ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «**ПОБУДОВА СИСТЕМ БЕЗПЕКИ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ НА ОСНОВІ СУЧАСНИХ МЕТОДІВ ШИФРУВАННЯ**»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

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

_____ Артем ФІЛІППОВ
(*підпис*)

Виконав: Здобувач вищої освіти гр.ТСДМ-63

Артем ФІЛІППОВ

Керівник: Михайло МАЛЮЖЕНКО
ктн, доцент

Рецензент:

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

Кафедра Телекомунікаційних систем та мереж
Ступінь вищої освіти Магістр
Спеціальність 172 Електронні комунікації та радіотехніка
Освітньо-професійна програма Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Телекомунікаційних систем та мереж
_____Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Філіппову Артему Олексійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: **:** «Побудова систем безпеки в телекомунікаційних мережах на основі сучасних методів шифрування»
керівник кваліфікаційної роботи Михайло МАЛЮЖЕНКО, КТН, доцент
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «__» _____ 2025 р. № ___.

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.
3. Вихідні дані до кваліфікаційної роботи:
   1. Принцип роботи інтернет мережі
   2. Переваги та перспективи технології шифрування
   3. Основні типи кіберзагроз
   5. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

   1. Аналіз перспектив та особливостей застосування сучасних методів шифрування;
   2. Дослідження сучасних типів кіберзагроз;
   3. Дослідження сучасних методів шифрування;
   4. Реалізація захищеної мережі на основі протоколу SSL;

5. Перелік ілюстративного матеріалу: (Слайди на *Презентації)*
6. Дата видачі завдання «___» _____ 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	11.10.2025	Викон.
2.	Аналіз сучасних рішень забезпечення безпеки в телекомунікаційних мережах	22.10.2025	Викон.
3.	Аналіз існуючих типів кіберзагроз	31.10.2025	Викон.
4.	Дослідження сучасних методів шифрування та шляхи їх реалізації	11.11.2025	Викон.
5.	Висновки, вступ, реферат	25.11.2025	Викон.
6.	Розробка презентації	15.12.2025	Викон.

Здобувач вищої освіти Артем ФІЛІППОВ

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи Михайло МАЛЮЖЕНКО

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій
ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Філіппов А.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Побудова систем безпеки в телекомунікаційних мережах на основі сучасних методів шифрування».

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав Кравченко
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Філіпов Артем Олексійович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до наукової роботи.
Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Філіпова Артема Олексійовича на оцінку «**добре**» та присвоїти йому кваліфікацію Магістр з електронних комунікацій та радіотехніки.

Керівник роботи Михайло МАЛЮЖЕНКО
(підпис) *(Ім'я,ПРІЗВИЩЕ)*

«____» _____ 2025року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Філіппов А.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Телекомунікаційних систем та мереж Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я,ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Філіппова Артема Олексійовича

(прізвище, ім'я, по батькові)

на тему « Побудова систем безпеки в телекомунікаційних мережах н основі сучасних методів шифрування»

Актуальність: В системах безпеки телекомунікацій ключову роль відігра шифрування. Цей метод забезпечує конфіденційність даних, роблячи і читабельними лише для власників прав на доступ. Процес створення т впровадження систем безпеки у телекомунікаційних мережах передбача цілісний підхід. Це включає в себе аудит існуючих систем, вибір оптимальни методів шифрування, встановлення інтегрованих систем моніторингу т постійне оновлення технологічної бази для забезпечення захисту від нови загроз. Таким чином існує багато підходів забезпечення безпеки на осно шифрування, що робить вибрану тему актуальною.

Позитивні сторони : У роботі розглянуті різни типи сучасни кіберзагроз. Наведені приклади забезпечення безпеки різними способам Розглянуті сучасні методи шифрування. Виконано порівняння різни алгоритмів шифрування та розраховано їх ефективність. Наведені приклад створення мережі з впровадженням систем безпеки на основі сучасних метод шифрування.

Недоліки:

1.Слід було більше уваги приділити різним алгоритмам шифрування

2. Недостатньо розглянуті сучасні методи шифрування

Відзначені зауваження не впливають на загальну позитивну оцінк магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна магістерська робота заслуговує оцінку "***добре** *а здобувач* Філіпов Артем Олексійович *заслуговує присвоєння кваліфікаці* Магістр з електронних комунікацій та радіотехніки.

Рецензент: _____ _____

науковий ступінь, вчене звання

Підпис *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: ___ стор., ___ рис., ___ табл., ___ джерел

Мета роботи – визначення та дослідження основних типів кіберзагроз та методика та методика створення систем безпеки в телекомунікаційних мережах.

Об'єкт дослідження – системи безпеки в телекомунікаційних мережах.

Предмет дослідження – сучасні методи шифрування та їх впровадження.

У роботі виконувався розгляд сучасних типів кіберзагроз, технологій та методів забезпечення безпеки в телекомунікаційних мережах, а також їх порівняння.

Було розглянуто основні типи шифрування, а також технології які їх використовують. Наведені приклади побудови мережі з урахуванням безпеки та шифруванням даних.

КЛЮЧОВІ СЛОВА:

АРХІТЕКТУРА, СТАНДАРТИ ТЕХНОЛОГІЇ, IP, TLS, SSL, RSA, DSA ЗАХИСТ ІНФОРМАЦІЇ, ПОБУДОВА МЕРЕЖ.

ABSTRACT

The text part of the qualification work: ___ pages, ____ figures, ____ tables, ___sources.

The purpose of the work is to identify and study the main types of cyber threats and methods and techniques for creating security systems in telecommunication networks.

The object of research is security systems in telecommunication networks.

The subject of research is modern encryption methods and their implementation.

The paper considered modern types of cyber threats, technologies and methods of ensuring security in telecommunication networks, as well as their comparison.

The main types of encryption, as well as the technologies that use them, were considered. Examples of building a network with security and data encryption in mind are given.

KEYWORDS:

ARCHITECTURE, TECHNOLOGY STANDARDS, IP, TLS, SSL, RSA, DSA INFORMATION PROTECTION, NETWORK CONSTRUCTION.

ЗМІСТ

ВСТУП 10
1. АНАЛІЗ СУЧАСНИХ РІШЕНЬ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ 12
1.1. Типи кіберзагроз та їх вплив на телекомунікаційні мережі 12
1.1.1. Атаки на основі шкідливих програм 12
1.1.2. Фішингові атаки 15
1.1.3. Атака "людина посередині" 16
1.1.4. Атаки SQL ін'єкції 19
1.1.5. Тунелювання DNS 21
1.1.6. Міжсайтові скриптові атаки 23
1.1.7. Уразливість нульового дня 24
1.2. Сучасні технології забезпечення безпеки 26
1.2.1. Аналіз систем виявлення вторгнень 26
1.2.2. Система запобігання вторгненням 28
1.2.3. Фізична безпека 31
1.3. Визначення вразливостей в мережевій інфраструктурі 34
2. ОРГАНІЗАЦІЯ ЗАХИСТУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗА ДОПОМОГОЮ СУЧАСНИХ МЕТОДІВ ШИФРУВАННЯ 40
2.1. Огляд сучасних методів шифрування 40
2.1.1. Симетричні алгоритми шифрування 43
2.1.2. Асиметричні алгоритми шифрування 47
2.1.3. Порівняння різних типів шифрування 51
2.1.4. Розрахунок швидкості роботи симетричного та асиметричного алгоритмів шифрування 52
2.2. Розробка стратегії шифрування 53
2.2.1. Забезпечення безпеки при передачі даних через інтернет за допомогою протоколу TLS/SSL 53
2.2.2. Наскрізне шифрування 56
2.2.3. Шифрування кінцевого вузла 60

3. ПОБУДОВА МЕРЕЖІ З ВИКОРИСТАННЯМ СУЧАСНИХ МЕТОДІВ ШИФРУВАННЯ 61
3.1. Огляд доступних рішень для впровадження TLS/SSL 61
3.2. Впровадження шифрування на основі протоколу SSL/TLS на базі AWS (Amazon Web Services) 63
3.3. Впровадження шифрування на основі протоколу SSL/TLS на базі Google Cloud 67
ВИСНОВКИ 76
ПЕРЕЛІК ПОСИЛАНЬ 77
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 78

ВСТУП

Актуальність дослідження. У сучасному інформаційному суспільстві, де телекомунікаційні мережі стали невід'ємною частиною нашого повсякденного життя, питання забезпечення безпеки цих мереж виявляється крайньою актуальністю. З кожним днем обсяги передачі даних у мережах та їх важливість для функціонування суспільства зростають, а це робить сучасні телекомунікаційні системи метою для різноманітних кіберзагроз. За таких обставин, розробка та впровадження ефективних систем безпеки в телекомунікаційних мережах стає необхідністю. Одним із ключових елементів таких систем є сучасні методи шифрування, які вирішують завдання надійного захисту конфіденційності, цілісності та доступності переданих даних. Зростання обсягів та складності передачі даних у телекомунікаційних мережах супроводжується інтенсивними атаками на ці мережі. Кіберзлочинці активно використовують різноманітні техніки, спрямовані на отримання несанкціонованого доступу, перехоплення конфіденційної інформації та порушення цілісності даних. З цього приводу, розробка імунітету до сучасних кіберзагроз стає вирішальною задачею для забезпечення стабільності та безпеки телекомунікаційного середовища.

В системах безпеки телекомунікацій ключову роль відіграє шифрування. Цей метод забезпечує конфіденційність даних, роблячи їх читабельними лише для власників прав на доступ. Процес створення та впровадження систем безпеки у телекомунікаційних мережах передбачає цілісний підхід. Це включає в себе аудит існуючих систем, вибір оптимальних методів шифрування, встановлення інтегрованих систем моніторингу та постійне оновлення технологічної бази для забезпечення захисту від нових загроз. Таким чином існує багато підходів забезпечення безпеки на основі шифрування, що робить вибрану тему актуальною.

У роботі розглянуто методику створення та впровадження систем безпеки в телекомунікаційних мережах, зосереджуючись на сучасних підходах до шифрування. Розглядання цієї теми дозволить визначити оптимальні рішення для

захисту важливих даних у телекомунікаційних системах та вдосконалити їхню стійкість до сучасних кіберзагроз.

У результаті дослідження різних типів кібератак на телекомунікаційні системи було досліджено основні методи забезпечення безпеки в телекомунікаційних мережах, а також застосування протоколів SSL/TLS для шифрування даних на основі різних провайдерів хмарних обчислень, це допоможе підвищити рівень безпеки при передачі та зберіганні даних через мережу інтернет.

1. АНАЛІЗ СУЧАСНИХ РІШЕНЬ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

1.1. Типи кіберзагроз та їх вплив на телекомунікаційні мережі

1.1.1. Атаки на основі шкідливих програм

Атаки на основі зловмисного програмного забезпечення – це шкідливі програми, призначені для зараження та використання вразливостей у комп’ютерних системах, мережах і програмах. Ці атаки можуть приймати різні форми, включаючи віруси, трояни, шпигунське програмне забезпечення, рекламне програмне забезпечення та програми-вимагачі. Ці атаки спрямовані на отримання несанкціонованого доступу до конфіденційних даних, таких як паролі, фінансова інформація, захищена інформація про стан здоров’я та особиста інформація. У деяких випадках атаки на основі зловмисного програмного забезпечення використовуються для викрадення даних з метою викрадення особистих даних або порушення нормального функціонування комп’ютерної системи.



Рис 1.1 Шкідливі програми

Вірус — це зловмисне програмне забезпечення, яке заражає комп'ютерну систему та поширюється на інші системи через вкладення електронної пошти, завантаження або мережеві з'єднання. Якщо комп'ютер заражений вірусом, це може спричинити багато проблем, від уповільнення роботи систем, додатків, інтерфейсів прикладного програмування і баз даних до фактичного знищення даних. Коли вірус проникає в мережу, програму або базу даних, наслідки можуть бути жахливими. Продуктивність системи може зменшитись, що унеможливить виконання навіть основних завдань. У деяких випадках вірус може повністю вивести з ладу програми, мережі та бази даних. Крім того, критично важливі дані можуть бути знищені або пошкоджені, що призведе до незлічуваних втрат як для окремих осіб, так і для компаній.

Троян — це тип зловмисного програмного забезпечення, яке маскується під законну програму або файл. Під час запуску троян відкриває з'єднання у мережі, програмі, пристрої або базі даних, дозволяючи зловмисникам отримати несанкціонований доступ до особистих даних.

Наслідки зараження трояном є важкими. Вплив трояна може бути катастрофічним: від крадіжки ідентифікаційної інформації та даних до знищення критичних системних файлів. У деяких випадках трояни використовувалися для атак програм-вимагачів, утримуючи дані користувачів у заручниках, доки не буде сплачено викуп. Потенційна втрата даних або фінансовий збиток від зараження трояном вражає.

Шпигунське програмне забезпечення — це зловмисне програмне забезпечення, призначене для збору інформації про дії користувача комп'ютера в Інтернеті. Ця інформація може включати паролі, фінансову інформацію та інші конфіденційні дані. Підступна природа шпигунського програмного забезпечення робить його небезпечною загрозою. Це зловмисне програмне забезпечення може проникнути в систему через різні канали, включаючи вкладення електронної пошти, атаки соціальної інженерії та скомпрометоване програмне забезпечення. Після встановлення шпигунське програмне забезпечення може працювати непоміченим, відстежувати дії користувача та надсилати ці дані зловмисникам.

Рекламне програмне забезпечення – це шкідливе програмне забезпечення, яке відображає небажану рекламу в комп'ютерній системі. Це зловмисне програмне забезпечення може сповільнювати роботу комп'ютерної системи та порушувати конфіденційність, відстежуючи дії користувачів в Інтернеті. Підступна природа рекламного програмного забезпечення робить його особливо неприємною та руйнівною загрозою. Після встановлення рекламне ПЗ може перервати робочий процес користувача, уповільнити його комп'ютер і спричинити збої. Це зловмисне програмне забезпечення може проникнути в систему через різні канали, включаючи вкладення електронної пошти, атаки соціальної інженерії та скомпрометоване програмне забезпечення. Рекламне програмне забезпечення іноді використовувалося для відстеження активності користувачів і збору персональних даних для продажу третім особам. Наслідки зараження рекламним ПЗ можуть бути серйозними. Постійний шквал небажаної реклами може не тільки дратувати, але й виснажувати системні ресурси.

Програмне забезпечення-вимагач шифрує дані користувача комп'ютера, роблячи їх недоступними. Потім зловмисники вимагають викуп в обмін на ключ дешифрування. Програмне забезпечення-вимагач є небезпечною загрозою, оскільки воно може швидко поширюватися різними каналами, такими як вкладення електронної пошти, атаки соціальної інженерії та скомпрометоване програмне забезпечення. Після встановлення це зловмисне програмне забезпечення може шифрувати файли та блокувати користувачів у їхніх системах, завдаючи значної шкоди та збоїв. Наслідки атаки програм-вимагачів можуть бути серйозними: зловмисники часто вимагають значну плату викупу в криптовалюті, щоб уникнути виявлення. Навіть якщо викуп буде сплачено, немає ніякої гарантії, що ключ розшифровки спрацює, тому жертви не матимуть прав на захист. У деяких випадках зловмисники навіть заходили так далеко, що викрадали та витоку конфіденційних даних, щоб вимагати від жертви ще більше. Постійна загроза атак програм-вимагачів підкреслює необхідність постійної пильності у сфері кібербезпеки, оскільки наслідки атаки можуть бути руйнівними, завдаючи жертвам значних збитків і практично не маючи права на захист.

