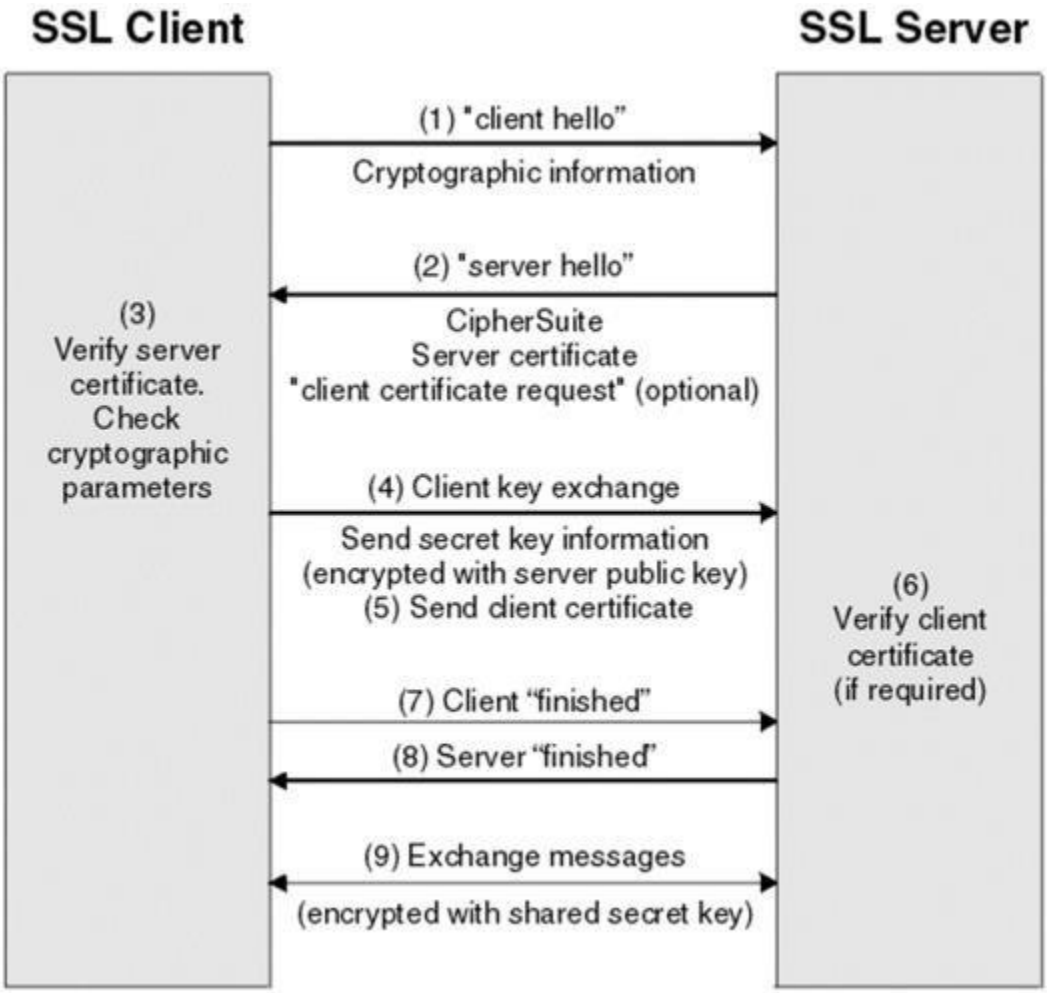

Рис. 2.4 – Процес SSL/TLS рукостискання

SSL/TLS рукостискання є досить складним процесом, однак забезпечує критично важливий рівень захисту для комунікацій у сучасних мережах. Завдяки йому можна запобігти численним кіберзагрозам, таким як атаки "людина посередині" (Man-in-the-Middle), і гарантувати безпечну передачу конфіденційної інформації.

Протокол TLS є вдосконаленою версією SSL, яка зберігає ту ж саму основну архітектуру та протоколи, але вводить кілька важливих покращень у параметри безпеки, обчислення MAC (коду автентичності повідомлення), цифрові підписи та обчислення ключових блоків. Також у TLS з’являються нові повідомлення про помилки та псевдовипадкова функція (PRF), що підвищує рівень безпеки в порівнянні з SSL. Розглянемо ключові компоненти TLS.

Версія: цей параметр вказує на основну та додаткову версії TLS,

підтримувані клієнтом. Основна та додаткова версії для різних версій TLS наведені в таблиці 1. У той час як для SSL основна версія завжди дорівнює 3, а додаткова — 0.

Таблиця 2.2.

Версії TLS

Основна версія	Додаткова версія	Клас
3	1	TLS 1.0
3	2	TLS 2.0
3	3	TLS 3.0

MAC (Код автентичності повідомлення): криптографічна хеш-функція, використовуючи спільний секретний ключ, використовується для обчислення MAC. У TLS compression_version додається до інших полів, подібних до полів фрагмента SSL, як показано у рівнянні: $MAC = MAC\_secret\_key + seq\_no + TLS\_compression\_type + TLS\_compression\_version + TLS\_compressed\_chunk\_length + TLS\_compressed\_chunk$

Псевдовипадкова функція (PRF): ця функція приймає спільний секретний ключ, тег та дані як вхідні дані і генерує результат, використовуючи операцію XOR над двома хеш-значеннями (MD5 та SHA). Спільний секретний ключ ділиться на ліву та праву частини, і дві псевдохеш-функції, Pseudo_MD5 та Pseudo_SHA, генерують кінцевий 48-байтовий результат: $PRF(shared_{secret}, tag, data) = Pseudo\_MD5\ (shared\_secret\_left,\ tag\ +\ data) + Pseudo\_SHA\ (shared\_secret\_right, tag\ +\ data)$

TLS підтримує багато з тих самих алгоритмів обміну ключами та шифрування, що й SSL, з додаванням алгоритму Еліптичної кривої Діффі-Хеллмана (ECDH) для підвищення безпеки. Однак TLS не підтримує алгоритм Fortezza.

У відповідь на запит сертифіката від сервера TLS видає сертифікати, підписані RSA або DSS, залежно від параметрів обміну ключами (RSA або відкриті параметри Діффі-Хеллмана). Вони описані в таблицях 2.3 і 2.4.

Таблиця 2.3.

Типи сертифікатів для RSA

Параметр	Тип
Обмін ключами	RSA
Підпис	Підписаний RSA

Таблиця 2.4.

Типи сертифікатів для Діффі-Хеллмана

Параметр	Тип
Обмін ключами	Відкриті параметри Діффі-Хеллмана
Підпис	Підписаний DSS або RSA

Повідомлення перевірки сертифіката: це повідомлення містить підпис сертифіката клієнта, обчислений на основі попередніх повідомлень рукопотискання. На відміну від SSL, TLS не додає до повідомлень рукопотискання головний секрет і заповнювальні біти перед хешуванням.

Заключне повідомлення: у TLS хеш (MD5 і SHA) обчислюється на основі повідомлень рукопотискання і подається на вхід PRF, що забезпечує цілісність даних.

Головний секрет у TLS обчислюється за допомогою функції PRF із трьома вхідними даними: попереднім головним секретом, тегом і конкатенацією випадкових чисел клієнта та сервера.

Ключовий блок обчислюється аналогічним чином, використовуючи головний секрет, тег і випадкові числа клієнта та сервера.

На відміну від SSL, TLS дозволяє додавати довільну кількість заповнювальних бітів (від 0 до 255) перед шифруванням. Це заповнення забезпечує, що розмір фрагмента є кратним розміру блоку шифру.

Архітектура SSL/TLS є складною, але надзвичайно важливою для забезпечення безпеки обміну даними в сучасних мережах. Основні компоненти, такі як протокол запису, протокол рукостискання, алгоритми шифрування,

хешування та сертифікація, працюють разом для створення надійного захисту інформації. SSL/TLS не лише забезпечує конфіденційність і цілісність переданих даних, але й гарантує автентичність обох сторін з'єднання, що дозволяє захиститися від численних кіберзагроз, таких як атаки "людина посередині". Вдосконалення, що внесені у протокол TLS порівняно з SSL, роблять його ще більш захищеним та ефективним у боротьбі з сучасними викликами інформаційної безпеки. Розуміння кожного з компонентів архітектури SSL/TLS дозволяє краще оцінити їх важливість та використати для забезпечення максимальної безпеки в цифровому середовищі.

2.3 Порядок функціонування протоколу SSL/TLS

Протокол SSL/TLS лежить в основі сучасної безпеки передачі даних в Інтернеті, забезпечуючи захист конфіденційної інформації шляхом шифрування та автентифікації. Основу функціоналу цього протоколу становить процес рукостискання (рис. 2.5), під час якого встановлюються всі необхідні параметри для захищеного з'єднання, зокрема вибір алгоритмів шифрування та обмін ключами. Завдяки цим механізмам SSL/TLS гарантує, що дані залишаються недоступними для перехоплення чи модифікації зловмисниками, створюючи безпечне середовище для онлайн-комунікацій та передачі інформації.

Процес TLS затиснутий між рівнями додатків і транспорту. Зараз він працює поверх обох протоколів TCP, але, очевидно, використовується і поверх UDP. Він використовує тристороннє рукостискання [15].

Щоб створити безпечне з'єднання, насамперед потрібно переконатися, що все належним чином заблоковано. TLS справляється з цим, виконуючи кілька етапів шифрування і вибираючи правильний алгоритм шифрування та ключі. Але перш ніж це станеться, сервер і клієнт повинні домовитися про те, які криптографічні методи вони будуть використовувати. Саме для цього в TLS є ціла детальна процедура, відома як тристороннє рукостискання.

Під час цього рукостискання обидві сторони з'ясовують ідентифікатор сеансу (рис. 2.5), розробляють і обмінюються ключами шифрування, генерують відкриті і

закриті ключі, а також проходять перевірку автентичності сертифікатів, серед інших дрібніших завдань. Це досить складний процес, але він гарантує, що обидві сторони знаходяться на одній сторінці і готові безпечно обмінюватися даними.