1.1.2. Фішингові атаки

Основним елементом фішингової атаки є повідомлення, надіслане електронною поштою, соціальними мережами чи іншими засобами електронного зв’язку. Фішер може використовувати загальнодоступні ресурси, особливо соціальні мережі, для збору довідкової інформації про особистий і робочий досвід своєї жертви. Ці джерела використовуються для збору такої інформації, як ім’я потенційної жертви, посада та адреса електронної пошти, а також інтереси та діяльність. Потім фішер може використати цю інформацію для створення надійного підробленого повідомлення. Як правило, електронні листи, які отримує жертва, надходять від відомого контакту чи організації. Атаки здійснюються через шкідливі вкладення або посилання на шкідливі веб-сайти. Зловмисники часто створюють фальшиві веб-сайти, які, здається, належать довіреній організації, як-от банк, робоче місце чи університет жертви. Через ці веб-сайти зловмисники намагаються зібрати особисту інформацію, як-от імена користувачів і паролі або платіжну інформацію. Деякі фішингові електронні листи можна розпізнати через поганий копірайтинг і неправильне використання шрифтів, логотипів і макетів. Однак багато кіберзлочинців стають все більш досвідченими у створенні автентичних повідомлень і використовують професійні маркетингові методи для перевірки та підвищення ефективності своїх електронних листів.

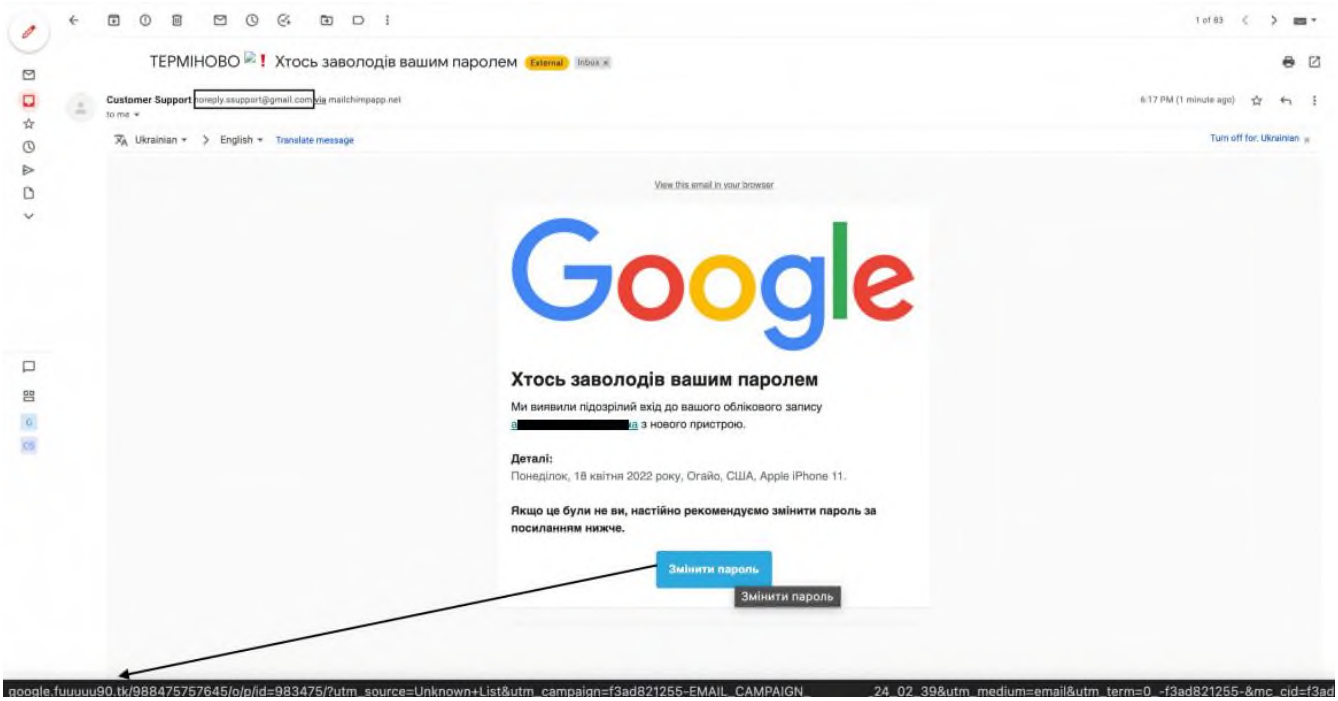


Рис 1.2 Приклад фішингової атаки

Більшість фішингових атак надсилаються електронною поштою. Зловмисники зазвичай реєструють підроблені доменні імена, які імітують справжні організації, і надсилають жертвам тисячі типових запитів.

Для підроблених доменів зловмисники можуть додавати або змінювати символи (наприклад, my-bank.com замість mybank.com), використовувати субдомени (наприклад, mybank.host.com) або використовувати назву надійної організації як ім’я користувача електронної пошти (наприклад, mybank@host.com).

Багато фішингових електронних листів використовують відчуття терміновості або загрози, щоб змусити користувача швидко виконати вимоги, не перевіряючи джерело чи автентичність електронного листа.

1.1.3. Атака "людина посередині"

Атаки «людина посередині» (MITM) — це поширений тип атак на кібербезпеку, які дозволяють зловмисникам прослуховувати спілкування між двома цілями. Атака відбувається між двома хостами, які легально спілкуються, дозволяючи зловмиснику «прослухати» розмову, яку він зазвичай не має можливості прослухати, звідси й назва «людина посередині».

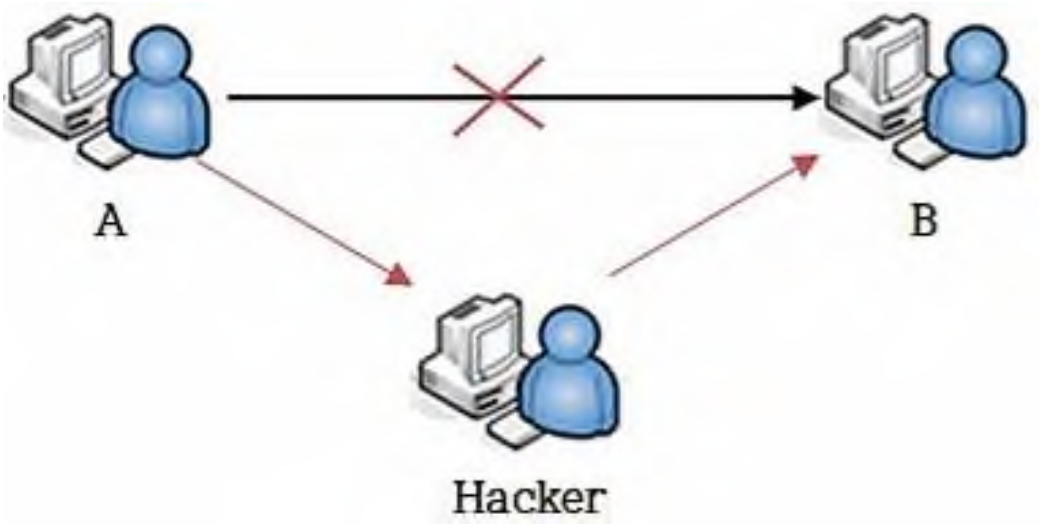


Рис 1.3 Атака “Людина посередині”

Ось аналогія: Аліса та Боб розмовляють. Єва хоче підслуховувати розмову, але також залишатися прозорою. Єва могла сказати Алісі, що вона Боб, і сказати Бобу, що вона Аліса. Це змусить Алісу повірити, що вона розмовляє з Бобом, а насправді розкриє свою частину розмови Єві. Тоді Єва могла б зібрати з цього інформацію, змінити відповідь і передати повідомлення Бобу (який думає, що розмовляє з Алісою). У результаті Єва може прозоро захопити їхню розмову.

Атаки MITM можуть приймати різні форми, але наведено деякі з найпоширеніших:

- IP-спуфінг. Кожен пристрій, який підключається до Інтернету, робить це через IP-адресу, яка є номером, призначеним вашому пристрою на основі вашого фізичного розташування. Підробивши IP-адресу, злочинні хакери можуть обманом змусити вас повірити, що ви взаємодієте з веб-сайтом або особою, з якою ви намагалися зв’язатися.

- ARP (Address Resolution Protocol) — це процес, який дозволяє мережевим зв’язкам досягати певного пристрою в мережі. Він робить це шляхом перекладу IP-адреси на MAC-адресу (Media Access Control) і навпаки. Зловмисники можуть маніпулювати цим процесом, пов’язуючи свою MAC-адресу з IP-адресою цілі за допомогою підроблених повідомлень ARP. У

результаті будь-які дані, надіслані користувачем на IP-адресу хоста, замість цього спрямовуються до зловмисника.

- Підробка DNS. Цей метод атаки, також відомий як отруєння кешу DNS, використовує модифіковані записи DNS (сервера доменних імен) для надсилання трафіку на шахрайський веб-сайт. Ці веб-сайти зазвичай нагадують справжній сайт, тобто відвідувачі навряд чи помітять невірну адресу. Потім сайт просить їх надати дані для входу, надаючи зловмиснику можливість отримати їхні облікові дані доступу.

- Підробка HTTPS. Загальне емпіричне правило, щоб дізнатися, чи веб-сайт є справжнім, полягає в тому, що він має зелений символ замка поруч із ним і починається з «https://», а не просто «http://». Додаткова «s» означає «захищений», вказуючи на те, що з'єднання між вами та сервером було зашифровано і тому його не можна зламати. На жаль, зловмисники знайшли спосіб обійти це. Вони створюють власний веб-сайт, який виглядає ідентично тому, на який ви намагаєтеся зайти, але з дещо іншою URL-адресою. Наприклад, мала буква «l» може стати великою буквою «I», або домен використовуватиме літери кириличного алфавіту. Коли жертви намагаються перейти на законний сайт, зловмисник перенаправляє їх на власний сайт, звідки вони можуть перекачувати інформацію. Зловмисники зазвичай роблять це, щоб викрасти облікові дані електронної пошти та веб-сайтів, які вони можуть використовувати для цілеспрямованих атак, як-от фішингових електронних листів. Але якщо зловмиснику пощастить, жертва мимоволі відвідає портал онлайн-банку та передасть інформацію про свій рахунок.
- Викрадення електронної пошти. Кіберзлочинці часто націлюються на електронні листи між банками та клієнтами з наміром підробити електронну адресу банку та надіслати власні інструкції. Це хитрість, щоб змусити жертву надати свої облікові дані та дані платіжної картки.

1.1.4. Атаки SQL ін'єкції

SQL ін’єкція — це тип ін’єкційної атаки, яка дає змогу виконувати зловмисні оператори SQL. Ці оператори керують сервером бази даних за веб-програмою. Зловмисники можуть використовувати вразливості SQL Injection, щоб обійти заходи безпеки програми. Вони можуть обійти автентифікацію та авторизацію веб-сторінки або веб-додатку та отримати вміст всієї бази даних SQL. Вони також можуть використовувати SQL ін’єкцію для додавання, зміни та видалення записів у базі даних. Вразливість SQL ін’єкції може вплинути на будь-який веб-сайт або веб-програму, яка використовує базу даних SQL, таку як MySQL, Oracle, SQL Server або інші. Злочинці можуть використовувати його для отримання несанкціонованого доступу до ваших конфіденційних даних: інформації про клієнтів, особистих даних, комерційної таємниці, інтелектуальної власності тощо. Атаки впровадження SQL є однією з найстаріших, найпоширеніших і найнебезпечніших вразливостей веб-додатків. Організація OWASP (Open Web Application Security Project) перераховує ін’єкції у своєму як загрозу номер один для безпеки веб-додатків.

Щоб здійснити атаку SQL ін’єкція, зловмисник повинен спочатку знайти вразливі дані користувача на веб-сторінці чи веб-додатку. Веб-сторінка або веб-додаток, які мають вразливість SQL Injection, використовують такі дані користувача безпосередньо в SQL-запиті. Зловмисник може створити вхідний вміст. Такий вміст часто називають шкідливим корисним навантаженням і є ключовою частиною атаки. Після того, як зловмисник надсилає цей вміст, у базі даних виконуються зловмисні команди SQL.

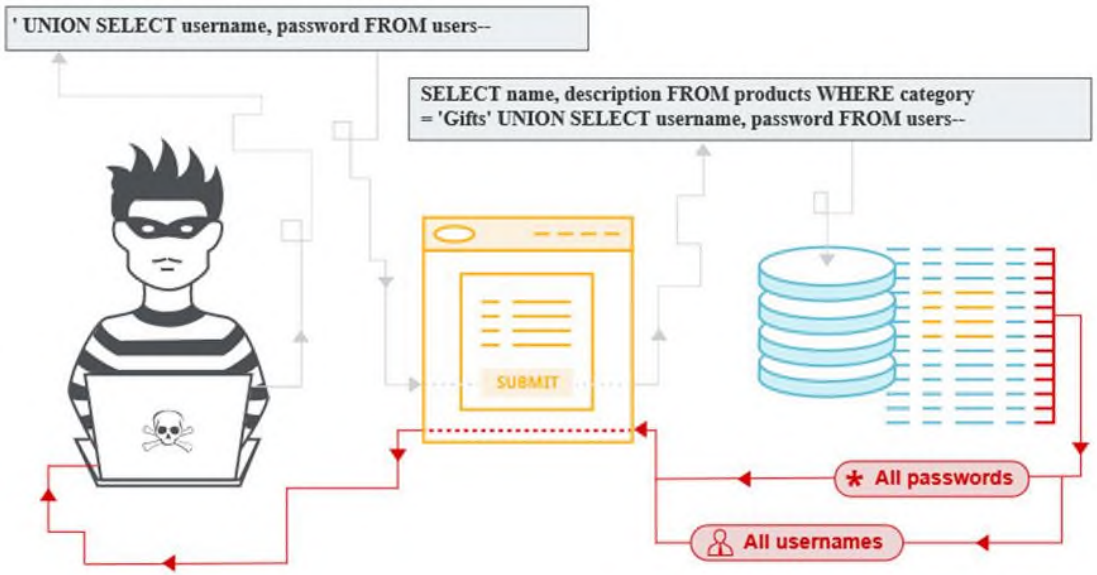


Рис 1.4 SQL ін’єкція

SQL — це мова запитів, розроблена для керування даними, що зберігаються в реляційних базах даних. Ви можете використовувати його для доступу, зміни та видалення даних. Багато веб-додатків і веб-сайтів зберігають усі дані в базах даних SQL. У деяких випадках ви також можете використовувати команди SQL для запуску команд операційної системи. Таким чином, успішна атака SQL ін’єкції може мати дуже серйозні наслідки:

- Зловмисники можуть використовувати SQL ін’єкції, щоб знайти облікові дані інших користувачів у базі даних. Потім вони можуть видати себе за цих користувачів. Уособлений користувач може бути адміністратором бази даних з усіма привілеями бази даних.
- SQL дозволяє вибирати та виводити дані з бази даних. Уразливість SQL Injection може дозволити зловмиснику отримати повний доступ до всіх даних на сервері бази даних.
- SQL також дозволяє змінювати дані в базі даних і додавати нові дані. Наприклад, у фінансовій програмі зловмисник може використовувати SQL Injection, щоб змінити баланси, анулювати транзакції або переказати гроші на свій рахунок.
- Ви можете використовувати SQL для видалення записів із бази даних, навіть видалення таблиць. Навіть якщо адміністратор створює резервні копії

бази даних, видалення даних може вплинути на доступність програми, доки база даних не буде відновлена. Крім того, резервні копії можуть не охоплювати найновіші дані.

- На деяких серверах баз даних ви можете отримати доступ до операційної системи за допомогою сервера баз даних. Це може бути навмисно або випадково. У такому випадку зловмисник може використати SQL-ін’єкцію як початковий вектор, а потім атакувати внутрішню мережу за брандмауэром.

1.1.5. Тунелювання DNS

Тунелювання DNS – це техніка DNS-атаки, яка передбачає кодування інформації інших протоколів або програм у запитах і відповідях DNS. DNS-тунелювання зазвичай містить корисні дані, які можуть закріплюватися на цільовому сервері DNS, дозволяючи зловмиснику керувати програмами та віддаленим сервером. Тунелювання DNS, як правило, покладається на підключення до зовнішньої мережі скомпрометованої системи — для тунелювання DNS потрібен вихід на внутрішній сервер DNS, який має доступ до мережі. Зловмисники також повинні контролювати сервер і домен, який може функціонувати як авторитетний сервер для виконання виконуваних програм корисного навантаження даних і тунелювання на стороні сервера.

DNS спочатку був створений для розпізнавання імен, а не для обміну даними, тому часто не розглядається як ризик для викрадення даних або зловмисного обміну інформацією. Більшість організацій зосереджують свої зусилля з безпеки на веб-трафіку та трафіку електронної пошти, оскільки вважають це регулярним джерелом атак. У результаті DNS часто не помічають.

DNS — це конфіденційний і надійний протокол, тому кіберзлочинці можуть скористатися тим фактом, що багато організацій не часто перевіряють DNS-пакети на наявність зловмисної поведінки. Окрім цього, пакети програм для тунелювання тепер є індустрією та широко доступні через Інтернет. Зловмиснику не потрібно бути особливо досвідченим, щоб здійснити тунелювання DNS.

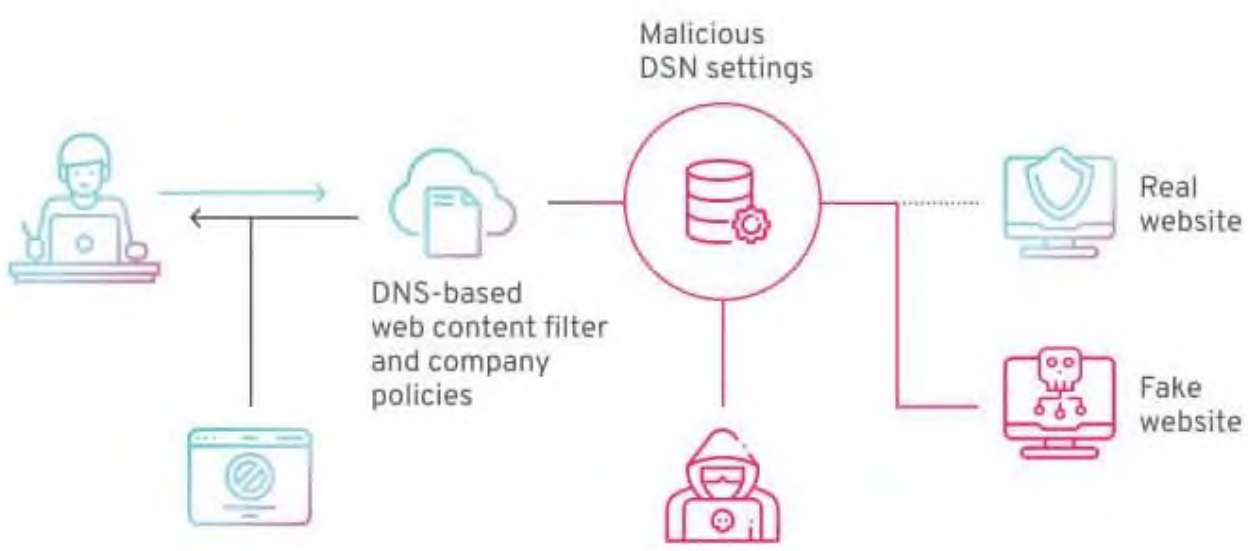


Рис 1.5 Тунелювання DNS

Загрози, створені DNS-тунелюванням, включають:

- DNS-тунелювання можуть надати зловмисникам доступ до зворотного каналу для вилучення викраденої інформації. DNS забезпечує приховані засоби листування для обходу брандмауерів.
- Кіберзлочинці тунелюють різні види протоколів, наприклад HTTP або SSH, з DNS, що дозволяє їм приховано передавати вкрадені дані або IP-трафік.
- Тунель DNS можна використовувати як повний канал контролера для внутрішнього хосту, який уже був використаний. Це дозволяє

кіберзлочинцям завантажувати код шкідливого програмного забезпечення, таємно вилучати записи з організації або мати повний віддалений доступ до серверів тощо.

- DNS-тунелі також можна використовувати для обходу приєднаних порталів, тому їм не потрібно платити за послуги Wi-Fi.
- Тунелювання DNS використовує протокол DNS для тунелювання інформації та зловмисного програмного забезпечення через модель клієнт-сервер.

1.1.6. Міжсайтові скриптові атаки

Міжсайтовий сценарій — це атака з ін’єкцією коду, під час якої зловмисник вставляє шкідливий код на законний веб-сайт. Потім код запускається як інфікований сценарій у веб-браузері користувача, що дозволяє зловмиснику викрасти конфіденційну інформацію або видати себе за користувача. Веб-форуми, дошки оголошень, блоги та інші веб-сайти, які дозволяють користувачам публікувати свій вміст, найбільш вразливі до цих атак. Якщо введені дані не перевірено, перевірено та не закодовано веб-програмою, будь-який шкідливий сценарій, включений у код, автоматично запускатиметься у веб-переглядачах інших користувачів. Потім цей сценарій може отримати доступ до файлів cookie користувача, маркерів сеансу або іншої конфіденційної інформації, яка зберігається браузером і використовується на цьому сайті.

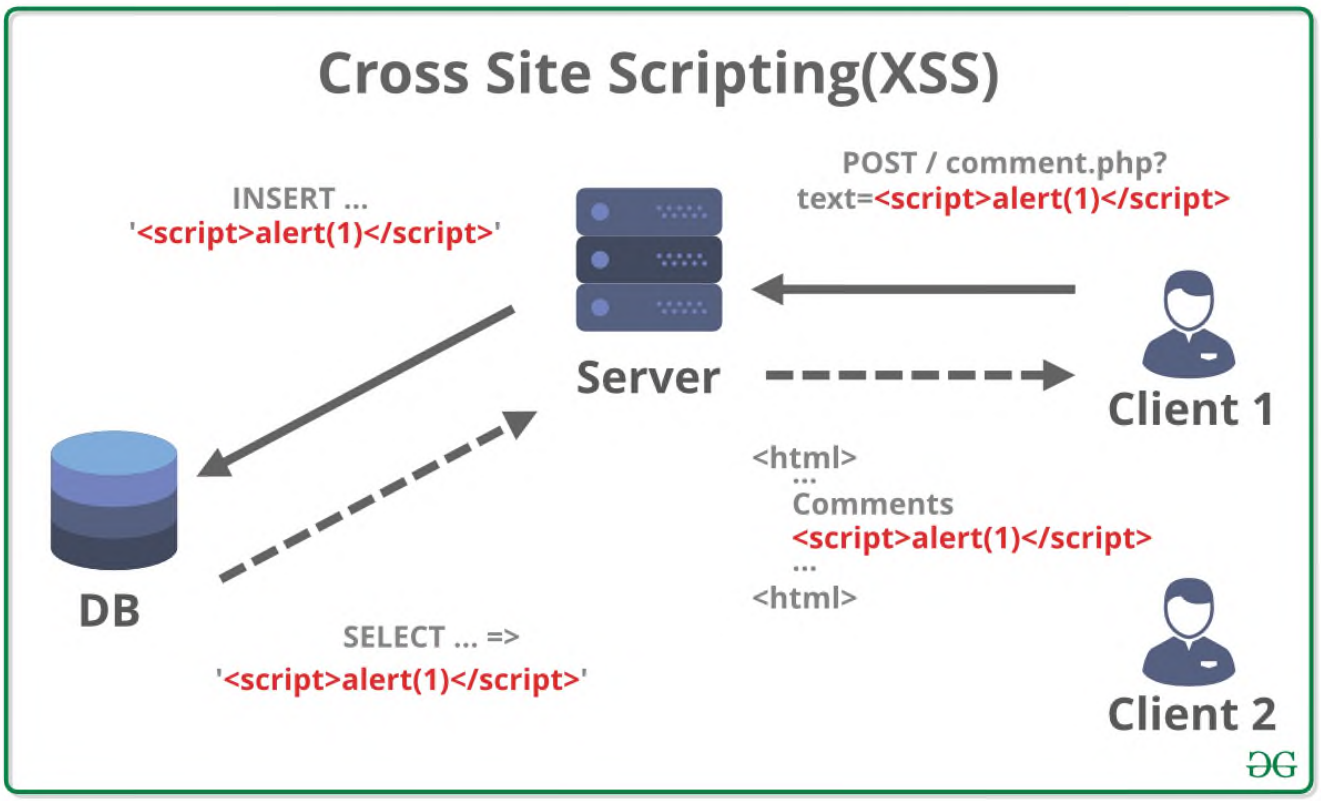


Рис 1.6 Міжсайтові скриптові атаки

Ці сценарії навіть можуть переписати вміст зараженої веб-сторінки в більш складних атаках. Безфайлові атаки та атаки на основі сценаріїв, такі як XSS, останніми роками зростають через їх здатність уникати. Ці атаки можуть легко обійти традиційні антивірусні рішення та брандмауери, що робить їх відносно простими у виконанні. Організації повинні включити виявлення та запобігання XSS як частину своєї загальної стратегії кібербезпеки, щоб захистити відвідувачів своїх веб-сайтів і зменшити ризик шкоди репутації організації.

1.1.7. Уразливість нульового дня

Вразливість нульового дня — це загроза в частині програмного забезпечення, про яку публічно не відомо та про яку не знає постачальник. Експлойт нульового дня — це метод, який зловмисник використовує для доступу до вразливої системи. Це серйозні загрози безпеці з високим рівнем успіху, оскільки компанії не мають засобів захисту, щоб їх виявити або запобігти. Атака

нульового дня називається так, оскільки вона відбувається до того, як ціль дізнається про існування вразливості. Зловмисник випускає зловмисне програмне забезпечення до того, як розробник або постачальник мав можливість створити патч для усунення вразливості. У контексті цього визначення атаки нульового дня термін «нульовий день» походить зі світу піратських цифрових медіа. Піратська версія фільму, музики чи програмного забезпечення називається «нульовим днем», якщо вона стає доступною в той самий час або до офіційного випуску. Іншими словами, піратська версія публікується через нуль днів після офіційної версії. Атака нульового дня починається з того, що хакер виявляє вразливість нульового дня, яка є помилкою в коді чи програмному забезпеченні, яку ціль ще не виявила. Потім зловмисник працює над експлойтом нульового дня, методом атаки, який він може використати, щоб скористатися наявною вразливістю.

Атака нульового дня починається з того, що розробник програмного забезпечення випускає вразливий код, який помічає та використовує зловмисник. Тоді атака або є успішною, що, ймовірно, призведе до крадіжки особи чи інформації зловмисником, або розробник створює патч, щоб обмежити її поширення. Як тільки патч буде написаний і застосований, експлойт більше не буде називатися експлойтом нульового дня.

Як тільки виробник програмного забезпечення дізнається про вразливість, він може розробити патч, який спеціально змінює відповідальну частину коду. Або публікує оновлення, тобто переглянуту та очищену версію своєї програми. Щойно з’явиться патч або оновлення, експлойт більше не діє, загроза нульового дня офіційно закінчена. Однак, оскільки багато користувачів застосовують новую версію не відразу, а лише через кілька днів або тижнів, небезпека, яку створює вразливість, залишається певний час. Атаки нульового дня є одними з найнебезпечніших з усіх. Тому що поки уразливість невідома виробникам і користувачам, вони не вживають жодних превентивних захисних заходів. Днями, іноді тижнями чи місяцями зловмисники можуть непомітно досліджувати комп’ютерні системи інших людей, отримувати вищі права, завантажувати конфіденційні дані або встановлювати зловмисне програмне забезпечення.

Антивірусні засоби призначені для виявлення таких дій. Тим не менш, зловмисникам раз у раз вдається так добре замаскуватися, що іноді вони залишаються непоміченими.

Уразливість нульового дня має високу цінність на чорному ринку. У дарк-мережі пропонуються шести-семизначні суми за щойно виявлену та ще не виправлену діру в безпеці Windows. Але не тільки злочинці зацікавлені в уразливостях. Раніше спецслужби також використовували прогалини для здійснення атак на бази даних та інфраструктуру інших держав. Найвідомішим прикладом є Stuxnet: комп'ютерний черв'як, як повідомляється, розроблений Ізраїлем і США, був проникнутий у системи іранської ядерної програми. Через кілька раніше невідомих дірок у безпеці Windows йому вдалося вкоренитися в системі. Потім він маніпулював керуванням центрифуг для виробництва матеріалу, що розщеплюється, так що через короткий час вони вийшли з ладу, але не видавали повідомлення про помилку.

1.2. Сучасні технології забезпечення безпеки

1.2.1. Аналіз систем виявлення вторгнень

Система виявлення вторгнень — це технологія мережевої безпеки, спочатку розроблена для виявлення вразливостей цільової програми або комп'ютера.

Система виявлення вторгнень також є пристроєм лише для прослуховування. Вона відстежує трафік і повідомляє результати адміністратору. Він не може автоматично вжити заходів, щоб запобігти виявленому експлойту захопити систему. Зловмисники здатні швидко використовувати вразливі місця, коли вони проникають у мережу. Таким чином, ця система не підходить для профілактики. Системи виявлення та запобігання вторгненням важливі для безпеки інформації та керування подіями.

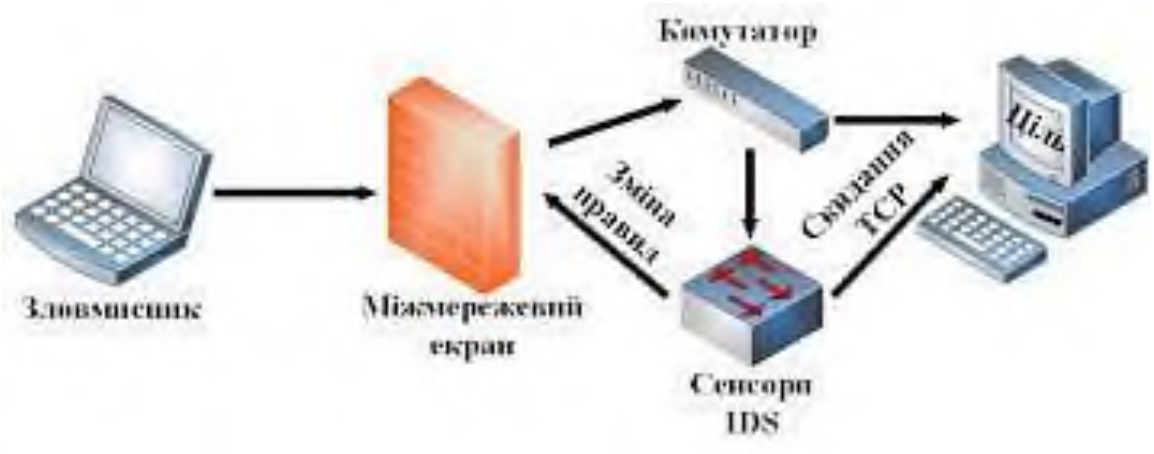


Рис 1.7 Система виявлення вторгнень

Система виявлення вторгнень лише виявляє потенційні загрози. Вона розміщена поза смугою мережевої інфраструктури. Отже, ця система не знаходиться на шляху зв'язку в реальному часі між відправником і отримувачем інформації. Коли ця система була розроблена, глибина аналізу, необхідна для виявлення вторгнення, не могла бути виконана досить швидко. Швидкість не встигає за компонентами на прямому шляху зв'язку мережевої інфраструктури. Системи виявлення мережевих вторгнень використовуються для виявлення підозрілої активності, щоб зловити хакерів до того, як мережі буде завдана шкода. Існують мережеві та хост-системи виявлення вторгнень. Система виявлення вторгнень на основі хоста встановлюються на клієнтські комп'ютери; мережеві системи виявлення вторгнень знаходяться в самій мережі.
Ця система працює, шукаючи відхилення від нормальної активності та відомі сигнатури атак. Аномальні шаблони надсилаються в стек і перевіряються на протокольному та прикладному рівнях. Він може виявляти такі події, як отруєння DNS, неправильно сформовані інформаційні пакети та сканування ялинки. Система виявлення вторгнень може бути реалізований як пристрій безпеки мережі або програмне забезпечення. Для захисту даних і систем у хмарних середовищах також доступні хмарні рішення.