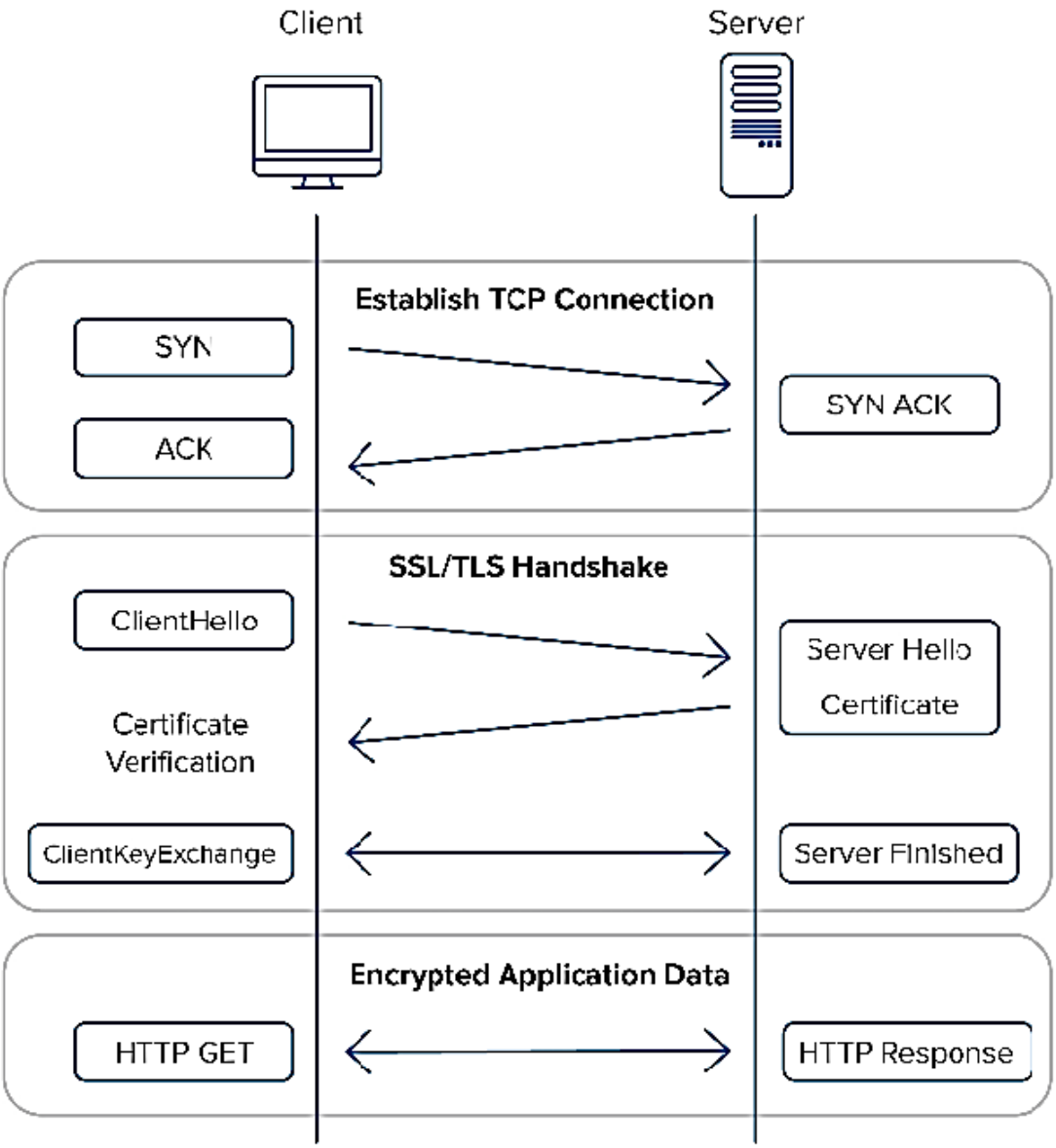

Рис. 2.5. Детальний процес SSL/TLS рукостискання [11]

Коли спостерігати аналіз трафіку у Wireshark для HTTPS-сайту, цей процес стає видимим (рис. 2.6, рис. 2.7). Початкові три пакети, позначені прапорцями для TCP-з'єднання [SYN -> SYN/ACK -> ACK], ілюструють тристороннє рукостискання TCP. Ця послідовність встановлює синхронізацію і

готовність між двома сторонами перед початком безпечного з'єднання.

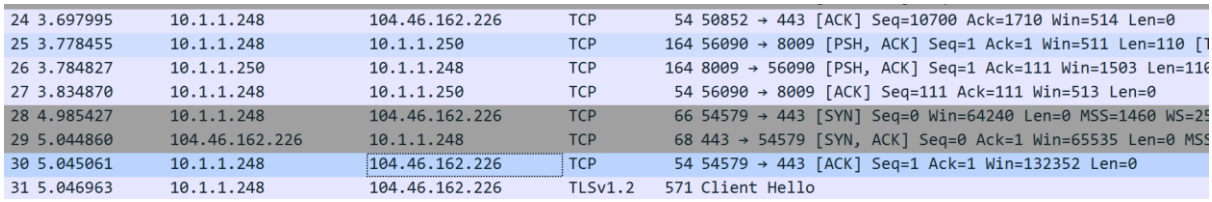

Рис. 2.6. Трафік у Wireshark для HTTPS-сайту

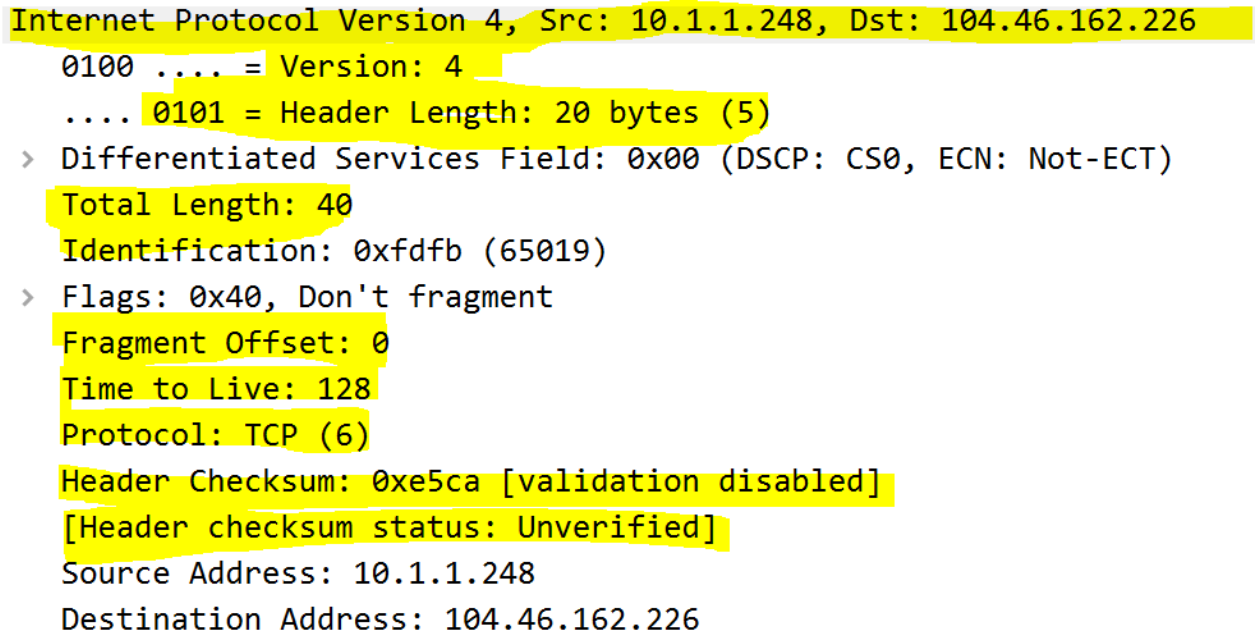

Рис. 2.7. Детальний огляд пакету

На цьому моменті можна спостерігати IPv4. Під ним - IP-адреса джерела і IP-адреса призначення. У нас є заголовок 20 байт. А загальна довжина 40. Зсув фрагмента дорівнює 0, тому що це перший фрагмент. Протокол тут - TCP (протокол транспортного рівня). TTL тут дорівнює 128. Отже, спочатку SYN буде 0, а наступний SYN буде 1. Потім буде ACK 1, після чого і SYN, і ACK встановляться на 1. Нарешті, буде встановлено лише прапорець ACK (рис. 2.8).

```
Flags: 0x012 (SYN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
```

Рис. 2.8. Встановлення прапорців

Якщо ми зануримося глибше, то побачимо, що повідомлення містить версію TLS (рис. 2.9). 32-байтне випадкове число, яке використовується для створення ключа шифрування. Ідентифікатор сесії та довжина ідентифікатора сесії. Це ідентифікаційний номер, який використовується для ідентифікації сесії клієнтом. Тут є довжину набору шифрів, яка дорівнює 32. У цьому наборі шифрів згадано 16 наборів. Цей набір може мати алгоритми для шифрування, обміну ключами та створення випадкових функцій, а також алгоритм MAC-адреси. Нижче розглянемо це детальніше.

```
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (517 bytes)
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 508
        Version: TLS 1.2 (0x0303)
        Random: 1382c58df887afe30dc66d57f77d8fea8ca0b59cffa144fed7175a53139ea7f4
        Session ID Length: 32
        Session ID: 7a11000016227ad15752722ce6047d042e493e4c956fd22fb0508b63d062b25c
        Cipher Suites Length: 32
        Cipher Suites (16 suites)
        Compression Methods Length: 1
        Compression Methods (1 method)
        Extensions Length: 403
        Extension: Reserved (GREASE) (len=0)
        Extension: server_name (len=32)
```

Рис. 2.9. Деталі пакету

Як можна спостерігати на рис. 2.10, цей шифр містить інформацію про 16 компонентів. Зокрема, у ньому представлено:

- TLS — протокол безпеки транспортного рівня, що забезпечує конфіденційність, цілісність та автентичність переданих даних.
- AES — Advanced Encryption Standard (AES), алгоритм симетричного шифрування, що використовується для створення надійного захисту. Відомий своєю високою стійкістю до злому, AES практично неможливо зламати без значних обчислювальних ресурсів.
- RSA_WITH_AES_128_GCM_SHA256 — набір алгоритмів, що включає RSA для обміну ключами, AES для шифрування даних, та SHA256 як алгоритм хешування для забезпечення автентичності повідомлень.
- Метод стиснення — необов'язковий параметр, який включає список алгоритмів, що можуть бути використані для стиснення даних на вимогу клієнта, з метою підвищення ефективності передачі.

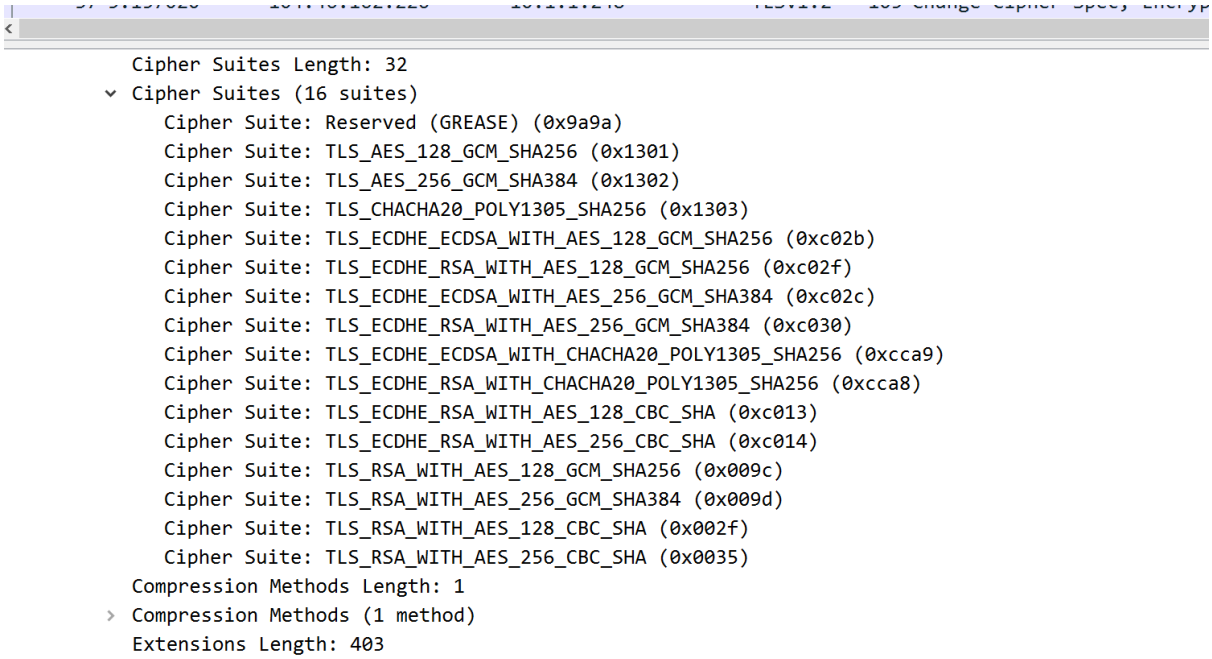

Рис. 2.10. Інформація про компоненти

Отже, протокол SSL/TLS є складним і багатогранним механізмом, який формує основу безпеки сучасних інтернет-комунікацій. Завдяки продуманій

архітектурі, що охоплює кілька етапів шифрування і перевірки, SSL/TLS забезпечує надійний захист даних від перехоплення та модифікації зловмисниками. Його процес рукостискання гарантує, що клієнт і сервер домовляються про безпечні параметри обміну даними, створюючи середовище, в якому передача інформації залишається конфіденційною та автентичною. Аналіз роботи протоколу через інструменти, як-от Wireshark, дозволяє наочно побачити, як ретельно забезпечується ця безпека на кожному етапі встановлення з'єднання. У результаті SSL/TLS продовжує залишатися критично важливою технологією, що підтримує безпечне функціонування цифрових послуг у всьому світі.

3 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ В ОРГАНІЗАЦІЇ

3.1 Розробка архітектури впровадження протоколу SSL/TLS в організації

Впровадження протоколу SSL/TLS дозволяє створити захищені канали комунікації між користувачами, системами та сервісами, мінімізуючи ризики перехоплення чи модифікації інформації. Проте, щоб протокол SSL/TLS працював ефективно і відповідав потребам організації, необхідно ретельно спланувати його інтеграцію в існуючу інфраструктуру.

Розробка архітектури впровадження SSL/TLS передбачає врахування багатьох аспектів, таких як вибір сертифікатів, налаштування серверів, підтримка актуальних версій протоколу, управління ключами та забезпечення сумісності з іншими компонентами мережі. Кожен із цих елементів має бути гармонійно інтегрований, щоб забезпечити баланс між рівнем безпеки, продуктивністю та зручністю використання.

Ефективне впровадження протоколу SSL/TLS починається з глибокого аналізу інформаційної інфраструктури організації. Цей етап є основоположним, оскільки дозволяє визначити слабкі місця та ключові компоненти системи, які потребують додаткового захисту [19].

Організації мають різні потреби залежно від типу даних, з якими вони працюють. Наприклад, фінансові установи або медичні заклади часто обробляють чутливу інформацію, яка потребує максимально високого рівня захисту. Аналіз вимог до безпеки включає [5]:

- Оцінку категорій даних (персональні дані, фінансова інформація, інтелектуальна власність).
- Визначення стандартів і нормативних вимог, таких як GDPR, HIPAA або PCI DSS, які організація зобов'язана виконувати.
- Визначення критичних сценаріїв передачі даних, що можуть становити ризик

(наприклад, обмін даними з клієнтами або між офісами).

Розглянемо умовну організацію середнього розміру, яка займається наданням фінансових послуг. Основні сервіси включають:

- Клієнтський веб-портал для управління рахунками.
- Мобільний додаток для транзакцій.
- Інтранет для співробітників із доступом до внутрішніх ресурсів.
- Обмін даними з партнерами через API.

Інфраструктура організації складається з:

1. Серверів веб-додатків і баз даних, розміщених у хмарному середовищі.
2. Локальної мережі для внутрішнього обміну інформацією.
3. IoT-пристроїв, таких як термінали для прийому платежів.

Оскільки організація працює з фінансовими даними, безпека є пріоритетом. Основними потребами є: захист персональної інформації клієнтів, включаючи номери рахунків та історію транзакцій, гарантія конфіденційності внутрішніх даних, таких як стратегічні плани та документи та захист інтеграційних API, через які здійснюється взаємодія з партнерами [14].

Інтеграція протоколу SSL/TLS у мережеву інфраструктуру є критично важливою для забезпечення безпеки даних, особливо в організаціях, що обробляють платіжні транзакції. Відповідно до стандарту PCI DSS (Payment Card Industry Data Security Standard), всі організації, які приймають, обробляють або зберігають дані платіжних карток, повинні використовувати сучасні протоколи шифрування для захисту переданих даних. Це включає впровадження SSL/TLS для захищеного обміну даними між клієнтами, серверами та внутрішніми системами [16].

Основним місцем інтеграції SSL/TLS є веб-сервери, що обслуговують клієнтські запити. У рамках PCI DSS (вимога 4.1), всі транзакції з платіжними даними повинні бути захищені під час передачі через публічні мережі. Це означає, що SSL/TLS має бути налаштований для захисту HTTPS-з’єднань, забезпечуючи конфіденційність і цілісність переданих даних. Сервери повинні використовувати сертифікати, видані довіреним центром сертифікації (CA), та виключати

використання застарілих протоколів, таких як SSL 3.0 та TLS 1.0.

Іншим важливим місцем інтеграції є API, що використовується для обміну даними між серверами або з партнерами. Відповідно до PCI DSS, необхідно забезпечити двосторонню аутентифікацію сертифікатів для всіх зовнішніх і внутрішніх API-з’єднань, що передають платіжні дані. Це не лише захищає від атак "людина посередині" (Man-in-the-Middle), але й гарантує, що дані доступні лише авторизованим сторонам.

Інтеграція SSL/TLS у внутрішню мережу організації є ключовим елементом захисту критичних даних, які передаються між різними серверними компонентами, додатками та базами даних. Такий підхід особливо важливий для організацій, що працюють з конфіденційною інформацією, зокрема даними платіжних карток, які потребують особливого рівня безпеки. Згідно з вимогою 3.4 стандарту PCI DSS, дані, що передаються в межах локальної мережі, повинні бути зашифровані, аби уникнути ризиків перехоплення або несанкціонованого доступу.

Для забезпечення цього рівня безпеки SSL/TLS використовується для встановлення захищених каналів між додатками, що обробляють дані, та базами даних, де ці дані зберігаються. Наприклад, якщо веб-додаток з'єднується з сервером бази даних для виконання запиту, під час передачі інформації використовується TLS-з’єднання. Це з’єднання гарантує, що навіть якщо зловмисник отримає доступ до мережевого трафіку, він не зможе розшифрувати дані без відповідних криптографічних ключів.

Крім того, під час інтеграції SSL/TLS у внутрішню мережу важливо забезпечити належну автентифікацію обох сторін з'єднання. Сервери баз даних і додатки повинні використовувати сертифікати SSL, видані довіреним центром сертифікації (CA), або внутрішнім CA, якщо організація має власну інфраструктуру управління сертифікатами. Це дозволяє переконатися, що зв’язок встановлюється виключно між довіреними компонентами системи.

Впровадження SSL/TLS у внутрішній мережі також передбачає регулярне оновлення та підтримку криптографічних бібліотек для забезпечення захисту від сучасних загроз. Старі версії TLS (наприклад, TLS 1.0 і 1.1) не повинні

використовуватися, оскільки вони мають відомі вразливості. Сучасні версії TLS (1.2 і 1.3) є рекомендованими стандартом PCI DSS, оскільки вони забезпечують покращену криптографічну стійкість та продуктивність.

Особливу увагу слід приділити налаштуванню параметрів шифрування. Наприклад, використання надійних алгоритмів, таких як AES-256, та відповідних режимів шифрування, таких як Galois/Counter Mode (GCM), гарантує захист даних від атак на рівні шифру. Крім того, варто налаштувати мінімально допустимі параметри хешування для підпису даних, наприклад, використовуючи SHA-256 або новіші алгоритми.

Роль управління ризиками ключів (PKI, або PKI – Public Key Infrastructure) є ключовою складовою інтеграції SSL/TLS у внутрішню мережу організації. PKI забезпечує створення, управління, розповсюдження, використання та відкликання цифрових сертифікатів і ключів, які є фундаментом для захищеного функціонування протоколу SSL/TLS. Без ефективного управління ключами навіть найсучасніші криптографічні механізми можуть стати вразливими до атак. Приблизна схема впровадження PKI зображена на рис. 3.1.