Існує п'ять типів таких систем: на основі мережі, на основі хоста, на основі протоколу, на основі протоколу програми та гібридний:

- Мережева система виявлення вторгнень (NIDS). Мережевий IDS контролює всю захищену мережу. Він розгортається по всій інфраструктурі в стратегічних точках, таких як найбільш уразливі підмережі. NIDS відстежує весь трафік, що надходить до та від пристроїв у мережі, роблячи визначення на основі вмісту пакетів і метаданих.
- Система виявлення вторгнень на основі хоста (HIDS). IDS на основі хоста відстежує комп'ютерну інфраструктуру, на якій її встановлено. Іншими словами, він розгортається на певній кінцевій точці, щоб захистити її від внутрішніх і зовнішніх загроз. IDS досягає цього, аналізуючи трафік, реєструючи зловмисну активність і повідомляючи призначені органи.
- На основі протоколу (PIDS)

  Система виявлення вторгнень на основі протоколу зазвичай встановлюється на веб-сервері. Він відстежує та аналізує протокол між користувачем/пристроєм і сервером. PIDS зазвичай знаходиться на передній частині сервера та контролює поведінку та стан протоколу.
- На основі протоколу додатків (APIDS) APIDS — це система або агент, який зазвичай знаходиться всередині серверної сторони. Він відстежує та інтерпретує листування за протоколами, що стосуються окремих програм. Наприклад, це відстежуватиме протокол SQL для проміжного програмного забезпечення під час транзакцій із веб-сервером.
- Гібридна система виявлення вторгнень Гібридна система виявлення вторгнень поєднує два або більше підходів до виявлення вторгнень. Використання цієї системи, даних системи або хост-агента в поєднанні з мережевою інформацією для повного уявлення про систему. Гібридна система виявлення вторгнень більш потужна порівняно з іншими системами. Одним із прикладів гібридних IDS є Prelude.

1.2.2. Система запобігання вторгненням

Багато в чому автоматизовані рішення IPS допомагають відфільтрувати зловмисну активність до того, як вона досягне інших пристроїв безпеки або

елементів керування. Це зменшує ручні зусилля команд безпеки та дозволяє іншим продуктам безпеки працювати ефективніше. Рішення IPS також дуже ефективні для виявлення та запобігання використанню вразливостей. Коли виявляється вразливість, зазвичай є вікно можливостей для використання, перш ніж можна буде застосувати виправлення безпеки. Тут використовується система запобігання вторгненням, щоб швидко блокувати такі типи атак. Пристрої IPS спочатку були створені та випущені як автономні пристрої в середині 2000-х років. Ця функція була інтегрована в рішення для єдиного управління загрозами (UTM), а також у брандмауэры наступного покоління. Рішення IPS нового покоління тепер підключені до хмарних обчислень і мережевих послуг.

IPS розміщується в мережі, безпосередньо в потоці мережевого трафіку між джерелом і одержувачем. Це те, що відрізняє IPS від його попередника, системи виявлення вторгнень (IDS). І навпаки, IDS є пасивною системою, яка сканує трафік і повідомляє про загрози. Зазвичай розташовуючись безпосередньо за брандмауером, рішення аналізує всі потоки трафіку, що надходять у мережу, і вживає автоматизованих дій, коли це необхідно.

Ці дії можуть включати:

- Надсилання тривоги адміністратору
- Відкидання шкідливих пакетів
- Блокування трафіку з адреси джерела
- Скидання з'єднання
- Налаштування брандмауерів для запобігання майбутнім атакам

Як вбудований компонент безпеки, IPS має мати можливість:

- Працювати ефективно, щоб уникнути погіршення продуктивності мережі
- Працювати швидко, оскільки експлойти можуть відбуватися майже в реальному часі
- Виявляти та точно реагувати, щоб усунути загрози та помилкові спрацьовування

Щоб зробити це успішно, існує кілька методів, які використовуються для пошуку експлойтів і захисту мережі від несанкціонованого доступу. До них належать:

- Виявлення на основі сигнатур – це метод виявлення, заснований на словнику унікальних шаблонів (або сигнатур) у коді кожного експлойта. Коли експлойт виявлено, його підпис записується та зберігається в постійно зростаючому словнику сигнатур. Виявлення сигнатур для IPS поділяється на два типи:
- Сигнатури, що захищають від експлойтів, ідентифікують окремі експлойти, запускаючи унікальні шаблони конкретної спроби експлойту. IPS може ідентифікувати конкретні експлойти, знаходячи в потоці трафіку збіг із сигнатурою, що стикається з експлойтом.
- Сигнатури, спрямовані на вразливість, — це ширші сигнатури, спрямовані на основну вразливість у системі, на яку націлено. Ці підписи дозволяють захищати мережі від невідомих. Вони також підвищують ризик помилкових спрацьовувань.
- Виявлення на основі аномалій бере вибірки мережевого трафіку випадковим чином і порівнює їх із попередньо розрахованим базовим рівнем продуктивності. Коли активність трафіку виходить за межі параметрів базової продуктивності, IPS вживає заходів.
- Виявлення на основі політики вимагає від системних адміністраторів налаштування політик безпеки на основі політик безпеки організації та мережевої інфраструктури. Якщо відбувається будь-яка дія, яка порушує визначену політику безпеки, запускається сповіщення та надсилається адміністраторам.

Існує кілька типів рішень IPS, які можна розгорнути для різних цілей. До них належать:

- Мережева система запобігання вторгненням (NIPS), яка встановлюється в стратегічних точках для моніторингу всього мережевого трафіку та пошуку загроз.

- Система запобігання вторгнень на хост (HIPS), яка встановлюється на кінцевій точці та переглядає вхідний/вихідний трафік лише з цієї машини. Часто в поєднанні з NIPS, HIPS служить останньою лінією захисту від загроз.
- Аналіз поведінки мережі (NBA) аналізує мережевий трафік, щоб виявити незвичайні потоки трафіку та виявити нове зловмисне програмне забезпечення або вразливі місця нульового дня.
- Система запобігання бездротовому вторгненню (WIPS) сканує мережу Wi-Fi на предмет несанкціонованого доступу та видаляє всі неавторизовані пристрої.

Система запобігання вторгненням має багато переваг безпеки:

- Зниження бізнес-ризиків і додаткова безпека
- Краща видимість атак і, отже, кращий захист
- Підвищена ефективність дозволяє перевіряти весь трафік на наявність загроз
- Менше ресурсів, необхідних для керування вразливими місцями та виправленнями

1.2.3. Фізична безпека

Фізична безпека в телекомунікаціях є ключовим аспектом забезпечення надійності та стабільності мереж. З поглибленням залежності від технологій зв'язку та інформаційного обміну, вирішення питань фізичної безпеки стає вкрай важливим завданням для телекомунікаційних компаній та організацій. Однією з основних аспектів фізичної безпеки є захист інфраструктури, такої як центри обробки даних (ЦОД), вузли передачі даних і транзитні точки. Фізичний доступ до цих об'єктів повинен бути суворо контрольованим і обмеженим. Використання сучасних систем контролю доступу, відеоспостереження та сигналізаційних систем грає ключову роль у забезпеченні безпеки. Важливо також враховувати природні катастрофи, такі як землетруси, повені або пожежі, які можуть вплинути на фізичну інфраструктуру телекомунікацій. Розташування об'єктів на безпечних

відстанях від потенційно небезпечних зон та використання технологій, які забезпечують відмовостійкість та відновлення послуг, є необхідними стратегіями. Зокрема, велика увага приділяється захисту фізичної інфраструктури від вибухових та хімічних загроз. Застосування сучасних матеріалів та технологій допомагає зменшити можливість пошкоджень у разі подібних інцидентів, а також дозволяє більш ефективно управляти ризиками. Окрім того, захист від фізичних загроз передбачає розробку та реалізацію планів екстреного реагування, тренувань персоналу та вдосконалення систем виявлення та реагування на потенційні загрози. Усі ці заходи повинні бути частиною комплексного підходу до забезпечення фізичної безпеки в телекомунікаціях. Запобігання, виявлення та ефективне управління ризиками є критичними елементами стратегій, спрямованих на забезпечення неперервності та надійності телекомунікаційних мереж.

У світлі постійного розвитку технологій та зростаючої загрози кібератак, важливо також розглядати фізичну безпеку в контексті кібербезпеки. Забезпечення безпеки фізичної інфраструктури пов'язане з захистом від потенційних кіберзагроз. Наприклад, атаки на центри обробки даних через мережеві канали можуть призвести до фізичних пошкоджень обладнання або втрати даних. Однією з ключових аспектів є впровадження технологій "Security by Design" в архітектуру фізичної інфраструктури. Це включає в себе врахування аспектів безпеки на кожному етапі розробки та експлуатації системи. Використання шифрування та інших методів захисту даних під час їх транспортування через фізичні канали також є важливою складовою стратегії. Забезпечення ефективного контролю доступу в телекомунікаційних об'єктах є однією з найважливіших завдань. Це охоплює не тільки фізичний доступ до приміщень, але і здійснення контролю за електронними та мережевими ресурсами. Автентифікація, авторизація та аудит - це важливі елементи систем безпеки, які дозволяють визначити, хто, куди і що може зробити в системі телекомунікацій. Необхідно також враховувати аспекти стійкості до фізичних атак. Використання бар'єрів та стійких до вибуху матеріалів для захисту від

несанкціонованого доступу або здійснення атак є ключовим завданням. Впровадження систем виявлення та реагування на інциденти, які можуть автоматично виявляти аномальну діяльність та приймати заходи для запобігання можливим загрозам, грає важливу роль в забезпеченні безпеки. Загалом, фізична безпека в телекомунікаціях вимагає комплексного підходу, що об'єднує сучасні технології, стратегії управління ризиками та впровадження найкращих практик у галузі кібербезпеки. Тільки такий підхід може гарантувати стабільну та безпечну роботу телекомунікаційної інфраструктури в умовах постійно зростаючих загроз.

У доповнення до зазначених аспектів, розвиток технологій в області фізичної безпеки в телекомунікаціях також охоплює впровадження інноваційних засобів та концепцій:

- Застосування систем розпізнавання обличчя для ідентифікації та аутентифікації персоналу в зонах обмеженого доступу.
- Використання біометричних даних, таких як відбитки пальців чи розпізнавання пульсу, для додаткового рівня безпеки.
- Використання аналізу великих обсягів даних для попередження можливих інцидентів або виявлення невичерпних патернів у фізичній безпеці.
- Розробка та впровадження технологій для усунення можливості зламування фізичних бар'єрів.

Ці інновації допомагають забезпечити фізичну безпеку в телекомунікаціях на новому рівні, створюючи надійні та стійкі системи в умовах непередбачуваних загроз та швидко змінюючих технологічного середовища.

Ефективний контроль доступу в телекомунікаційних об'єктах є критичним завданням, охоплюючи не лише фізичний доступ до приміщень, але і керування електронними та мережевими ресурсами. Автентифікація, авторизація та аудит грають важливу роль у визначенні, хто, куди і що може зробити в системі телекомунікацій. Забезпечення стійкості до фізичних атак також потребує використання бар'єрів та стійких до вибухів матеріалів для захисту від несанкціонованого доступу чи атак. Впровадження систем виявлення та

реагування на інциденти грає важливу роль у виявленні аномальної діяльності та автоматичному реагуванні на можливі загрози. У додаток до основних аспектів, розвиток технологій в області фізичної безпеки включає в себе інновації, такі як використання технологій розпізнавання обличчя та біометрії для ідентифікації персоналу, інтеграцію з системами штучного інтелекту для аналізу великих обсягів даних, використання дронів та робототехніки для моніторингу та реагування на загрози. Розробка та використання матеріалів з підвищеною стійкістю, використання квантової криптографії, а також застосування блокчейн-технологій для захисту фізичної інфраструктури - це лише кілька напрямків, які спрямовані на зміцнення фізичної безпеки в телекомунікаціях. Загальний успіх у цьому напрямку потребує також участі в глобальних ініціативах з координації та стандартизації, а також врахування соціально-інженерних аспектів та забезпечення екологічної стійкості. Постійне навчання та розвиток персоналу, а також постійне тестування та оновлення стратегій безпеки, є ключовими елементами для забезпечення ефективної фізичної безпеки в телекомунікаціях. Врахування широкого спектру факторів та застосування комплексного підходу допомагає створювати стійкі та безпечні системи телекомунікацій в умовах постійно зростаючих загроз та технологічних викликів.

1.3. Визначення вразливостей в мережевій інфраструктурі

Визначення вразливостей в мережевій інфраструктурі – це невід'ємна частина стратегії забезпечення інформаційної безпеки. Цей процес необхідний для постійного моніторингу та адаптації систем безпеки до зростаючих загроз та змін у кіберпросторі. Аналіз мережі включає в себе глибокий огляд архітектури, конфігурації та топології мережевої інфраструктури з метою виявлення можливих точок вразливості. Проведення сканування портів та служб допомагає ідентифікувати активні елементи та служби, що дозволяє вчасно виявляти можливі шляхи атак. Оцінка програмного забезпечення грає важливу роль у визначенні вразливостей. Регулярне виявлення та оновлення програм дозволяє уникнути експлуатації вразливостей і зміцнює загальний рівень безпеки. Оцінка

конфігурацій безпеки, включаючи мережеві пристрої та сервери, також стає важливим етапом в процесі виявлення слабкостей. Вивчення вразливостей веб-додатків стає необхідною складовою, оскільки вони можуть стати потенційними точками входу для атак. Моніторинг та аналіз журналів подій, а також проведення пенетраційних тестів, спрямовані на виявлення аномалій та можливих вразливостей. Регулярне оновлення та встановлення патчів для операційних систем та програмного забезпечення є ключовим для усунення визначених вразливостей та запобігання потенційним атакам. Важливо також враховувати соціально-інженерні аспекти, оскільки людський фактор може бути використаний для експлуатації вразливостей. Усі ці аспекти визначення вразливостей взаємодіють, утворюючи комплексний підхід до забезпечення безпеки мережевої інфраструктури. Цей підхід є постійним та адаптивним, враховуючи постійні зміни в кіберпросторі та вимагає систематичного оновлення та вдосконалення стратегій для ефективного захисту від потенційних загроз. Однією з ключових аспектів визначення вразливостей є також проведення пенетраційних тестів, які імітують атаки з боку зловмисників для виявлення слабких місць у системі. Ці тести дозволяють спеціалістам з безпеки перевірити дійсну стійкість системи в умовах реальних атак. Окрім технічних аспектів, важливо приділяти увагу аспектам соціальної інженерії. Навчання персоналу щодо технік обережності та виявлення спроб маніпулювання може запобігти багатьом видам атак, що базуються на соціальних векторах. Створення чіткої системи відстеження та реагування на інциденти також входить в обов'язки забезпечення безпеки. Швидке виявлення та реагування на потенційні атаки може значно зменшити можливі шкоди внаслідок вразливостей. З урахуванням динаміки кіберзагроз, стратегії визначення вразливостей повинні бути постійно оновлюваними. Команди забезпечення безпеки повинні бути готовими адаптувати свої підходи до нових видів загроз та використовувати найновіші технології для покращення стійкості систем. Важливим є також забезпечення прозорості та співпраці між всіма сторонами, що займаються кібербезпекою. Обмін інформацією про нові вразливості та методи атак може допомогти всьому галузеві краще захищати себе

від спільних загроз. Загалом, визначення вразливостей – це багатоаспектний підхід, який об'єднує технічні, соціальні та стратегічні аспекти. Тільки завдяки комплексному підходу можна досягти високого рівня безпеки в умовах постійно зростаючих загроз та еволюції кіберзлочинності.

Паралельно з ідентифікацією та усуненням вразливостей, важливим етапом є розробка та впровадження стратегій передбачення та захисту. Аналіз інтелектуальних систем та алгоритмів для передбачення можливих атак дозволяє попереджувати інциденти до їх виникнення. Однією з інноваційних областей є використання блокчейн-технологій для підвищення безпеки мережевих систем. Розподілена структура блокчейну може служити ефективним механізмом виявлення та запобігання атак, оскільки вона ускладнює завдання зловмисникам змінити інформацію чи порушити систему. Також, в сучасному світі велика увага приділяється розробці та впровадженню технологій квантового шифрування, які обіцяють більшу стійкість до атак з боку квантових комп'ютерів. Важливим елементом в забезпеченні безпеки є реагування на визначені загрози. Планування та тренування персоналу на випадок кібер інцидентів стає критично важливим елементом готовності до атак та миттєвого реагування на їхні наслідки. І, зрештою, наголос на культурі кібербезпеки у всій організації є важливим фактором. Засвоєння кращих практик, включаючи регулярні навчання та оновлення стандартів безпеки, допомагає створити середовище, де безпека є пріоритетом для всіх. В цілому, комплексний підхід до визначення вразливостей та забезпечення безпеки охоплює технічні, стратегічні та соціальні аспекти. Тільки завдяки цілісному розумінню загроз та використанню передових технологій можна створити стійку та надійну систему інформаційної безпеки в умовах постійних змін кібер середовища.