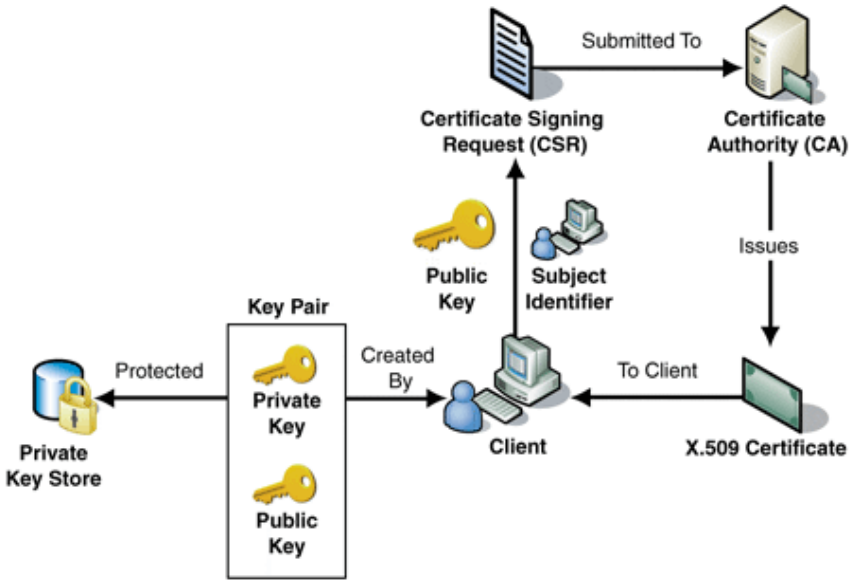

Рис. 3.1. Приклад імплементації PKI у інфраструктурі організації [14]

Цифрові сертифікати в рамках PKI використовуються для автентифікації

серверів і клієнтів у мережі. SSL/TLS потребує надійного процесу видачі сертифікатів для підтвердження довіреності обох сторін. Це досягається шляхом залучення довірених центрів сертифікації (CA). Для внутрішніх мереж організація може створити власний внутрішній CA, що дозволить зменшити витрати на сертифікацію та забезпечити контроль над видачею сертифікатів.

PKI передбачає суворі вимоги до зберігання приватних ключів. Вони мають зберігатися у захищених середовищах, таких як апаратні модулі безпеки (HSM). Це гарантує, що приватні ключі, які є основою для шифрування і підпису, не будуть скомпрометовані навіть у разі фізичного доступу до серверів.

Важливо, щоб сертифікати мали чітко визначений життєвий цикл, що включає регулярне оновлення і своєчасне відкликання у разі компрометації. Механізми, такі як списки відкликаних сертифікатів (CRL) або протокол OCSP (Online Certificate Status Protocol), дозволяють перевіряти актуальність сертифікатів у реальному часі. Це критично важливо для підтримання безпеки у динамічному середовищі організації.

Ефективна PKI передбачає створення та підтримання політик управління ключами, які визначають правила генерації, зберігання, розповсюдження та відкликання ключів. Наприклад, згідно зі стандартом PCI DSS, ключі повинні генеруватися за допомогою криптографічно стійких алгоритмів і мати достатню довжину (мінімум 2048 біт для RSA або еквівалент для ECC).

PKI інтегрується з іншими компонентами організації, такими як сервіси автентифікації, системи моніторингу та управління подіями безпеки (SIEM). Це дозволяє автоматизувати процеси управління сертифікатами та забезпечити прозорість операцій.

PKI має бути налаштована відповідно до нормативних вимог, зокрема PCI DSS, що передбачає регулярний аудит використання ключів і сертифікатів. Це дозволяє не тільки підтримувати високий рівень безпеки, але й відповідати вимогам регуляторів.

Інтеграція SSL/TLS разом із ефективним управлінням PKI створює надійне середовище для захисту даних, що передаються в межах організації. Завдяки цьому

підходу знижуються ризики компрометації ключів, забезпечується прозорість обміну даними та підтримується довіра між усіма компонентами системи.

Інтеграція SSL/TLS у внутрішню мережу не тільки мінімізує ризик компрометації даних, але й сприяє дотриманню організацією нормативних вимог, таких як PCI DSS. Завдяки цьому забезпечується цілісність, конфіденційність і автентичність переданої інформації навіть у межах локальної мережі. Такий підхід дозволяє захистити організацію від потенційних витоків даних через внутрішні вразливості або несанкціонований доступ, забезпечуючи безпеку операцій на всіх рівнях.Мобільні додатки, що взаємодіють із сервером організації, також повинні використовувати SSL/TLS для захищеного обміну даними. Відповідно до вимог PCI DSS, необхідно впроваджувати сучасні криптографічні алгоритми (наприклад, AES-256) для захисту даних, що передаються через мобільні додатки. Сертифікати, встановлені на сервері, мають бути сумісними із сучасними мобільними платформами.

Окрему увагу слід приділити IoT-пристроям, які можуть використовуватися для обробки платіжних даних, наприклад, платіжні термінали. PCI DSS рекомендує, щоб всі пристрої підтримували сучасні версії TLS, а їхні з’єднання перевірялися на предмет автентичності сертифікатів. Це знижує ризик компрометації платіжних даних через слабкі точки в архітектурі.

Інтеграція SSL/TLS відповідно до вимог PCI DSS забезпечує всебічний захист платіжних даних та інших конфіденційних даних, які передаються через мережу. Цей підхід дозволяє організаціям гарантувати дотримання стандартів безпеки, мінімізувати ризики кіберзагроз та підвищувати довіру клієнтів до наданих послуг.

Інтеграція протоколу SSL/TLS в архітектуру організації є критично важливим кроком для забезпечення захищеного обміну даними та відповідності нормативним вимогам, зокрема PCI DSS. Цей процес охоплює широкий спектр завдань, включаючи захист веб-серверів, мобільних додатків, внутрішніх мереж і IoT-пристроїв. Завдяки правильному впровадженню SSL/TLS організації отримують не лише технологічний інструмент для забезпечення безпеки, але й

підвищують свою конкурентоспроможність, створюючи довіру клієнтів та партнерів.

Використання сучасних криптографічних алгоритмів, таких як AES-256, забезпечення надійного управління ключами через PKI, а також підтримка актуальних версій протоколу TLS дозволяють мінімізувати ризики компрометації даних і знижують вразливість до сучасних кіберзагроз. Крім того, SSL/TLS надає можливість інтеграції з іншими системами безпеки, такими як SIEM, для моніторингу подій і виявлення потенційних загроз у режимі реального часу.

Дотримання стандарту PCI DSS, який визначає строгі вимоги до безпеки платіжних даних, є важливим аспектом інтеграції SSL/TLS. Це не лише допомагає уникнути штрафів і репутаційних ризиків, але й демонструє відповідальність організації перед клієнтами за захист їхніх конфіденційних даних. Такий підхід створює захищене середовище для передачі інформації, що є ключовим для організацій, які працюють з фінансовими, медичними чи іншими чутливими даними.

Розробка архітектури впровадження SSL/TLS є складним, але необхідним процесом, який вимагає врахування унікальних потреб кожної організації. Завдяки ретельному аналізу інфраструктури, плануванню, налаштуванню та регулярному оновленню компонентів системи організація може не лише забезпечити високий рівень безпеки, але й створити основу для довготривалого розвитку в умовах зростаючих кіберзагроз.

3.2 Вибір та налаштування криптографічних параметрів протоколу SSL/TLS

Вибір та налаштування криптографічних параметрів є ключовим етапом інтеграції протоколу SSL/TLS у мережеву інфраструктуру організації. Цей процес визначає рівень захисту даних, що передаються, а також стійкість системи до сучасних кіберзагроз. Криптографічні параметри, такі як алгоритми шифрування, довжина ключів, протоколи хешування та налаштування сертифікатів, мають бути

ретельно підібрані відповідно до потреб організації та вимог нормативних стандартів, таких як PCI DSS [4].

Сучасні версії TLS (1.2 і 1.3) надають широкий вибір криптографічних параметрів, які дозволяють налаштувати баланс між безпекою, продуктивністю та сумісністю. Неправильний вибір цих параметрів може призвести до вразливостей, які можуть бути використані зловмисниками, тому організації повинні приділяти особливу увагу цим аспектам. Розглянемо основні аспекти вибору криптографічних параметрів, їх налаштування та практичні рекомендації для забезпечення високого рівня захисту.

Одним із перших кроків під час налаштування SSL/TLS є вибір відповідної версії протоколу. Сучасні стандарти безпеки, такі як PCI DSS, вимагають використання виключно TLS 1.2 або TLS 1.3, адже попередні версії (SSL 3.0, TLS 1.0 та TLS 1.1) мають численні вразливості, наприклад, атаки POODLE або BEAST. TLS 1.3 є найновішою версією і включає покращення, які підвищують безпеку та продуктивність, зокрема усунення застарілих алгоритмів і спрощення процесу рукостискання. Водночас підтримка TLS 1.2 є необхідною для забезпечення сумісності з клієнтами, які ще не підтримують TLS 1.3. Таким чином, ідеальним рішенням буде встановлення TLS 1.3 із резервною підтримкою TLS 1.2 для забезпечення сумісності.

Cipher Suites — це набір криптографічних алгоритмів, які використовуються для шифрування, обміну ключами та перевірки цілісності даних [7]. Під час налаштування SSL/TLS важливо вибрати сучасні алгоритми, які відповідають вимогам безпеки. Рекомендовані алгоритми включають AES-256-GCM для симетричного шифрування, ECDHE для обміну ключами та SHA-256 або SHA-384 для хешування. Алгоритми RC4, MD5 та 3DES не рекомендуються через їхню вразливість до сучасних атак. Використання надійних Cipher Suites забезпечує конфіденційність даних та захищає від атак, таких як атака «людина посередині».

Довжина криптографічного ключа визначає стійкість алгоритму до атак грубою силою. Для алгоритмів RSA мінімальна довжина ключа повинна становити 2048 біт, що відповідає сучасним вимогам безпеки. У випадку використання

алгоритмів на основі еліптичних кривих (ECC), рекомендована довжина ключа — 256 біт. Більші ключі, наприклад RSA 4096 біт, забезпечують вищий рівень захисту, але можуть впливати на продуктивність. PCI DSS передбачає регулярне оновлення ключів, щоб забезпечити їхню актуальність та мінімізувати ризик компрометації.

LibreSSL, як сучасна та безпечна альтернатива OpenSSL, підтримує функціонал Cipher Suites, що дозволяє налаштовувати алгоритми для шифрування, обміну ключами та перевірки цілісності даних [12]. Це ключовий компонент протоколу SSL/TLS, який визначає набір криптографічних алгоритмів для забезпечення безпечного з’єднання між клієнтом і сервером. LibreSSL зосереджується на підтримці лише сучасних і перевірених алгоритмів, забезпечуючи високий рівень безпеки для організацій, що працюють із чутливими даними.

У межах LibreSSL доступні такі популярні алгоритми шифрування, як AES-128-GCM і AES-256-GCM, які вважаються галузевими стандартами для безпечного шифрування даних. Для обміну ключами використовуються алгоритми ECDHE (Еліптична крива Діффі-Геллмана), які забезпечують захист навіть у разі компрометації довготривалих ключів. Також підтримуються алгоритми хешування, такі як SHA-256 і SHA-384, які гарантують автентичність і цілісність даних. Ця комбінація алгоритмів дозволяє створювати безпечні з’єднання, які відповідають сучасним вимогам до криптографії.

LibreSSL має зручний механізм налаштування Cipher Suites. Це можна зробити через конфігураційний файл або параметри сервера, які визначають, які саме алгоритми будуть використовуватися для з'єднання. Наприклад, адміністратори можуть виключити застарілі або небезпечні Cipher Suites, такі як RC4 або MD5, і залишити лише сучасні й рекомендовані для використання алгоритми. Це дозволяє організаціям дотримуватися найкращих практик у галузі інформаційної безпеки.

Однією з ключових переваг LibreSSL є те, що вона спрощує впровадження безпечної конфігурації. На відміну від OpenSSL, LibreSSL виключає застарілі протоколи та алгоритми, які визнані небезпечними. Це зменшує ризик помилок у

налаштуванні та робить інтеграцію SSL/TLS простішою та безпечнішою. Такий підхід є особливо важливим для організацій, що працюють у регульованих галузях, де дотримання стандартів безпеки має критичне значення.

Відповідність стандартам PCI DSS є ще однією перевагою LibreSSL. Відповідно до цього стандарту, організації, що обробляють платіжні дані, повинні використовувати сучасні протоколи шифрування, такі як TLS 1.2 або 1.3, і безпечні Cipher Suites. LibreSSL дозволяє налаштувати алгоритми так, щоб вони відповідали вимогам PCI DSS, наприклад, обрати AES для шифрування, ECDHE для обміну ключами та SHA-256 для хешування. Це забезпечує не лише захист даних, а й відповідність нормативним вимогам.

Завдяки фокусу на безпеці, LibreSSL стає надійним вибором для організацій, що прагнуть забезпечити захист чутливих даних. Його підтримка сучасних криптографічних стандартів, простота налаштування та відповідність галузевим стандартам роблять цю бібліотеку ефективним інструментом для реалізації протоколу SSL/TLS у різноманітних інфраструктурах.

SSL/TLS сертифікати є фундаментом для встановлення захищених з'єднань між клієнтом і сервером, забезпечуючи автентифікацію обох сторін і створення довіри у цифровому середовищі. Ці сертифікати підтверджують автентичність серверів, гарантують, що користувачі взаємодіють із справжнім ресурсом, а не з підробленим. Без них неможливо забезпечити необхідний рівень безпеки під час обміну чутливими даними, такими як платіжна інформація чи персональні дані.

Сертифікати SSL/TLS повинні бути видані довіреним центром сертифікації (CA), який гарантує їхню легітимність. Для організацій, що працюють у приватних мережах або внутрішньому середовищі, можливе створення власного центру сертифікації (internal CA). Такий підхід дозволяє організації контролювати видачу та управління сертифікатами, зменшуючи залежність від сторонніх провайдерів. Проте у публічних середовищах для взаємодії з клієнтами використання сертифікатів від відомих CA є обов’язковим.

На рис. 3.2 представлено процес отримання сертифіката SSL/TLS, який включає наступні етапи:

1. Запит від клієнта до центру сертифікації (CA). Клієнт (наприклад, веб-браузер або інший пристрій) ініціює запит до центру сертифікації (CA) для перевірки автентичності сервера.
2. Сервер відправляє запит на сертифікацію до CA разом з інформацією про свою ідентифікацію, включаючи відкритий ключ і доменне ім’я.
3. Центр сертифікації перевіряє інформацію, що надходить від сервера, підтверджує його автентичність і видає підписаний сертифікат SSL/TLS.
4. Сервер отримує сертифікат, встановлює його і використовує для забезпечення захищеного з'єднання.
5. Клієнт та сервер встановлюють захищене з'єднання, обмінюючись даними через SSL/TLS, використовуючи сертифікат для автентифікації.

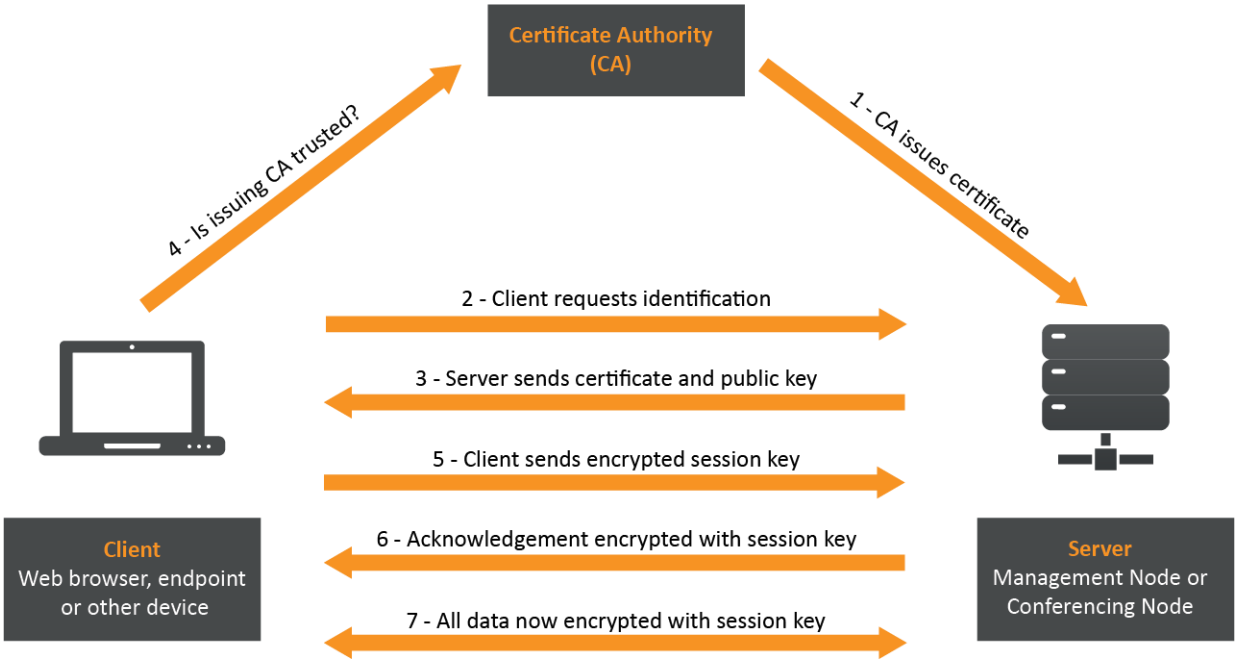

Рис. 3.2. Процес отримання сертифіката SSL/TLS [23]

Стандарт PCI DSS встановлює жорсткі вимоги до сертифікатів SSL/TLS. Вони мають бути дійсними, регулярно оновлюватись і відповідати доменам серверів, з якими відбувається комунікація. Це означає, що сертифікати не можуть бути простроченими або налаштованими на невірні домени. Для забезпечення цього важливо запровадити механізми моніторингу й автоматичного оновлення

сертифікатів. Недотримання цих вимог може призвести до ризику несанкціонованого доступу до даних та невідповідності стандартам безпеки.

Використання самопідписаних сертифікатів дозволяється лише у внутрішніх середовищах, де знижується ризик зовнішніх атак. Однак навіть у таких випадках необхідно дотримуватися чіткої політики управління сертифікатами, яка включає регулярне оновлення, контроль доступу та аудит їх використання. Без належного управління самопідписані сертифікати можуть стати джерелом вразливостей.

Криптографічна стійкість сертифікатів є ще одним ключовим аспектом. Відповідно до сучасних вимог, сертифікати повинні використовувати надійні алгоритми шифрування. Наприклад, RSA з довжиною ключа не менше 2048 біт або ECC (криптографія на основі еліптичних кривих), що забезпечує високу безпеку при меншій довжині ключів. Це дозволяє захистити дані навіть у разі спроб злому.

Отже, правильне налаштування, регулярне оновлення та використання сучасних криптографічних алгоритмів у сертифікатах SSL/TLS є критично важливими для забезпечення безпечної роботи організації та відповідності стандартам безпеки, таким як PCI DSS.Під час налаштування SSL/TLS необхідно виключити підтримку застарілих протоколів, таких як SSL 3.0, TLS 1.0 та TLS 1.1. Вони мають численні відомі вразливості, які можуть бути використані для атак, наприклад, POODLE або атаки на CBC-моди [22]. Вимоги PCI DSS чітко визначають необхідність відключення таких протоколів для захисту переданих даних. Для забезпечення безпеки слід також відключити застарілі алгоритми шифрування, які використовуються в деяких старих браузерах або сервісах. Використання лише сучасних версій протоколу знижує ризик компрометації даних і відповідає вимогам стандартів.

Після налаштування криптографічних параметрів необхідно провести тестування для перевірки їхньої ефективності. Інструменти, такі як SSL Labs [21], допомагають оцінити конфігурацію SSL/TLS сервера, виявити слабкі місця та надати рекомендації щодо покращення безпеки. Відповідно до PCI DSS, організації зобов’язані регулярно перевіряти свої криптографічні налаштування та виконувати аудит для забезпечення їхньої відповідності стандартам. Ретельне тестування та

аудит дозволяють виявляти потенційні вразливості та оперативно їх усувати, забезпечуючи надійний рівень захисту.

Отже, вибір і налаштування криптографічних параметрів SSL/TLS є ключовим етапом організації безпеки передачі даних у цифровому середовищі. Сертифікати SSL/TLS, видані довіреним центром сертифікації (CA) або внутрішнім CA, підтверджують автентичність сервера і є основою довіри між клієнтом і сервером. Сучасні стандарти, такі як PCI DSS, вимагають регулярного оновлення сертифікатів, використання сучасних алгоритмів (наприклад, AES-256-GCM, ECDHE, SHA-256) та виключення застарілих протоколів, таких як SSL 3.0 і TLS 1.0. Рекомендується використовувати версії TLS 1.2 або TLS 1.3, які забезпечують баланс між сумісністю і безпекою. LibreSSL як сучасна бібліотека підтримує всі необхідні алгоритми і спрощує налаштування протоколу, виключаючи застарілі та небезпечні функції. Регулярний аудит і тестування налаштувань за допомогою інструментів, таких як SSL Labs, допомагають виявляти слабкі місця і підтримувати високий рівень захисту даних. Завдяки правильно налаштованим криптографічним параметрам організації можуть забезпечити конфіденційність, цілісність та відповідність нормативним вимогам.

3.3 Технологія застосування протоколу SSL/TLS

Технологія застосування протоколу SSL/TLS є фундаментальною складовою забезпечення безпеки в сучасному цифровому середовищі. Цей протокол широко використовується для створення захищених каналів комунікації між клієнтами і серверами, гарантуючи конфіденційність, цілісність та автентичність переданих даних. Реалізація SSL/TLS передбачає інтеграцію шифрування, автентифікації та механізмів захисту від перехоплення інформації на всіх етапах передачі. Особливо важливим є застосування цього протоколу у сферах, де обробляються чутливі дані, такі як фінансові транзакції, медичні записи чи корпоративні комунікації. У цьому розділі розглядаються основні аспекти технологічної реалізації SSL/TLS, включаючи налаштування серверів, сертифікацію, вибір алгоритмів та інтеграцію

в сучасні IT-системи. Застосування протоколу дозволяє не лише підвищити безпеку мережевих з’єднань, але й відповідати нормативним стандартам, таким як PCI DSS та GDPR.