На тлі зростаючих технологічних викликів та комплексності кіберзагроз, керівництво організацій повинно усвідомлювати, що безпека – це процес, а не одноразова подія. Регулярне оновлення політик безпеки та їх адаптація до нових реалій є ключем до успішного управління кібербезпекою. Також, слід враховувати глобальний характер кіберзагроз та необхідність міжнародного

співробітництва. Обмін інформацією та кращими практиками між країнами та компаніями може значно підвищити загальний рівень стійкості та відповідальності в кіберпросторі. Деякі ініціативи також спрямовані на розвиток стандартів безпеки для різних галузей, забезпечуючи узгодженість та високий рівень захисту даних та інфраструктури. Здійснення аудитів відповідності та впровадження сертифікаційних стандартів допомагає забезпечити, що організації дотримуються визначених вимог щодо безпеки. У світлі новітніх технологій, таких як Інтернет речей (IoT) та штучний інтелект (AI), безпека стає ще більш актуальною. Зростання кількості підключених пристроїв та використання алгоритмів машинного навчання вимагає вдосконалення заходів забезпечення безпеки та впровадження нових методів виявлення та запобігання атакам. Завдяки вдосконаленню інфраструктури, розвитку нових технологій та посиленню свідомості у сфері кібербезпеки, можна ефективно протистояти сучасним викликам. Прагнення до вдосконалення заходів безпеки та забезпечення сталої захищеності мережевої інфраструктури стає невід'ємною частиною стратегії будь-якої організації в умовах сучасного цифрового світу.

На шляху до забезпечення повноцінної кібербезпеки важливо також розглядати аспекти етичного використання та прозорості в розробці та впровадженні технологій. Забезпечення приватності користувачів та відкритість щодо методів збору та обробки даних стає ключовим завданням. Особлива увага повинна бути приділена інформаційній гігієні та кібергігієні – освітнім ініціативам, спрямованим на підвищення свідомості користувачів щодо безпеки в кіберпросторі. Інформовані та навчені користувачі є важливим ланцюгом у загальній системі кіберзахисту. Додатковою складовою стає розробка і впровадження стандартів та правил в області кібербезпеки. Це включає в себе встановлення обов'язкових вимог щодо безпеки для розробників програмного забезпечення, операторів мереж та виробників обладнання. Такий підхід дозволяє підняти планку безпеки на високий рівень та вирівняти загальні стандарти у цифровому середовищі. Ще однією важливою складовою стратегії кібербезпеки є удосконалення міжнародного співробітництва та розробка міжнародних

стандартів. Оскільки кіберзагрози не мають кордонів, важливо, щоб країни та організації спільно працювали над розробкою та впровадженням заходів забезпечення безпеки. У заключенні, питання кібербезпеки стає невід'ємною складовою нашого цифрового життя. Нинішні та майбутні виклики вимагають від нас постійної готовності адаптувати та удосконалювати заходи безпеки. Тільки через об'єднані зусилля всіх сторін – від індивідів та підприємств до держав та міжнародних організацій – можна забезпечити сталу та ефективну кібербезпеку в сучасному цифровому світі.

Поруч із постійним удосконаленням технічних засобів та стратегій кібербезпеки, важливим аспектом є також формування відповідальної кіберкультури серед користувачів. Забезпечення освіти та навчання у сфері кібербезпеки на всіх рівнях суспільства є запорукою того, що люди не лише користуються технологіями безпечно, але й розуміють загрози та можуть ефективно реагувати на них. Досягнення цієї мети також вимагає врахування економічних та правових аспектів. Забезпечення необхідних ресурсів для реалізації заходів з кібербезпеки та створення ефективних механізмів правозахисту є ключовим елементом національних та міжнародних стратегій в цій області. Паралельно з цим, важливо розвивати динамічну систему міжнародного обміну інформацією про кіберзагрози. Спільна реакція на нові види атак та взаємне співробітництво у розслідуванні інцидентів може виявитися вирішальним чинником в сучасному цифровому ландшафті. Також важливо наголосити на принципах прозорості та відкритості. Відкритий обмін досвідом та інформацією, відкрите спілкування між експертами та галузевими спільнотами – це не лише важливий крок у напрямку поліпшення захисту, але й сприяє виникненню інновацій та розвитку нових підходів до кібербезпеки. У світлі непередбачуваності кіберзагроз, розвиток гнучких та адаптивних стратегій кібербезпеки стає необхідністю. Це передбачає поєднання традиційних методик з новаторськими рішеннями, а також готовність до постійного вдосконалення та апгрейдування існуючих систем. Загалом, створення надійної кібербезпеки є складним завданням, що вимагає системної роботи на багатьох рівнях суспільства

та галузей економіки. Вирішення цього завдання стане кроком вперед до забезпечення стійкості та безпеки в цифровому віці.

Для впровадження ефективних стратегій кібербезпеки важливо не лише реагувати на існуючі загрози, але і активно анігілювати їх народження. Розвиток передових методів виявлення аномалій та попередження інцидентів вимагає використання сучасних технологій, таких як штучний інтелект та аналіз великих обсягів даних. Принцип оборони у глибину є ключовим у підході до кібербезпеки. Забезпечення безпеки не обмежується лише зовнішнім захистом, але й включає в себе внутрішні бар'єри та механізми виявлення порушень. Комплексне застосування технічних, організаційних та адміністративних засобів стає важливим аспектом створення надійної кібербезпекової системи. Особливу увагу слід звертати на кібергігієну організацій, яка включає в себе визначення та виконання найкращих практик в галузі кібербезпеки. Регулярні навчання персоналу, аудити безпеки та усунення ідентифікованих вразливостей є необхідними складовими для забезпечення сталої захищеності. Необхідно також активно сприяти розвитку міжнародних стандартів та норм для кібербезпеки. Створення єдиної системи принципів та вимог може значно полегшити взаємодію країн та підприємств у сфері кіберпростору. Зокрема, створення інтернаціональних центрів обміну інформацією про кіберзагрози та події може стати ефективним механізмом для попередження та реагування на інциденти. Спільні зусилля на міжнародному рівні сприятимуть розвитку глобальної кібербезпекової спільноти. У кінці кінців, створення ефективної системи кібербезпеки вимагає від нас не лише технічної компетентності, але й готовності до співпраці, інновацій та постійного вдосконалення. Тільки таким чином можна гарантувати сталу стійкість у світі, де технології швидко розвиваються, а загрози постійно змінюються.

2. ОРГАНІЗАЦІЯ ЗАХИСТУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗА ДОПОМОГОЮ СУЧАСНИХ МЕТОДІВ ШИФРУВАННЯ

2.1. Огляд сучасних методів шифрування

У сучасну інформаційну епоху комунікації відіграють важливу роль, що сприяло розвитку технологій. Електронна безпека все більше бере участь у поширенні комунікацій. Тому потрібен механізм для забезпечення безпеки та конфіденційності інформації, що надсилається через засоби електронного зв'язку. Незалежно від того, чи є комунікаційне середовище дротовим чи бездротовим, обидва не можуть бути захищені від несанкціонованого прийому або перехоплення передачі. Метод перетворення вихідної інформації у нечитабельний формат називається шифруванням і дешифруванням інформації. Вивчення шифрування та дешифрування відоме як криптографія. Криптографія або спілкування за допомогою секретного коду використовувалася єгиптянами близько 4000 років тому. Всього існує два типи ключів криптографії, заснованих на публічній доступності ключа: криптографія закритого ключа та Криптографія з відкритим ключем. І відправник, і одержувач мають спільний ключ, який має бути закритим. У першому випадку відправник і одержувач діляться особистим ключем між собою, який має бути розподілений перед тим, як відбудеться фактичне спілкування. Найвідомішим прикладом цього типу криптографії є стандарт шифрування даних (DES). У криптографії з відкритим ключем кожна сторона має два набори ключів; один ключ відомий громадськості, а інший зберігається в секреті для власника

За своєю суттю шифрування — це процес, який перетворює читабельні дані, відомі як відкритий текст, у нечитабельний формат, який називається зашифрованим текстом. Це перетворення досягається за допомогою складних алгоритмів і ключа. Ключ, який може бути рядком випадкових чисел і літер, використовується для дешифрування зашифрованого тексту назад у відкритий текст. Це гарантує, що навіть якщо дані перехоплено під час передачі, вони залишаються незрозумілими для будь-кого без ключа дешифрування. Телекомунікаційне шифрування можна розділити на два типи: симетричне та

асиметричне. Симетричне шифрування використовує той самий ключ як для шифрування, так і для дешифрування. Він швидший і ефективніший, що робить його ідеальним для шифрування великих обсягів даних. Однак необхідність обміну ключем між відправником і одержувачем може становити загрозу безпеці. Асиметричне шифрування, з іншого боку, використовує два різні ключі: відкритий ключ для шифрування та закритий ключ для дешифрування. Відкритий ключ доступний кожному, але закритий ключ залишається конфіденційним для власника. Цей метод усуває ризик перехоплення ключа під час передачі, але він повільніший і вимагає більше обчислювальних ресурсів.



Рис 2.1 Шифрування

Роль шифрування в телекомунікаціях не обмежується захистом даних під час передачі. Він також забезпечує цілісність даних, перевіряючи, що вони не були підроблені під час передачі. Крім того, він забезпечує автентифікацію шляхом підтвердження ідентичності сторін, що спілкуються. Одним із найпоширеніших застосувань шифрування в телекомунікаціях є мобільні мережі. Наприклад, мережа 4G LTE використовує шифрування для захисту конфіденційності та

цілісності даних користувача. Коли здійснюється дзвінок або надсилається повідомлення, дані шифруються перед тим, як покинути пристрій, і залишаються зашифрованими, доки не досягнуть пристрою одержувача, де розшифровуються. Ще одна програма – це служби голосового зв'язку через Інтернет-протокол (VoIP), які передають голосові дані через Інтернет. Провайдери VoIP використовують шифрування для захисту голосових даних від прослуховування та перехоплення. Подібним чином постачальники послуг Інтернету (ISP) використовують шифрування для захисту інтернет-трафіку користувачів. Незважаючи на численні переваги, шифрування в телекомунікаціях не позбавлене проблем. Однією з головних проблем є компроміс між безпекою та продуктивністю. Вищі рівні шифрування забезпечують кращий захист, але можуть уповільнити швидкість передачі. Крім того, шифрування може ускладнити правоохоронним органам перехоплення комунікацій для законних цілей, що призводить до дискусій про баланс між конфіденційністю та безпекою.

Важливо зашифрувати повідомлення, файли та дані, які обмінюються онлайн, якщо вони відповідають особистій, конфіденційній або секретній інформації. Шифрування бере звичайний текст, як-от текстове повідомлення чи електронний лист, і перетворює його в нечитабельний формат, який називається зашифрованим текстом. Це допомагає захистити конфіденційність цифрових даних, які зберігаються в комп'ютерних системах або передаються через мережу, як-от Інтернет. Коли призначений одержувач отримує доступ до повідомлення, інформація повертається до початкової форми. Це називається дешифруванням. Щоб розблокувати повідомлення, і відправник, і одержувач повинні використовувати «секретний» ключ шифрування — набір алгоритмів, які кодують і декодують дані назад у читабельний формат.

Ключ шифрування — це ряд чисел, які використовуються для шифрування та розшифровки даних. Ключі шифрування створюються за допомогою алгоритмів, і кожен ключ є випадковим і унікальним. Існує два основних типи систем шифрування: симетричне шифрування та асиметричне шифрування. Ось чим вони відрізняються.

2.1.1. Симетричні алгоритми шифрування

Симетричне шифрування — це тип шифрування, який використовує той самий ключ для шифрування та розшифрування даних. І відправник, і одержувач мають ідентичні копії ключа, які вони зберігають у секреті та нікому не діляться. Це відрізняється від асиметричного шифрування, яке використовує два ключі — відкритий ключ (до якого може отримати доступ будь-хто) для шифрування інформації та закритий ключ для розшифровки інформації.



Рис 2.2 Симетричне шифрування

Наявність лише одного ключа для обох функцій шифрування та дешифрування спрощує процес шифрування. Зрештою, ви застосовуєте один ключ, щоб перетворити зрозумілу текстову інформацію на нечитабельну тарабарщину (зашифрований текст) і навпаки. Однією з переваг використання симетричного шифрування є те, що воно забезпечує приватність і конфіденційність даних без додаткової складності кількох ключів. Шифрування з симетричним ключем працює самостійно, у певних випадках використання.

Наприклад, це корисно для шифрування баз даних і файлів, де ви не обмінюєтеся даними публічно між сторонами.

Компоненти процесу симетричного шифрування:

- Ваше вихідне повідомлення, яке ви бажаєте зашифрувати (відкриті текстові дані).
- Алгоритм шифрування з симетричним ключем
- Ідентичний секретний ключ, який маєте лише ви та ваш передбачуваний одержувач, який шифрує та розшифровує дані.
- Зашифроване повідомлення, яке ніхто не може прочитати (зашифрований текст).

Симетричне шифрування працює шляхом шифрування та дешифрування даних за допомогою ідентичних ключів. Дані, зашифровані в зашифрований текст, не можуть бути прочитані або іншим чином зрозумілі тим, хто не має ключа. Це означає, що вам і стороні, з якою ви спілкуєтеся, потрібна ідентична копія ключа для безпечного обміну даними. Однією з ключових особливостей симетричних алгоритмів є їхня здатність до швидкого та ефективного оброблення великої кількості даних. Це робить їх особливо корисними для широкого спектру застосувань, включаючи передачу даних через мережу, зберігання файлів та обробку інформації в реальному часі.

Незважаючи на успіхи та широке використання, симетричні алгоритми шифрування стикаються з деякими викликами та вимогами, які потребують постійного удосконалення. Один із важливих аспектів — це проблема керування ключами. Зі зростанням обсягу оброблюваних даних і розширенням мережевих структур, управління та збереженням ключів стає складнішим завданням. Нові методи керування ключами, такі як використання квантових ключів, розглядаються як можливі рішення для покращення цього аспекту симетричного шифрування. Іншим важливим аспектом є стійкість алгоритмів до атак. З плином часу з'являються нові методи криптоаналізу, і важливо забезпечити, щоб симетричні алгоритми залишалися стійкими в обличчі нових викликів.

Константне вдосконалення алгоритмів шифрування є ключовим елементом для забезпечення безпеки оброблюваних даних. Перспективи розвитку симетричних алгоритмів включають в себе інтеграцію з іншими методами шифрування, такими як асиметричні алгоритми, для створення більш комплексних та надійних систем шифрування. Крім того, застосування інноваційних технологій, таких як квантове шифрування, може відкривати нові горизонти у сфері захисту даних. У світлі постійного росту кількості кіберзагроз та необхідності забезпечення конфіденційності, симетричні алгоритми шифрування залишаються ключовим елементом цифрової безпеки. Їх розвиток та вдосконалення мають стратегічне значення для забезпечення стійкості та ефективності сучасних систем захисту інформації.

Однією з ключових переваг симетричних алгоритмів є їхня висока інтероперабельність. Це означає, що однаковий ключ може бути використаний для зв'язку між системами різних виробників. Ця характеристика дозволяє ефективно обмінюватися конфіденційною інформацією між різними платформами та програмним забезпеченням, сприяючи глобальній безпеці. Однак інтероперабельність також ставить виклик перед розробниками та інженерами — забезпечити стандартизацію та взаємодію між різними реалізаціями алгоритмів. Розвиток відкритих стандартів та протоколів грає важливу роль у забезпеченні сумісності та безпеки систем, що використовують симетричне шифрування. Однією з областей активного дослідження є вдосконалення стійкості симетричних алгоритмів до квантових обчислень. Розвиток квантових комп'ютерів може поставити під сумнів сучасні методи шифрування, і тому важливо розглядати альтернативи та модифікації симетричних алгоритмів для забезпечення стійкості в умовах постійного технологічного прогресу. Враховуючи різноманіття загроз та змін у технологічному середовищі, симетричні алгоритми шифрування лишаються важливим інструментом для забезпечення конфіденційності даних. Їхні переваги у високій швидкодії та ефективності роблять їх невід'ємною складовою глобальної кібербезпеки. Однак важливо продовжувати дослідження

та розвиток, щоб забезпечити їхню стійкість у змінюючомуся та динамічному цифровому ландшафті.

Симетричні алгоритми шифрування грають ключову роль у забезпеченні приватності індивідуальних користувачів та конфіденційності корпоративних даних. Із зростанням обсягу цифрової інформації, яку ми обробляємо та обмінюємо, необхідність ефективних методів шифрування стає більш важливою ніж будь-коли. Однією з переваг симетричних алгоритмів є їх здатність до застосування в різних сценаріях, починаючи від захисту особистих повідомлень та закінчуючи шифруванням великих обсягів корпоративних даних. Це робить їх ефективними та універсальними інструментами для забезпечення безпеки на різних рівнях. Інноваційні розробки в галузі симетричного шифрування включають в себе оптимізацію алгоритмів для забезпечення мінімального впливу на продуктивність систем та пристроїв. Забезпечення високої швидкодії шифрування стає ключовим завданням у світі, де темпи оброблення даних штучного інтелекту та інших технологій стрімко зростають. Деякі сучасні симетричні алгоритми використовують різні техніки, такі як блочне або потокове шифрування, для забезпечення більшої гнучкості та адаптабельності. Це дозволяє їм легше впроваджуватися в різні системи та враховувати особливості конкретних викликів та вимог в області безпеки. Насамкінець, симетричні алгоритми шифрування залишаються невід'ємною частиною технологічного прогресу та гарантії приватності у цифровому віці. Їхній постійний розвиток в сфері безпеки та захисту даних визначає нові стандарти ефективності та надійності.

Одним із показників ефективності симетричних алгоритмів є їхній рівень безпеки, який часто вимірюється у бітах. Найпопулярніші сучасні симетричні алгоритми, такі як Advanced Encryption Standard (AES), надійно забезпечують високий рівень безпеки. Наприклад, AES використовує ключі розміром 128, 192 або 256 біт, забезпечуючи високий ступінь стійкості до криптоаналітичних атак. Низька обчислювальна складність симетричних алгоритмів також грає важливу роль у їхній ефективності. Наприклад, швидкість шифрування та розшифрування важлива для застосувань в реальному часі, таких як трансляція відео, обробка

транзакцій та мобільні додатки. Сучасні симетричні алгоритми можуть досягати вражаючих швидкостей оброблення, вимірюваних в гігабайтах на секунду (GB/s), забезпечуючи ефективне використання ресурсів.

У таблиці нижче представлені порівняння розмірів ключів та швидкостей деяких сучасних симетричних алгоритмів:

Таблиця 2.1

Швидкість роботи різних симетричних алгоритмів

Алгоритм	**Розмір ключа (біти)**	**Швидкість (GB/s)**
AES (128 біт)	128	До 10
AES (256 біт)	256	До 6
Twofish	256	До 4
Serpent	256	До 1.5

Враховуючи ці показники, можна побачити, що сучасні симетричні алгоритми комбінують високий рівень безпеки з вражаючою продуктивністю, роблячи їх ефективними для різноманітних застосувань в сучасному цифровому середовищі.

2.1.2. Асиметричні алгоритми шифрування

Асиметричне шифрування є основою безпеки в Інтернеті. Без цього для більшості кіберзлочинців викрасти ваші критично конфіденційні дані так само легко, як забрати цукерку у дитини. Протягом останніх кількох років ми бачили багато болючих нагадувань про витоки даних через прострочені сертифікати SSL/TLS. Простіше кажучи, асиметричне шифрування шифрує та розшифровує дані, які передаються між двома сторонами в загальнодоступних незахищених

каналах (наприклад, в Інтернеті). Цей процес передбачає використання двох окремих, але пов’язаних ключів. Коротше кажучи, це стосується захисту вашої конфіденційної інформації, щоб вона не потрапила в руки неавторизованих користувачів або організацій (наприклад, кіберзлочинців), коли вам потрібно завантажити її на веб-сайт, надіслати електронною поштою тощо.

Асиметричне шифрування також є частиною того, що називається криптографією з асиметричним ключем і криптографією з відкритим ключем, оскільки два ключі, що використовуються, є математично пов’язаними, але унікальними (отже, асиметричними):

- Один ключ, який називається відкритим, оскільки він відомий усім, зазвичай шифрує дані.
- Другий ключ, влучно названий приватним ключем, оскільки він відомий лише власнику ключа, розшифровує дані.



Рис 2.3 Асиметричне шифрування

Асиметричне шифрування можна використовувати для шифрування даних та/або для цифрового підпису даних. Процес, показаний на цьому малюнку, ілюструє використання асиметричної криптографії для шифрування даних. Відверто кажучи, асиметричне шифрування – це термін, який звучить складніше та страшніше, ніж є насправді. Щойно ви зрозумієте основи, уся справа матиме набагато більше сенсу. Але якщо все це трохи важко зрозуміти, уявімо, що у вас є спеціальний сейф, який використовує два замки: один ключ замикає сейф, а інший відкриває його. Так само з асиметричним шифруванням будь-хто, хто має доступ до відкритого ключа, може використовувати його для шифрування даних, але

лише особа, яка має доступ до закритого ключа, може розшифрувати цю інформацію. Асиметричне шифрування лежить в основі структури, відомої як інфраструктура відкритих ключів. Кожна особа, яка використовує асиметричне шифрування, має унікальний закритий ключ. Коли приватний ключ створено, він використовується для визначення так званого відкритого ключа. Кожен приватний ключ відповідає рівно одному відкритому ключу, звідси і фраза «приватно-відкритий ключ». На відміну від симетричного шифрування, обмін приватними ключами не потрібен. Насправді безпека асиметричного шифрування залежить від того, що кожна особа є єдиною особою, яка має доступ до свого приватного ключа. З іншого боку, відкритим ключем можна поділитися з будь-ким. Хоча кожен приватний ключ використовується для отримання точно одного відкритого ключа, неможливо визначити приватний ключ, знаючи відкритий ключ. У нових асиметричних методах шифрування, таких як криптографія на основі еліптичної кривої (ECC) і алгоритми цифрового підпису, для шифрування інформації використовуються самі відкриті ключі. Тоді лише призначений одержувач може розшифрувати цю інформацію за допомогою відповідного закритого ключа. Відкриті ключі по суті діють як відкриті кодові замки — вам не потрібно знати комбінацію, щоб використовувати її для блокування або шифрування повідомлення. Після замикання на замок лише особа, яка знає комбінацію, тобто особистий ключ, може відкрити замок і отримати вміст. В обох випадках проблеми обміну приватними ключами можна уникнути за допомогою асиметричного шифрування. Двом сторонам більше не потрібно надсилати закритий ключ у вигляді звичайного тексту. Мета шифрування полягає в тому, щоб будь-які конфіденційні дані, якими ви хочете поділитися з конкретною особою, зберігалися в таємниці для всіх, окрім одержувача. Це необхідно, тому що ми живемо в час, коли ми обмінюємося та передаємо дані через кілька провайдерів і маршрутизаторів, а також багато миль кабелів під океанами. Історично вам доводилося зустрічатися з кимось віч-на-віч, щоб обмінюватися повідомленнями або секретними ключами, щоб розблокувати майбутнє спілкування. Якщо користувачі не зможуть безпечно обмінюватися ключами для

шифрування своїх даних, будь-хто зможе перехопити передачу даних. Асиметричне шифрування вирішує цю проблему розподілу ключів, створюючи спосіб безпечного обміну ключами без необхідності особисто зустрічатися з іншою стороною.

Шифрування працює шляхом застосування складної математичної формули до ваших оригінальних даних у вигляді звичайного тексту (читабельних), щоб перетворити їх на довгий рядок даних, який неможливо розшифрувати. Отже, якщо ви взяли повідомлення «Я не можу дочекатися початку літа» і зашифрували його за допомогою 2048-бітного відкритого ключа RSA, ви отримаєте шифр, яка виглядає так: “gb7Ty/ZcAz2PQF8wLW28ji3g1znuIjucFkgbSjCvvkfgRWStvz/f4atUi NeLbzoJi/agxRJPGuffzPyEBUf4lwZESWEN+UNQRsqhKrp5dYtVYY+wMaevf7rOB BN8O/lHRdJXUyHgF2nPvjkJsnU1AspAB8llYOyUFyL/0vhfi9DAmT0PoB4a8TKKU PVuZG6WN0L56fXtEtl0sx9QMFPHZNU4EPfE+0H6KB7joGw8livqHACSHYL3r63e PFWh/0qG1s2ZYjf6CWrBghih2HUCJx6IcprA0+UJE7AgJBBLMqOTP53xwwz9sFRF hHRHepWaboxCuUXHNtbiebeB2qfVwg==”.

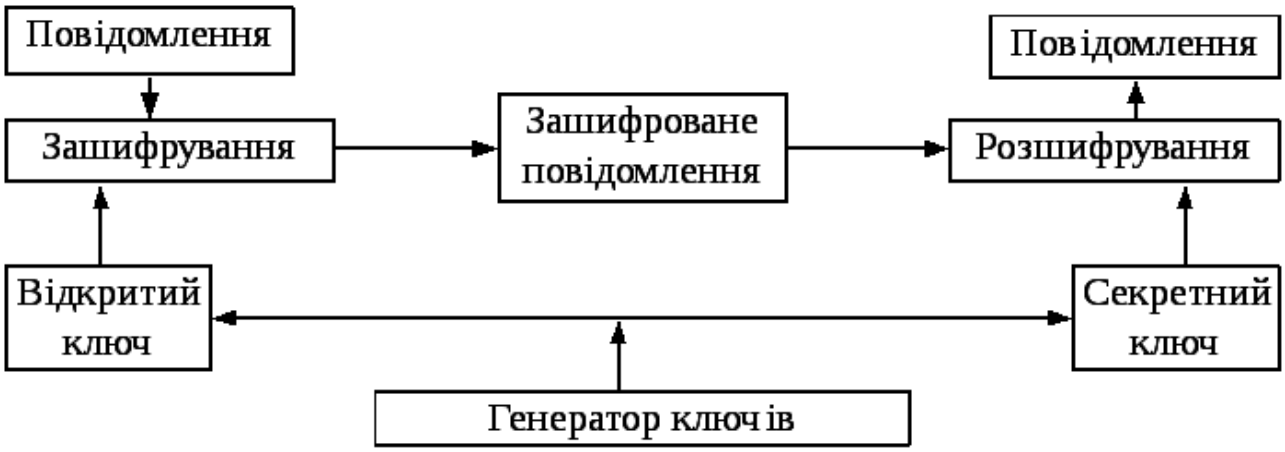


Рис 2.4 Відкритий та секретний ключ

Таблиця 2.2

Швидкість роботи різних асиметричних алгоритмів

Алгоритм	**Розмір ключа (біти)**	**Швидкість (GB/s)**
RSA	2048	До 10
ECC	256	До 6
DSA	2048	До 4
ElGamal	2048	До 1.5

2.1.3. Порівняння різних типів шифрування

Симетричне та асиметричне шифрування - це дві основні категорії криптографічних методів, які використовуються для захисту інформації. Наведемо порівняння цих типів шифрування.

Симетричне шифрування використовує один ключ для як шифрування, так і розшифрування. Ключ повинен бути переданий відправнику та отримувати безпечним шляхом, асиметричне шифрування використовує пару ключів: публічний і приватний. Публічний ключ використовується для шифрування, а приватний - для розшифрування. Кожен користувач має пару ключів.

Симетричне шифрування зазвичай є швидшим, оскільки використовує менше обчислювальних ресурсів. Ідеально підходить для шифрування великих обсягів даних. Асиметричне шифрування зазвичай повільніше, оскільки використовує більше обчислювальних ресурсів. Зазвичай використовується для обміну ключами та підписів.

Симетричне шифрування зазвичай менше стійке до квантових обчислень. При втраті ключа весь процес шифрування та розшифрування стає вразливим. Асиметричне шифрування зазвичай більш стійке до квантових обчислень, адже ключі використовують математичні властивості. Втрата одного ключа не руйнує всю систему.

Симетричне шифрування: Зазвичай використовується для шифрування великих обсягів даних, таких як файли або цілі диски. Асиметричне шифрування: Зазвичай використовується для обміну ключами, підписів та ідентифікації в мережі.

2.1.4. Розрахунок швидкості роботи симетричного та асиметричного алгоритмів шифрування

Порівняємо швидкість роботи симетричного та асиметричного алгоритму шифрування. У першому випадку використаємо алгоритм AES, а у другому випадку RSA.

Розрахунок швидкості роботи для AES-128. Припустимо, ми маємо 16 байт (128 біт) даних. AES-128 використовує 10 раундів. Середній час обробки одного раунду для одного блоку даних може бути приблизно $\frac{1}{10}$ часу на обробку.

Розрахунок загального часу:

$$10 \times (\frac{1}{10}) = 1 \quad (2.1)$$

В цьому прикладі, приблизно 1 одиниця часу на обробку одного блоку AES-128.

Приклад для RSA-2048. Розрахунок часу для одного блоку даних. Припустимо, ми маємо 2048-бітний ключ (256 байт) для RSA. RSA використовує більше часу для шифрування великих обсягів даних порівняно з AES. Середній час обробки одного блоку даних може бути приблизно 2-3 рази більше, ніж час для AES.

Розрахунок загального часу:

$$1 \times 3 = 3 \quad (2.2)$$

В цьому прикладі, приблизно 3 одиниці часу на обробку одного блоку RSA-2048.

Отже симетричний алгоритм шифрування працює швидже, що дозволяє йому мати більшу пропускну здатність.

2.2. Розробка стратегії шифрування

2.2.1. Забезпечення безпеки при передачі даних через інтернет за допомогою протоколу TLS/SSL

Шифрування/дешифрування SSL/TLS (Secure Sockets Layer/Transport Layer Security) — це метод, за допомогою якого захищено підключення до Інтернету, будь то клієнт-клієнт, сервер-сервер або клієнт-сервер. Це запобігає неавторизованим третім сторонам від перегляду або зміни будь-яких даних користувача, якими обмінюються через Інтернет.



Рис 2.5 Рукостискання SSL/TLS

SSL/TLS використовує як асиметричне, так і симетричне шифрування для захисту конфіденційності та цілісності даних, що передаються. Асиметричне

шифрування використовується для встановлення безпечного сеансу між клієнтом і сервером, найбільш часто використовувані алгоритми шифрування з асиметричним ключем включають ELGamal, RSA, DSA, методи еліптичної кривої та PKCS, а симетричне шифрування використовується для обміну даними в межах захищеного сеансу, найпоширенішими симетричними алгоритмами є AES-128, AES-192 і AES-256. Веб-сайт повинен мати сертифікат SSL/TLS для свого веб-сервера/доменного імені, щоб використовувати шифрування SSL/TLS. Після встановлення сертифікат дає змогу клієнту та серверу безпечно погоджувати рівень шифрування, виконавши такі кроки:

- Клієнт зв’язується з сервером за допомогою безпечної URL-адреси (HTTPS…).
- Сервер надсилає клієнту свій сертифікат і відкритий ключ.
- Клієнт перевіряє це за допомогою довіреного кореневого центру сертифікації, щоб переконатися, що сертифікат законний.
- Клієнт і сервер домовляються про найнадійніший тип шифрування, який кожен може підтримувати.
- Клієнт шифрує сеансовий (секретний) ключ відкритим ключем сервера та надсилає його назад на сервер.
- Сервер розшифровує зв’язок клієнта за допомогою свого закритого ключа, і сеанс встановлюється.
- Сеансовий ключ (симетричне шифрування) тепер використовується для шифрування та дешифрування даних, що передаються між клієнтом і сервером.