Реалізація SSL/TLS в інфраструктурі організації з використанням LibreSSL вимагає виконання кількох ключових етапів. LibreSSL є легкою у використанні бібліотекою, яка забезпечує надійну безпеку та сучасні алгоритми шифрування.

Для початку необхідно встановити LibreSSL на сервер, який буде використовуватися для захищених з'єднань. На Linux-системах можна скористатися менеджером пакетів та нештатними утилітами завантаження (рис. 3.3). Наприклад:

sudo apt update

wget https://ftp.openbsd.org/pub/OpenBSD/LibreSSL/libressl-3.7.2.tar.gz

tar -xvzf libressl-3.7.2.tar.gz

cd libressl-3.7.2

./configure

make

libressl version

Рис. 3.3. Процес встановлення LibreSSL

У разі успішного встановлення можна буде переглянути версію встановленого LibreSSL (рис. 3.4).

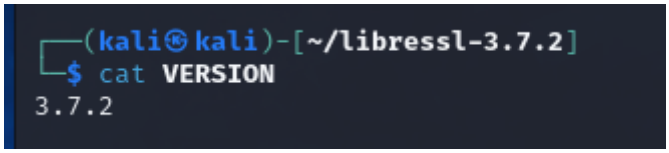

Рис. 3.4. Перегляд версії LibreSSL

Для генерації криптографічних ключів та сертифікатів у LibreSSL використовується утиліта командного рядка, яка забезпечує зручний інтерфейс для роботи з алгоритмами шифрування (рис. 3.5). Генерація приватного ключа є базовим етапом, що включає створення ключа RSA з довжиною 2048 біт, який забезпечує стійкість до атак грубою силою та відповідає сучасним стандартам безпеки. У разі необхідності підвищення продуктивності можна використовувати ключі на основі еліптичних кривих (ECC), що забезпечують подібний рівень безпеки при меншій довжині ключів. Процес генерації ключів у LibreSSL відбувається з урахуванням криптографічних вимог до конфіденційності та цілісності інформації. Наприклад:

openssl genrsa -out private.key 2048

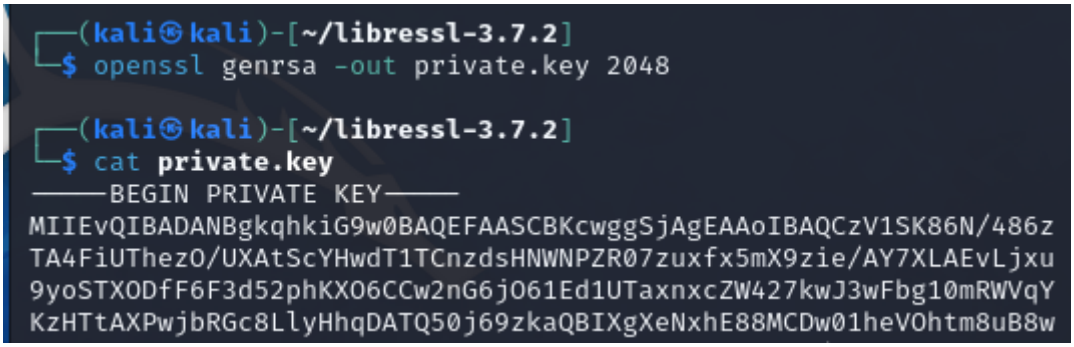

Рис. 3.5. Процес генерації приватного ключа

Генерація запиту на підпис сертифіката (CSR) є важливим етапом процесу створення SSL/TLS сертифіката, що містить інформацію про організацію, доменне ім'я та публічний ключ (рис. 3.6). Цей запит передається до центру сертифікації (CA) для перевірки та підпису, що підтверджує автентичність сервера або системи. CSR генерується з використанням приватного ключа, забезпечуючи унікальність та

безпеку сертифіката. Виконати ці дії можна у середовищі командного рядка за допомогою наступної команди:

openssl req -new -key private.key -out request.csr

При генерації CSR потрібно вказати інформацію про домен, організацію тощо.

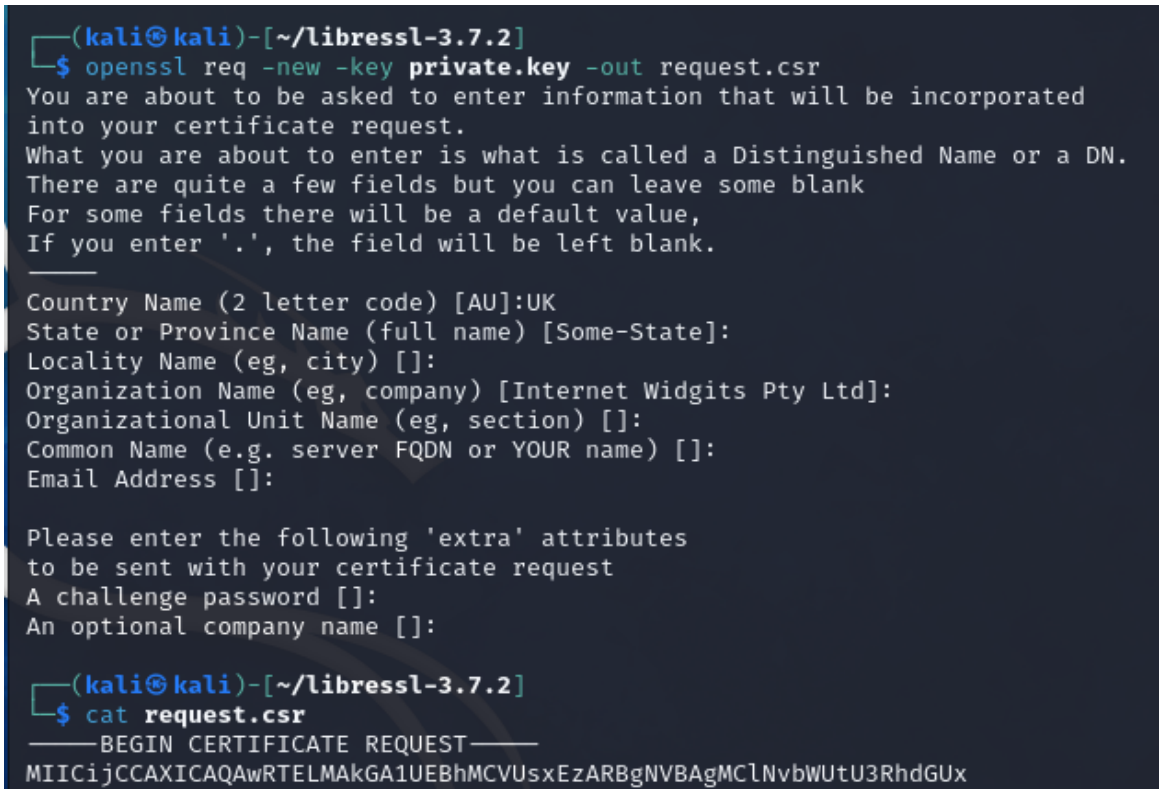

Рис. 3.6. Генерація запиту на підпис сертифіката

CSR передається до центру сертифікації (CA) для виконання перевірки та підпису, що забезпечує видачу дійсного сертифіката. У разі використання внутрішнього центру сертифікації (internal CA) здійснюється самостійне підписання запиту, відповідно до політик безпеки організації. Цей процес гарантує автентичність сертифіката та підтверджує його відповідність заданим вимогам. Усі вищезгадані дії можна виконати у середовищі командного рядку (рис. 3.7), наприклад:

openssl x509 -req -in request.csr -signkey private.key -out certificate.crt -days 365

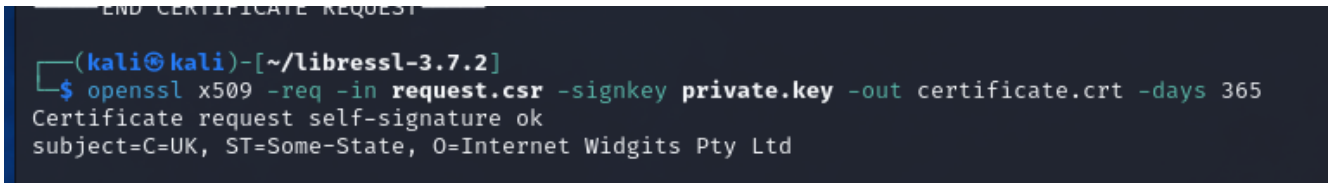

Рис. 3.7. Процес самостійного підпису запиту

Налаштування веб-сервера з використанням LibreSSL передбачає інтеграцію криптографічної бібліотеки як компонента для забезпечення захищених з’єднань. LibreSSL підтримується більшістю сучасних веб-серверів, таких як Nginx або Apache, що дозволяє використовувати його функціонал для шифрування трафіку. Під час налаштування веб-сервера необхідно вказати шлях до сертифікатів SSL/TLS, приватних ключів і параметрів шифрування для забезпечення сумісності з бібліотекою та високого рівня безпеки.

Для прикладу, здійснимо налаштування LibreSSL на Apache. Процес налаштування необхідно почати зі встановлення модуля mod_ssl:

sudo apt install apache2 apache2-utils mod_ssl

У конфігураційному файлі веб-сервера необхідно зазначити шляхи до файлів сертифіката та приватного ключа (рис. 3.8). Це забезпечує сервер можливістю використовувати криптографічні матеріали для встановлення захищених з'єднань. Правильне налаштування цих параметрів є критично важливим для функціонування протоколу SSL/TLS.

sudo nano /etc/apache2/sites-available/default-ssl.conf

Прикладом конфігураційного коду може бути наступний сценарій:

```
<VirtualHost *:443>
    ServerName example.com

    SSLEngine on
    SSLCertificateFile /libressl-3.7.2/certificate.crt
    SSLCertificateKeyFile /libressl-3.7.2/private.key

    SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
```

SSLCipherSuite HIGH:!aNULL:!MD5

</VirtualHost>Перезапустіть Apache:

Після внесення усіх необхідних змін, потрібно підтвердити модифікації та перезапустити сервер, використовуючи наступну команду:

sudo systemctl restart apache2

Для верифікації коректності конфігурації SSL/TLS рекомендовано використовувати утиліту OpenSSL, яка дозволяє здійснити перевірку встановленого захищеного з'єднання (рис. 3.9). Цей процес включає тестування доступності та правильності налаштувань сертифікатів, ключів і шифрувальних параметрів. Приклад реалізації команди у середовищі командного рядка:

openssl s_client -connect example.com:443

Рис. 3.9. Перевірка коректності конфігурації SSL/TLS

Після виконання перевірки буде надано детальну інформацію про використаний сертифікат, протокол шифрування та набір шифрів (Cipher Suite), застосовуваний під час з'єднання. Для більш повної оцінки конфігурації рекомендовано провести тестування сервера за допомогою спеціалізованих інструментів, таких як SSL Labs. Це дозволить переконатися, що налаштування відповідають сучасним вимогам безпеки та стандартам, наприклад PCI DSS. Використання таких засобів також дає можливість виявити потенційні вразливості,

слабкі Cipher Suites або застарілі протоколи. Завдяки цьому забезпечується відповідність найкращим практикам у сфері інформаційної безпеки.