І клієнт, і сервер тепер використовують HTTPS (SSL/TLS + HTTP) для зв’язку. Веб-браузери підтверджують це за допомогою значка замка в адресному рядку браузера. HTTPS працює через порт 443. Коли ви залишаєте веб-сайт, ці ключі скидаються. Під час вашого наступного візиту обговорюється нове рукостискання та генерується новий набір ключів.

Безпека транспортного рівня (TLS) і його попередник SSL — це протоколи шифрування (процес перетворення даних у формат, який неможливо прочитати

без секретного ключа), які забезпечують безпеку передачі даних через Інтернет. Вони, по суті, шифрують дані, щоб зберегти їх у безпеці під час переміщення між клієнтом і сервером або двома вузлами/кінцевими точками загалом. Однак для мережевих адміністраторів відсутність можливості перевірити цей зашифрований трафік може створити сліпі зони, які можуть приховати кіберзагрози. Кіберзлочинці все частіше використовують зашифрований трафік, щоб приховати свою зловмисну діяльність. Шифрування, призначене для захисту конфіденційності та безпеки даних, також забезпечує зручний щит для кіберзлочинців. Вони використовують зашифровані з'єднання для розповсюдження зловмисного програмного забезпечення, здійснення фішингових атак і непомітного вилучення конфіденційних даних. Це ухилення від традиційних інструментів безпеки є серйозним викликом для фахівців з кібербезпеки. Щоб боротися з цією тенденцією, організації змушені впроваджувати рішення для дешифрування TLS для перевірки та аналізу шифрованого трафіку з метою виявлення прихованих загроз і забезпечення цілісності своїх мереж і даних. Гра в кішки-мишки між кіберзлочинцями та захисниками продовжує розвиватися, підкреслюючи критичну важливість надійних заходів безпеки в сучасному цифровому середовищі.

Власники та оператори мережевої безпеки TLS/SSL отримають численні переваги від досягнення видимості зашифрованого трафіку, що проходить через їхні мережі. Деякі з цих переваг включають:

- Покращена безпека: дешифрування дозволяє організаціям перевіряти та аналізувати зашифрований трафік, допомагаючи виявляти та запобігати таким загрозам, як зловмисне програмне забезпечення, програми-вимагачі та викрадення даних, які можуть ховатися в зашифрованих комунікаціях
- Покращена видимість: дешифрування TLS забезпечує видимість вмісту зашифрованого трафіку, дозволяючи мережевим адміністраторам зрозуміти, які дані передаються, і виявити потенційні проблеми безпеки або порушення відповідності

- Оптимізована оптимізація продуктивності мережі: шляхом моніторингу та аналізу зашифрованого трафіку організації можуть виявляти вузькі місця, помилки та аномалії, які можуть вплинути на продуктивність мережі, що дозволяє здійснювати проактивну оптимізацію
- Швидке усунення несправностей: розшифровка TLS допомагає діагностувати проблеми з продуктивністю мережі та програм, пов’язані із зашифрованим трафіком, допомагаючи IT-командам швидко вирішувати проблеми та скорочувати час простою
- Виявлення загроз і покращене реагування на інциденти: розшифровка трафіку TLS допомагає групам безпеки виявляти розширені загрози та оперативно реагувати, підвищуючи загальні можливості реагування на інциденти
- Запобігання втраті даних: розшифровку TLS можна інтегрувати з рішеннями DLP для моніторингу та запобігання несанкціонованій передачі конфіденційних даних
- Аналіз зловмисного програмного забезпечення: дає змогу організаціям проводити поглиблений аналіз зашифрованого трафіку, щоб ідентифікувати та аналізувати потенційно шкідливий вміст або поведінку.
- Криміналістика та розслідування: розшифровка трафіку TLS може допомогти в розслідуванні цифрової криміналістики, дозволяючи групам безпеки перевіряти історичний трафік на наявність доказів у разі інциденту безпеки.

У чому різниця між SSL та TLS? Secure Sockets Layer (SSL) — це протокол зв'язку або набір правил, що створює безпечне з'єднання між двома пристроями або програмами в мережі. Перш ніж ділитися мандатами або даними через Інтернет, важливо встановити довіру та автентифікувати іншу сторону. SSL — це технологія, яку ваші програми або браузери, можливо, використовували для створення безпечного зашифрованого зв'язку в будь-якій мережі. Однак SSL – це стара технологія, яка містить деякі недоліки щодо безпеки. Протокол TLS – це

оновлена версія SSL, що усуває наявні уразливості SSL. TLS аутентифікується більш ефективно та продовжує підтримувати зашифровані канали зв'язку.

2.2.2. Наскрізне шифрування

Шифрування під час передавання та шифрування в стані спокою сьогодні є стандартними, але цього недостатньо для захисту ваших даних і забезпечення безпечного зв’язку. Коли ваші дані перебувають на сервері, вони вразливі. Як тільки хакер проникає на сервер, він може залишатися там на необмежений час, читаючи ваші повідомлення. На відміну від наскрізного шифрування, єдині люди, які можуть отримати доступ до даних, це відправник і призначений одержувач(и) – ніхто інший. Ні хакери, ні небажані сторонні особи не можуть отримати доступ до зашифрованих даних на сервері. У наскрізному шифруванні відбувається на рівні пристрою. Повідомлення та файли шифруються перед тим, як покинути телефон або комп’ютер, за допомогою відкритого ключа, який доступний кожному, але розшифровуються приватним ключем одержувача лише тоді, коли вони досягають місця призначення. Хакери не можуть отримати доступ до даних на сервері, оскільки вони не мають закритих ключів, необхідних для розшифровки даних. Натомість секретні ключі зберігаються на пристрої окремого користувача та доступні лише одержувачу. Цей процес створення пари відкритий-приватний ключ відомий як асиметрична криптографія. Окремі криптографічні ключі захищають і розшифровують повідомлення. Відкриті ключі широко поширені та використовуються для блокування або шифрування повідомлень. Приватні ключі відомі лише власнику та використовуються для розблокування або розшифровки повідомлення. У наскрізному шифруванні система створює відкритий і приватний криптографічні ключі для кожної особи, яка приєднується.

Щоб краще зрозуміти, як працює наскрізне шифрування, наведемо приклад. Скажімо, Дарина та Артем створюють облікові записи в системі. Система наскрізного шифрування надає кожному пару публічно-приватних ключів, за допомогою яких їхні відкриті ключі зберігаються на сервері, а їхні приватні ключі зберігаються на їхньому пристрої. Дарина хоче надіслати Артему зашифроване

повідомлення. Вона використовує відкритий ключ Артема, щоб зашифрувати своє повідомлення до нього. Потім, коли Артем отримує повідомлення, він використовує свій закритий ключ на своєму пристрої, щоб розшифрувати повідомлення від Дарини. Коли Артем хоче відповісти, він просто повторює процес, шифруючи своє повідомлення Дарини за допомогою відкритого ключа Дарини.

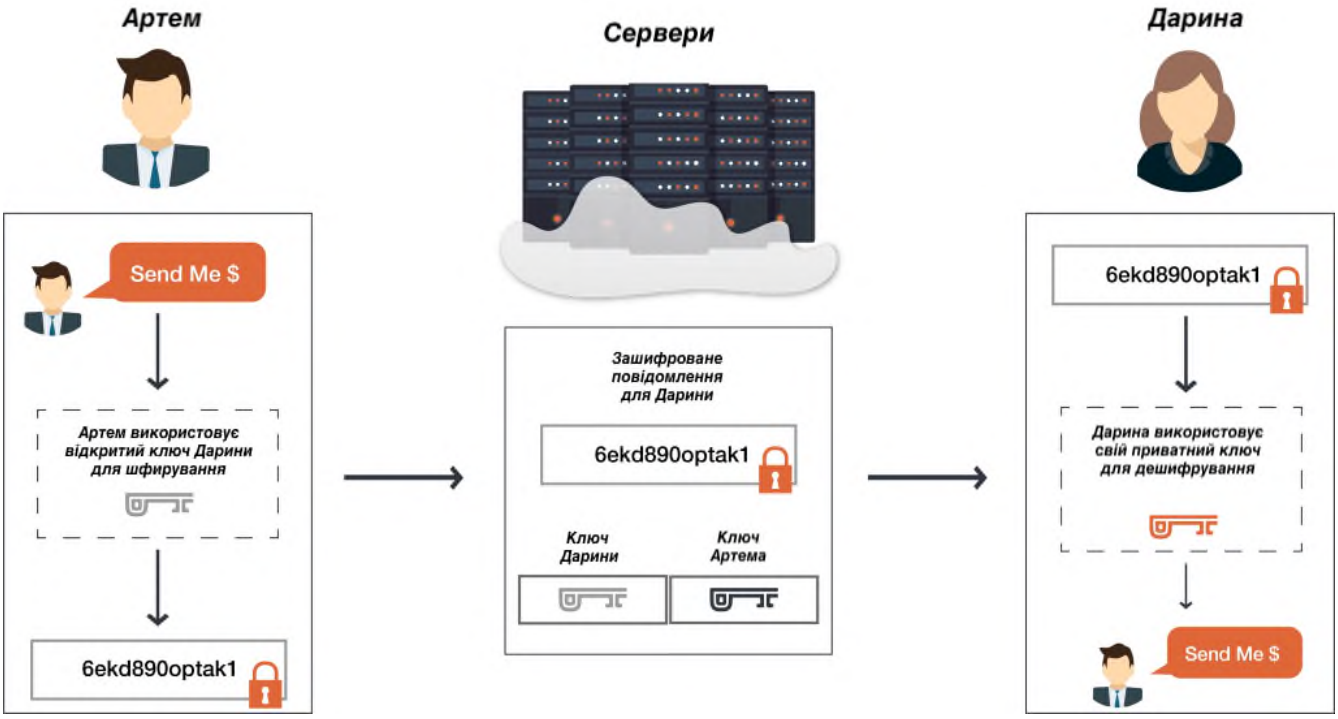


Рис 2.6 Наскрізне шифрування

Як зазначалося раніше, наскрізне шифрування є типом асиметричного шифрування. Асиметричний означає, що для шифрування та дешифрування даних використовуються різні ключі. Наскрізне шифрування зазвичай ґрунтується на використанні відкритих і закритих ключів для забезпечення безпеки та конфіденційності даних. На відміну від цього, симетричне шифрування використовує лише один ключ, наприклад пароль або рядок чисел для шифрування даних. Один і той же ключ використовується як для шифрування, так і для дешифрування даних. Симетричні ключі набагато швидше виконують операції шифрування та дешифрування, ніж асиметричне шифрування. Однак, якщо використовувати його як єдине джерело захисту даних, симетричне шифрування не дуже масштабоване. У міру того, як система росте та додається більше інформації та користувачів, стає все важче розповсюджувати та

оновлювати симетричні ключі. Іншим рішенням шифрування, яке часто використовується, є шифрування даних під час передавання та зберігання. За допомогою шифрування під час передавання (часто TLS) дані шифруються від кінцевої точки до сервера. Однак ці дані є вразливими, оскільки їх легко можуть винюхати хакери, які контролюють шкідливий сервер і використовують цей контроль для викрадення даних. Якщо шифрування не працює, дані можуть бути зашифровані на сервері, але ключі розшифровки цих даних часто знаходяться поблизу, на тому самому сервері або під керуванням централізовано. Слабкий захист ключа представляє єдину точку вразливості та атаки для сервера. Зловмисники часто використовують цю вразливість для програм-вимагачів або для читання та викрадення даних.



Рис 2.7 Різні типи шифрування

Для деяких онлайн-сервісів наскрізне шифрування неможливе. Будь-які служби, які потребують доступу до ваших вихідних даних (наприклад, онлайн-банкінг), не можуть використовувати цей тип шифрування. Але для онлайн-резервного копіювання комп’ютера доступ до вихідних даних не потрібен. Можливість переглядати ваші дані не впливає (або принаймні не повинна) впливати на здатність онлайн-компанії резервного копіювання обслуговувати вас.

Їх робота полягає в тому, щоб надійно зберігати ваші дані та повертати їх, коли ви їх запитуєте. Нічого більше і не менше. Наскрізне шифрування та SSL – не єдині позиції щодо конфіденційності даних, які може зайняти компанія. Є багато інших між ними. Однією з таких позицій, що стосується резервного копіювання комп'ютера, є наскрізне шифрування зі спільним володінням ключем. У ньому ви розміщуєте свої дані всередині іншої скриньки. Але замість того, щоб зберігати ключ від внутрішньої скриньки замка, ви ділитеся ним з одержувачем. Таким чином, хоча одержувач все ще має два ящики між ними та вашими даними, він також має можливість відкрити обидва. Спочатку це може здатися так, ніби він не забезпечує додаткової конфіденційності через SSL. Це неправда. По-перше, наявність другої скриньки (навіть якщо ключ є спільним) дійсно допоможе. Але що ще важливіше, компанії, які пропонують наскрізне шифрування зі спільним володінням ключем, часто вживають особливих заходів, щоб захистити ключ від внутрішньої коробки замка. Наприклад, лише довірені співробітники адміністратора можуть мати доступ до цього ключа.

2.2.3. Шифрування кінцевого вузла

Шифрування даних на кінцевих вузлах є важливою складовою сучасних стратегій кібербезпеки. Цей процес дозволяє захистити конфіденційні дані, зберігаючи їх в безпечній формі під час зберігання або передачі через мережі.

Шифрування даних на кінцевому вузлі гарантує, що інформація залишається безпечною, навіть якщо пристрій потрапить у руки несанкціонованої особи. Тільки користувач, який володіє правильним ключем чи паролем, може розшифрувати та отримати доступ до даних. Запобігає можливим атакам, таким як перехоплення даних або вторгнення в систему. Зашифровані дані важко читати без відповідного ключа, навіть якщо зловмисники отримають фізичний чи віртуальний доступ до пристрою. Воно гарантує конфіденційність даних, забезпечуючи, що лише авторизовані користувачі можуть отримати доступ до важливої інформації. Це стає важливою частиною дотримання регуляторних вимог та захисту особистої інформації. Шифрування на кінцевому вузлі

використовує сучасні шифрувальні алгоритми, які гарантують високий рівень безпеки. Розвиток криптографії сприяє появі нових методів шифрування, які стійкі до сучасних кіберзагроз. Сучасні методи шифрування на кінцевих вузлах надають ефективний захист, не суттєво впливаючи на продуктивність пристрою чи швидкість обробки даних. Вони забезпечують баланс між безпекою та зручністю використання. Шифрування на кінцевому вузлі надає переваги для мобільних пристроїв, де дані можуть передаватися через відкриті мережі. Це особливо важливо для облікових записів, паролів та іншої чутливої інформації, яку користувачі можуть зберігати на своїх смартфонах чи планшетах.

Шифрування кінцевого вузла - це ключовий аспект в будь-якій стратегії кібербезпеки. Захищаючи дані на рівні пристрою, ви створюєте надійний бар'єр для потенційних загроз, зберігаючи конфіденційність та цілісність інформації. З розвитком технологій шифрування та підходів до захисту даних, користувачі можуть спокійно користуватися своїми пристроями, знаючи, що їх особиста інформація залишається в безпеці. Правильне впровадження та управління шифруванням на кінцевих вузлах є критичним елементом сучасного цифрового життя.

3 ПОБУДОВА МЕРЕЖІ З ВИКОРИСТАННЯМ СУЧАСНИХ МЕТОДІВ ШИФРУВАННЯ

1.3 Огляд доступних рішень для впровадження TLS/SSL

Додавання SSL/TLS до вашого веб-сайту є важливим заходом для забезпечення безпеки передачі даних між клієнтами та сервером. Існує кілька рішень та підходів, які можна використовувати для цього:

- Використання Безкоштовних SSL/TLS Сертифікатів. Деякі сервіси надають безкоштовні SSL/TLS сертифікати та має простий інструментарій для їх автоматичного оновлення. Доцільно для більшості веб-сайтів.
- Платні SSL/TLS Сертифікати. Comodo, Symantec, DigiCert: Компанії, які надають комерційні SSL/TLS сертифікати. Придатно для корпоративних та великих проектів, де потрібен розширений набір функцій.
- Хмарні Постачальники SSL/TLS. Cloudflare, AWS Certificate Manager, Azure SSL, Google Cloud: Деякі хмарні постачальники пропонують свої сервіси SSL/TLS, що спрощує процес налаштування та оновлення.