LibreSSL підтримує низку функцій, які значно підвищують рівень безпеки організації при передачі даних. Однією з ключових можливостей є підтримка OCSP Stapling, що дозволяє виконувати перевірку сертифікатів у реальному часі. Завдяки цій технології, клієнт отримує перевірку сертифіката безпосередньо від сервера, що знижує навантаження на центри сертифікації (CA) і скорочує час очікування. Це забезпечує не лише швидкість, але й підвищену надійність з'єднання.

Ще одним важливим елементом є підтримка механізму HSTS (HTTP Strict Transport Security), який примусово забезпечує використання HTTPS. Завдяки налаштуванню HSTS [10], сервер автоматично інформує браузер про необхідність встановлення виключно захищеного з'єднання. Це усуває можливість атаки шляхом зниження рівня шифрування (SSL Stripping [20]) та гарантує, що користувачі завжди взаємодіють із захищеним ресурсом, навіть якщо вони вводять URL без указання HTTPS.

Важливою складовою безпеки протоколу SSL/TLS є впровадження Perfect Forward Secrecy (PFS) за допомогою алгоритмів ECDHE. Ця технологія гарантує, що компрометація довгострокового ключа сервера не вплине на безпеку минулих сесій. Завдяки використанню окремих тимчасових ключів для кожного сеансу шифрування, PFS забезпечує високий рівень захисту даних навіть у випадку складних атак на криптографічні системи.

Реалізація SSL/TLS за допомогою LibreSSL — це ефективний спосіб забезпечення безпеки в організації. Завдяки простоті налаштування, підтримці сучасних алгоритмів і фокусу на безпеці, LibreSSL стає надійним вибором для інтеграції захищених з'єднань.

3.4 Рекомендації щодо застосування технології забезпечення захищеного обміну даними в організації

Протокол SSL/TLS надає потужні механізми для захисту конфіденційної

інформації, забезпечуючи шифрування, автентифікацію і цілісність переданих даних. Однак правильне впровадження технології вимагає дотримання найкращих практик і врахування специфічних потреб кожної організації. Для коректної імплементації протоколу необхідне дотримання певних рекомендацій.

1. Перехід на TLS 1.3

Оновлення до протоколу TLS 1.3 є ключовим етапом підвищення безпеки інформаційної інфраструктури організації. Ця версія протоколу суттєво покращує захист даних, усуваючи низку вразливостей, властивих попереднім версіям (SSL, TLS 1.0, TLS 1.1, та частково TLS 1.2). Зокрема, TLS 1.3 виключає використання застарілих алгоритмів, таких як RC4, та покращує продуктивність завдяки скороченню кількості раундів рукостискання.

Для веб-порталів, мобільних додатків та інтранет-систем важливо забезпечити підтримку TLS 1.3 як основного протоколу. Це вимагає оновлення серверного програмного забезпечення, наприклад, Nginx, Apache чи IIS, до версій, сумісних із TLS 1.3. Крім того, слід перевірити відповідність конфігурацій сучасним стандартам безпеки, зокрема вимогам PCI DSS, які наполягають на використанні протоколів, стійких до сучасних атак.

Окрему увагу слід приділити IoT-пристроям, які часто використовують спрощені або застарілі криптографічні механізми. Для забезпечення сумісності з TLS 1.3 необхідно провести перевірку прошивки таких пристроїв. Якщо пристрої не підтримують нові стандарти, рекомендується оновити їхнє програмне забезпечення або, у разі неможливості такого оновлення, замінити їх на пристрої з підтримкою сучасних алгоритмів шифрування, таких як AES-256-GCM або ECDHE.

TLS 1.3 також спрощує управління криптографічними параметрами, оскільки деякі застарілі функції були вилучені з протоколу, зокрема підтримка статичних ключів RSA. Це знижує ризики неправильної конфігурації, роблячи інтеграцію більш зрозумілою та безпечною.

Застосування TLS 1.3 має забезпечувати не лише захист з’єднань між клієнтом і сервером, але й внутрішньої комунікації між компонентами системи.

Впровадження цього протоколу створює фундамент для захищеної архітектури організації, яка відповідає найкращим практикам сучасної інформаційної безпеки.

2. Управління сертифікатами

Централізоване управління сертифікатами є важливим аспектом забезпечення безпеки в організації, що використовує протокол SSL/TLS. Встановлення внутрішнього сертифікаційного центру (CA) дозволяє організації зменшити залежність від сторонніх провайдерів сертифікатів, знизити витрати на сертифікацію та забезпечити повний контроль над процесами видачі, оновлення та відкликання сертифікатів. Внутрішній CA стає надійною основою для автентифікації серверів, клієнтів і IoT-пристроїв, що взаємодіють у межах корпоративної мережі.

Використання LibreSSL як основного інструменту для генерації ключів і сертифікатів сприяє спрощенню процесів управління сертифікатами. Завдяки зручному функціоналу LibreSSL можна автоматизувати створення ключів, запитів на сертифікацію (CSR) і їх подальшу підписку. Це дозволяє оперативно забезпечувати нові системи необхідними сертифікатами та уникати простоїв, пов'язаних із ручною обробкою запитів.

Ротація сертифікатів є критичним компонентом управління сертифікатами. Відповідно до сучасних стандартів безпеки, зокрема PCI DSS, сертифікати повинні регулярно оновлюватися, щоб мінімізувати ризики їх компрометації. Внутрішній CA дозволяє автоматизувати процес ротації сертифікатів, встановивши чіткі часові рамки їх дії. Наприклад, сертифікати для внутрішніх серверів можуть мати термін дії в 6-12 місяців, після чого їх автоматично перевидають і оновлюють.

Процес відкликання сертифікатів також має бути інтегрованим у систему управління. Використання списків відкликаних сертифікатів (CRL) або протоколу перевірки статусу сертифікатів у реальному часі (OCSP) дозволяє оперативно реагувати на компрометацію ключів або сертифікатів. Це особливо важливо для динамічних середовищ, де швидкість реагування на інциденти є критичним фактором.

Для підвищення прозорості управління сертифікатами доцільно

використовувати системи моніторингу, які дозволяють відслідковувати статус сертифікатів, терміни їх дії та виконувати аудит дій із ключами. У поєднанні з LibreSSL такі системи можуть автоматично генерувати звіти, які забезпечують відповідність внутрішнім і зовнішнім вимогам безпеки.

Завдяки впровадженню централізованого управління сертифікатами організації отримують можливість ефективно захищати свої мережі, забезпечуючи автентифікацію та довіру між усіма компонентами інфраструктури. Це створює основу для стабільної, безпечної роботи систем, зменшуючи ризики, пов’язані з компрометацією сертифікатів або неправильною конфігурацією.

3. Захист API

Захист API є одним із ключових аспектів забезпечення безпеки інтеграцій між системами організації та її партнерами. Реалізація двосторонньої аутентифікації сертифікатів дозволяє гарантувати автентичність обох сторін з’єднання. Цей підхід забезпечує захист від атак типу «людина посередині» (Man-in-the-Middle), оскільки кожна сторона перевіряє дійсність сертифікатів, перш ніж встановити з'єднання.

Доступ до API має бути обмежений виключно для авторизованих партнерів. Це можна реалізувати за допомогою IP-фільтрації, що дозволяє взаємодія лише з конкретних IP-адрес, або впровадженням сучасних механізмів аутентифікації, таких як OAuth 2.0. Ці методи не лише мінімізують ризик несанкціонованого доступу, але й спрощують процес керування доступом до API.

Додатково до механізмів аутентифікації важливо впровадити шифрування всього трафіку, що проходить через API, використовуючи сучасні протоколи, такі як TLS 1.3. Це забезпечує захист даних від перехоплення навіть у разі компрометації мережевих з'єднань. Такий підхід створює багаторівневий захист, що відповідає вимогам сучасної кібербезпеки.

4. Шифрування внутрішнього трафіку

Шифрування внутрішнього трафіку є основою захисту даних в організаційній мережі, особливо у випадках, коли внутрішня інфраструктура піддається зовнішнім загрозам. Використання протоколу TLS для захищених

з’єднань між серверами, базами даних і іншими критично важливими компонентами дозволяє знизити ризик перехоплення або модифікації даних. Це особливо актуально для організацій, які працюють із фінансовими транзакціями, персональними даними або іншою чутливою інформацією.

У з’єднаннях через VPN також варто застосовувати TLS, що додає додатковий рівень захисту для трафіку, який передається через загальнодоступні мережі. Таке шифрування забезпечує конфіденційність даних, навіть якщо внутрішня мережа організації буде частково скомпрометована. Налаштування TLS для внутрішнього трафіку повинно враховувати вибір сучасних алгоритмів шифрування, таких як AES-256-GCM, а також забезпечувати періодичне оновлення ключів шифрування.

Окрім шифрування, варто впровадити стиснення даних на транспортному рівні, наприклад, за допомогою алгоритмів GZIP або Brotli. Це дозволяє значно знизити обсяги переданих даних, зменшити навантаження на мережеву інфраструктуру та підвищити загальну продуктивність. Такий підхід є особливо важливим для середовищ із великим обсягом внутрішнього трафіку, де ефективність використання мережевих ресурсів відіграє критичну роль.

Для забезпечення комплексного захисту шифрування внутрішнього трафіку слід поєднувати з іншими засобами безпеки, такими як автентифікація з використанням сертифікатів SSL/TLS та моніторинг активності мережі. Це дозволяє не лише захистити дані від потенційних атак, але й своєчасно виявляти та реагувати на підозрілі дії в межах внутрішньої інфраструктури.

5. Модернізація IoT-пристроїв

IoT-пристрої відіграють важливу роль у сучасних організаціях, але їх застарілі моделі можуть стати джерелом вразливостей через відсутність підтримки сучасних криптографічних алгоритмів. Тому необхідно проводити регулярну оцінку безпеки таких пристроїв і замінювати їх на моделі, які відповідають сучасним стандартам захисту даних. Це забезпечить мінімізацію ризиків, пов’язаних із перехопленням або компрометацією інформації, переданої через ці пристрої.

Сучасні IoT-пристрої повинні підтримувати алгоритми шифрування AES-256-GCM, які забезпечують надійний захист даних, а також механізми обміну ключами на основі еліптичних кривих (ECDHE), що сприяють збереженню конфіденційності навіть у разі компрометації довготривалих ключів. Крім того, слід налаштовувати використання сертифікатів SSL/TLS для автентифікації пристроїв і перевіряти їх на сумісність із протоколом TLS 1.3, що гарантує найвищий рівень захисту для IoT-інфраструктури.

6. Моніторинг і аудит

Ефективний моніторинг конфігурацій LibreSSL є критично важливим для підтримання безпеки системи. Використання інструментів моніторингу, таких як SIEM (системи управління подіями безпеки), дозволяє своєчасно виявляти невідповідності або потенційні вразливості в налаштуваннях криптографічних параметрів. Такі інструменти здатні надавати звіти про стан сертифікатів, активні протоколи та Cipher Suites, що сприяє проактивному підходу до захисту системи.

Проведення регулярного внутрішнього аудиту є ключовим компонентом управління безпекою. Щонайменше раз на 6 місяців необхідно перевіряти відповідність криптографічних параметрів сучасним стандартам, таким як PCI DSS. Аудит повинен включати оцінку використаних сертифікатів, протоколів і алгоритмів, а також тестування на можливість відомих атак, наприклад, "людина посередині" (Man-in-the-Middle). Це дозволяє вчасно адаптувати захисні механізми до змін у динамічному середовищі загроз.

Ці рекомендації розроблені для інтеграції протоколу SSL/TLS у мережеву інфраструктуру організації з урахуванням сучасних вимог безпеки. Їх реалізація дозволить мінімізувати ризики витоку даних, покращити продуктивність системи та забезпечити відповідність нормативним стандартам.

ВИСНОВКИ

У роботі проведено дослідження проблеми забезпечення захищеного обміну даними в організації із використанням протоколу SSL/TLS, визначено його призначення, основні функції та роль у сучасних умовах кіберзагроз.

Проведено детальний аналіз існуючих рішень для реалізації SSL/TLS, таких як LibreSSL, BoringSSL та WolfSSL, з акцентом на їх можливості забезпечення безпеки даних. LibreSSL було обрано як базове рішення завдяки його сучасним криптографічним алгоритмам, фокусуванню на усуненні застарілих компонентів, зручності налаштування та відповідності галузевим стандартам безпеки, зокрема PCI DSS. Крім того, його використання дозволяє значно спростити процес інтеграції захищених з'єднань у мережеву інфраструктуру організації.

Досліджено архітектуру впровадження протоколу SSL/TLS в умовах організації, що працює з чутливими даними, включаючи веб-портали, мобільні додатки, API та IoT-пристрої. Розглянуто специфічні потреби кожного елемента інфраструктури, що дозволило визначити оптимальні місця інтеграції SSL/TLS. Зокрема, особливу увагу приділено забезпеченню безпеки внутрішнього та зовнішнього трафіку, таких як з’єднання між додатками, серверами та базами даних. Це гарантує, що дані захищені як на рівні клієнтських запитів, так і в рамках внутрішніх процесів обробки інформації.

Розглянуто та проаналізовано рекомендації щодо вибору і налаштування криптографічних параметрів, таких як використання шифрування AES-256-GCM, алгоритмів обміну ключами ECDHE та хеш-функцій SHA-256. Також проведено аналіз впливу цих параметрів на продуктивність системи та загальний рівень безпеки. Важливим аспектом є забезпечення балансу між високим рівнем криптографічного захисту та підтримкою сумісності із сучасними пристроями й програмним забезпеченням.

На основі проведених досліджень запропоновано практичні рекомендації щодо впровадження технології SSL/TLS. Серед них оновлення серверів до версії

TLS 1.3, створення централізованого сертифікаційного центру (CA) для внутрішніх потреб, а також реалізація двосторонньої аутентифікації сертифікатів для захисту API. Особлива увага приділена модернізації IoT-пристроїв, оскільки вони можуть стати потенційними точками вразливості у мережі, якщо не відповідають сучасним стандартам криптографії.

Розроблено комплексний порядок застосування SSL/TLS в організації, що включає оцінку інформаційної інфраструктури, вибір сучасних криптографічних параметрів, інтеграцію протоколу в мережу, а також моніторинг і регулярний аудит для забезпечення відповідності стандартам безпеки. Такий підхід дозволяє не лише підвищити рівень захисту даних, але й мінімізувати ризики несанкціонованого доступу до корпоративних ресурсів.

Таким чином, реалізація запропонованих рекомендацій сприятиме створенню надійного середовища для обміну даними, забезпечить відповідність сучасним нормативним вимогам і підвищить рівень довіри до системи з боку клієнтів та партнерів. Використання SSL/TLS як основи для захисту комунікацій дозволяє організації ефективно протистояти викликам у сфері інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. 17 data breach statistics to know in 2024 | truelist. TrueList. URL: https://truelist.co/blog/data-breach-statistics/ (дата звернення: 24.11.2024).

2. 18 top SSL statistics which shows why website security matters. ClickSSL. URL: https://www.clickssl.net/blog/ssl-statistics (дата звернення: 24.11.2024).

3. About – embedded SSL/TLS library. wolfSSL. URL: https://www.wolfssl.com/about/ (дата звернення: 24.11.2024).

4. A complete overview of SSL/TLS and its cryptographic system. DEV Community. URL: https://dev.to/techschoolguru/a-complete-overview-of-ssl-tls-and-its-cryptographic-system-36pd (дата звернення: 24.11.2024).

5. Bansal P. Securing your website with SSL/TLS: a comprehensive guide. Medium. URL: https://medium.com/@prateekbansalind/securing-your-website-with-ssl-tls-a-comprehensive-guide-eea0fee6eb28 (дата звернення: 24.11.2024).

6. BoringSSL. boringssl Git repositories - Git at Google. URL: https://boringssl.googlesource.com/boringssl/+/HEAD/README.md#:~:text=BoringSSL%20is%20a%20fork%20of,of%20API%20or%20ABI%20stability. (дата звернення: 24.11.2024).

7. Cipher suites in TLS/SSL (schannel SSP) - win32 apps. Microsoft Learn. URL: https://learn.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel (дата звернення: 24.11.2024).

8. Cobb M., Loshin P. What is a secure sockets layer (SSL)? Definition from techtarget. Search Security. URL: https://www.techtarget.com/searchsecurity/definition/Secure-Sockets-Layer-SSL (дата звернення: 24.11.2024).

9. Cost of a data breach 2024. IBM. URL: https://www.ibm.com/reports/data-breach (дата звернення: 24.11.2024).

10. Dolnak I., Litvik J. Introduction to HTTP security headers and implementation of HTTP strict transport security (HSTS) header for HTTPS enforcing. 2017 15th international conference on emerging elearning technologies and applications (ICETA),

м. Stary Smokovec, 26–27 жовт. 2017 р. 2017. URL: https://doi.org/10.1109/iceta.2017.8102478 (дата звернення: 24.11.2024).

11. Guo L., Lee J. Y. B. TCP-FLASH - A fast reacting TCP for modern networks. IEEE access. 2021. Т. 9. С. 68861–68879. URL: https://doi.org/10.1109/access.2021.3077612 (дата звернення: 24.11.2024).

12. LibreSSL 4.0.0 released. LWN.net. URL: https://lwn.net/Articles/994320/ (дата звернення: 24.11.2024).

13. LibreSSL. Gentoo Wiki. URL: https://wiki.gentoo.org/wiki/LibreSSL (дата звернення: 24.11.2024).

14. Lynch V. SSL/TLS certificates – their architecture, process & interactions. URL: https://www.thesslstore.com/blog/ssltls-certificate-its-architecture-process-interactions/ (дата звернення: 24.11.2024).

15. Morrissey P., Smart N. P., Warinschi B. The TLS handshake protocol: a modular analysis. Journal of cryptology. 2009. Т. 23, № 2. С. 187–223. URL: https://doi.org/10.1007/s00145-009-9052-3 (дата звернення: 24.11.2024).

16. Official PCI security standards council site. compliance, download data security and credit card security standards. URL: https://east.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (дата звернення: 24.11.2024).

17. Prashar N., Hooda S., Kumar R. Current status of challenges in data security: a review. Lecture notes in electrical engineering. Singapore, 2023. С. 3–13. URL: https://doi.org/10.1007/978-981-99-5080-5_1 (дата звернення: 24.11.2024).

18. Satapathy A., Livingston J. A comprehensive survey on SSL/ TLS and their vulnerabilities. International journal of computer applications. 2016. Т. 153, № 5. С. 31–38. URL: https://doi.org/10.5120/ijca2016912063 (дата звернення: 24.11.2024).

19. SSL and TLS deployment best practices. GitHub. URL: https://github.com/ssllabs/research/wiki/ssl-and-tls-deployment-best-practices (дата звернення: 24.11.2024).

20. SSL stripping technique (DHCP snooping and ARP spoofing inspection) / H. A. S. Adjei та ін. 2021 23rd international conference on advanced communication

technology (ICACT), м. PyeongChang, Korea (South), 7–10 лют. 2021 р. 2021. URL: https://doi.org/10.23919/icact51234.2021.9370460 (дата звернення: 24.11.2024).

21. SSL server test (powered by qualys SSL labs). Qualys SSL Labs. URL: https://www.ssllabs.com/ssltest/ (дата звернення: 24.11.2024).

22. SSL 3.0 protocol vulnerability and POODLE attack. Cybersecurity and Infrastructure Security Agency CISA. URL: https://www.cisa.gov/news-events/alerts/2014/10/17/ssl-30-protocol-vulnerability-and-poodle-attack (дата звернення: 24.11.2024).

23. Managing TLS and trusted CA certificates. Pexip Infinity Docs. URL: https://docs.pexip.com/admin/certificate_management.htm (дата звернення: 24.11.2024).

24. Top 5 methods of protecting data. TitanFile. URL: https://www.titanfile.com/blog/5-methods-of-protecting-data/ (дата звернення: 24.11.2024).

25. What is an SSL/TLS certificate?. SSL.com. URL: https://www.ssl.com/article/what-is-an-ssl-tls-certificate/ (дата звернення: 24.11.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