Обираючи як AWS, так і Google Cloud для створення SSL-сертифікатів, можна враховувати кілька важливих аспектів, які можуть бути ключовими при виборі постачальників хмарних послуг та інфраструктури. Давайте розглянемо деякі причини, які можуть вас підтримати в цьому виборі. Обидві платформи надають широкі можливості гнучкості та можливості резервування ресурсів, що може бути корисним при оптимізації витрат. AWS та Google Cloud відомі своєю високою масштабованістю та швидкодією. Це важливо для проектів, які планують зростати та потребують великого обсягу ресурсів. AWS має сервіс AWS Certificate Manager (ACM), а Google Cloud пропонує своє рішення. Обидва сервіси дозволяють легко отримувати та управляти SSL-сертифікатами на своїх платформах. AWS і Google Cloud надають багато інших сервісів, таких як сховища даних, бази даних, інструменти моніторингу, які можуть бути важливими для вашого проекту. Обидві платформи мають глобальні мережі, що дозволяє ефективно обслуговувати клієнтів з різних регіонів світу.

Цінова політика для SSL/TLS сертифікатів на Amazon Web Services (AWS) та Google Cloud може варіюватися в залежності від кількох факторів, таких як тип сертифіката, термін його використання, відомий бренд чи безплатний сервіс, як Let's Encrypt. Нижче наведено загальний порівняльний огляд для обох платформ:

- AWS Certificate Manager. Безкоштовні Сертифікати: ACM надає безкоштовні сертифікати для використання на AWS-ресурсах, таких як Elastic Load Balancer (ELB) та Amazon CloudFront. Якщо вам потрібно використовувати сертифікати в інших місцях, ви можете придбати та імпортувати комерційні сертифікати в AWS, використовуючи сервіс IAM (Identity and Access Management).
- Google Cloud SSL/TLS Proxy: Платна послуга: використання SSL/TLS проксі в Google Cloud є платною послугою. Вартість може залежати від кількості переданих даних, кількості конфігурацій SSL та інших факторів. Let's Encrypt на Google Cloud: Якщо ви хочете безкоштовний сертифікат, ви можете використовувати Let's Encrypt. В Google Cloud є інструкції, як налаштувати Let's Encrypt на своєму веб-сервері на віртуальній машині.

2.3 Впровадження шифрування на основі протоколу SSL/TLS на базі AWS (Amazon Web Services)

Розглянемо забезпечення шифрування при передачі даних через мережу інтернет за допомогою протоколу SSL/TLS на базі AWS з використанням EC2 (Elastic Compute Cloud).

Спочатку нам потрібно отримати безкоштовний сертифікат від менеджера сертифікатів AWS. Для цього відкриємо вікно “Менеджер Сертифікатів” та натиснемо кнопку генерації сертифікату.

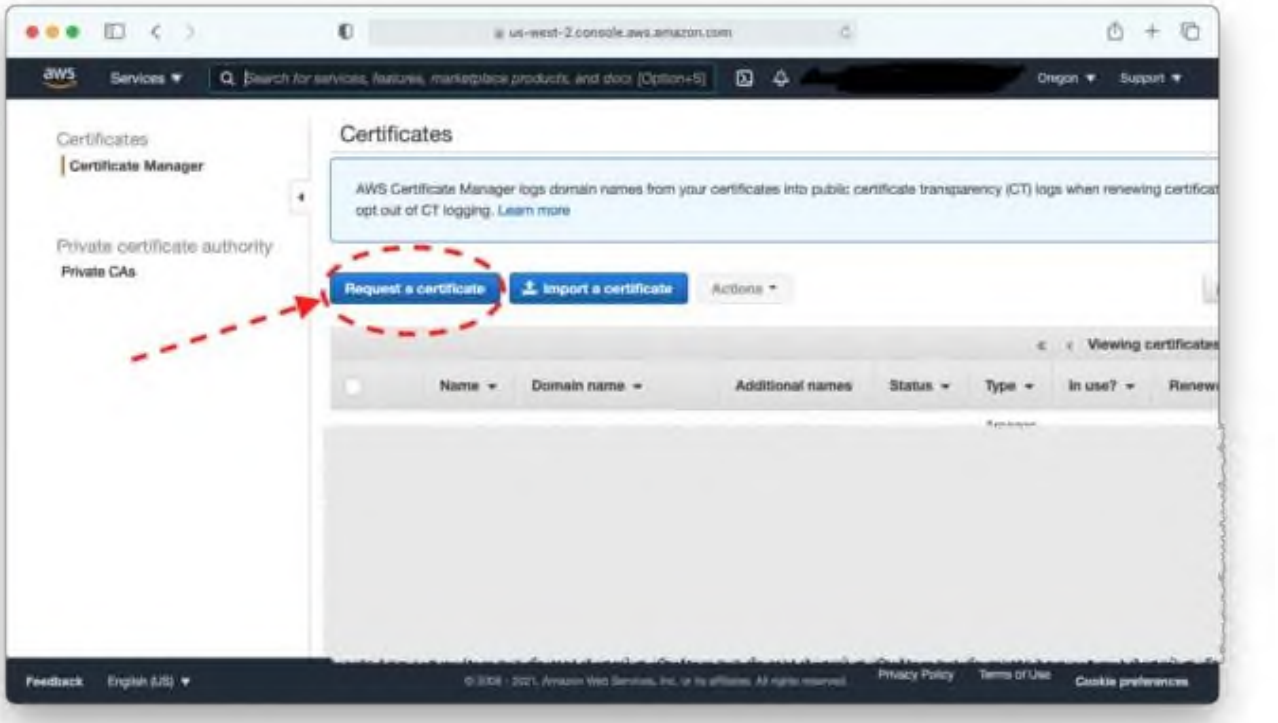


Рис 3.1 Менеджер сертифікатів AWS

Вибираємо Загальнодоступний сертифікат і натискаємо запит на сертифікат

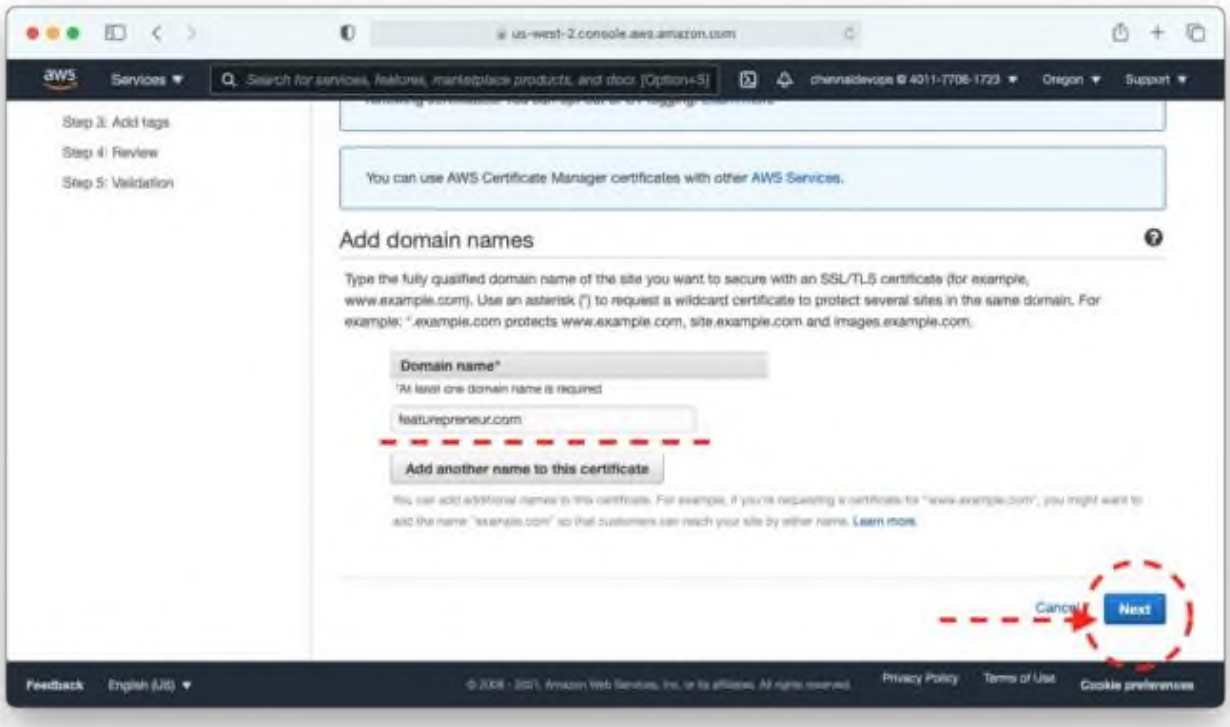


Рис 3.2 Запит на сертифікат

У наступному вікні вводимо ім’я нашого домену. Тепер перевіряємо всі деталі, якщо вони правильні, підтверджуємо та надсилаємо запит.

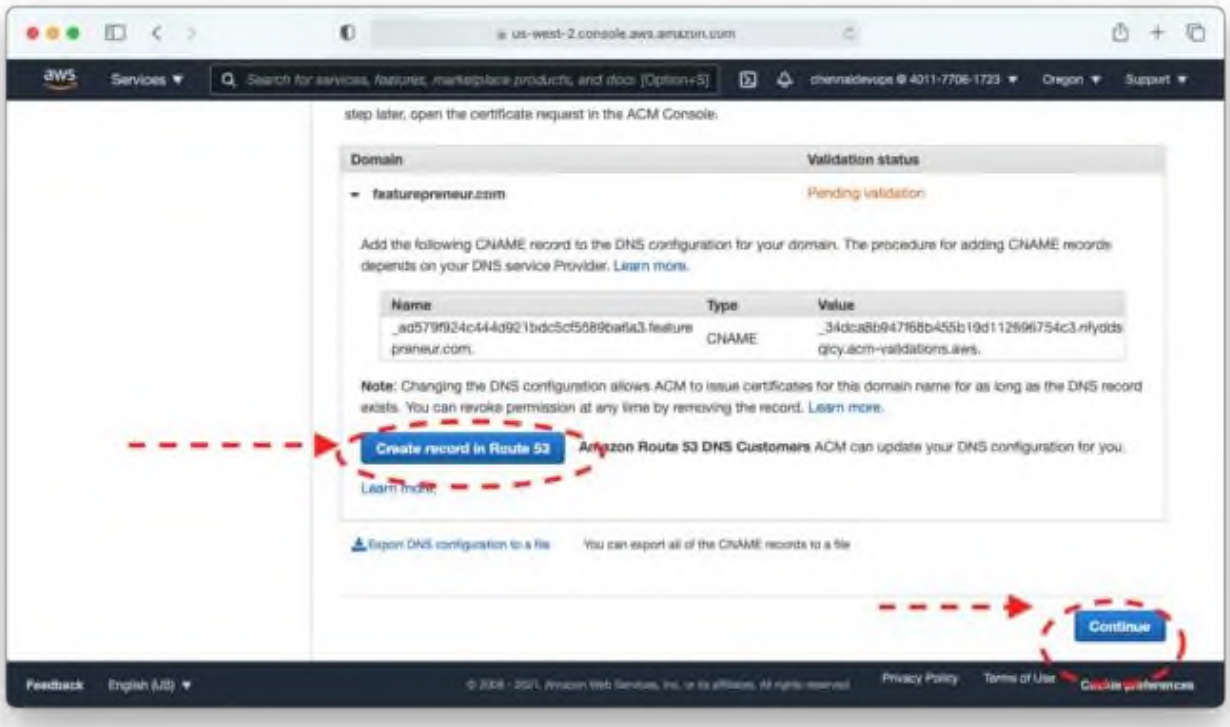


Рис 3.3 Надсилання запиту для отримання сертифікату

AWS підтримує кілька сервісів, де можна встановити SSL-сертифікат, наприклад Amazon Elastic Load Balancer (ELB), Amazon CloudFront або веб-сервер (наприклад, Apache або Nginx). В цій роботі ми додамо сертифікат для ELB, таким чином схема роботи нашої мережі буде виглядати наступним чином.

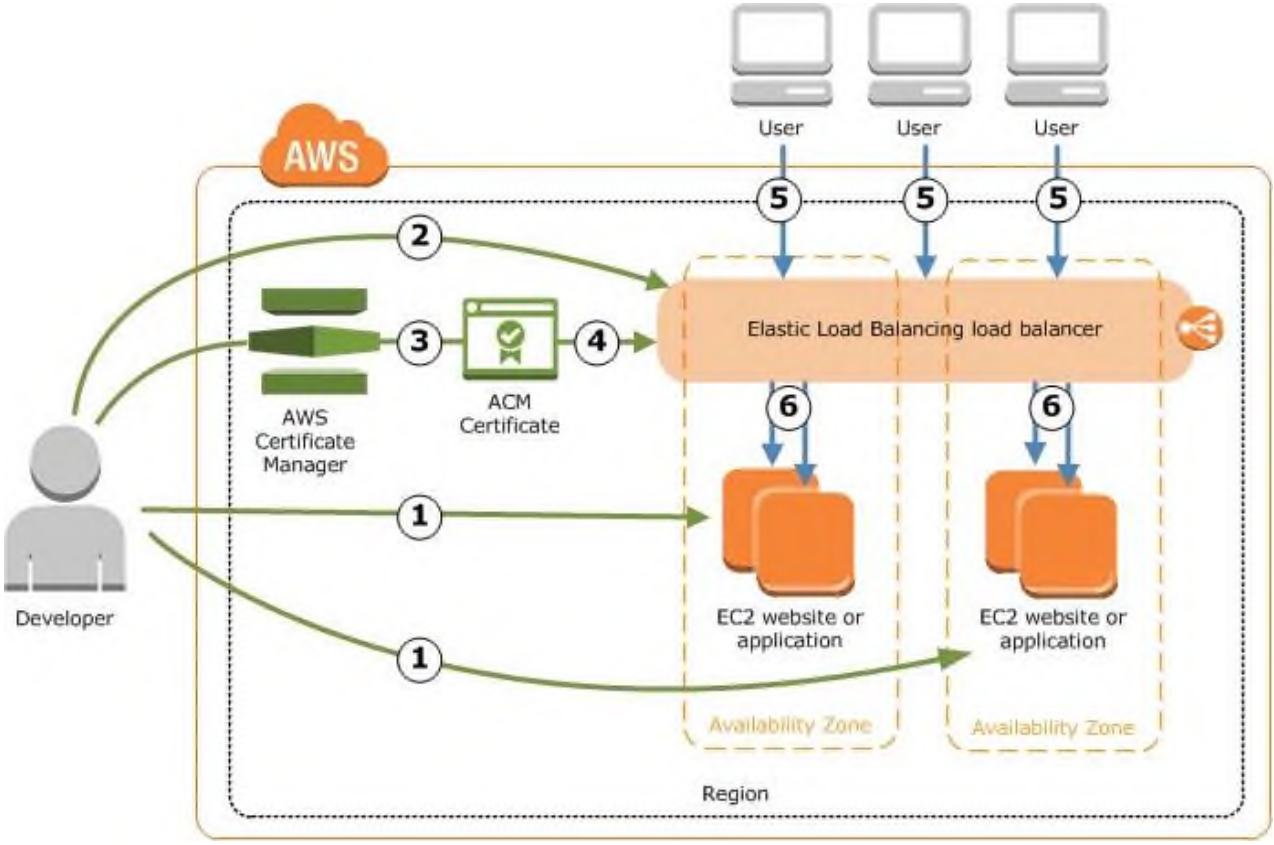


Рис 3.4 Схема побудови мережі з використанням ELB та SSL/TLS сертифікату

Для цього нам потрібно створити ELB.

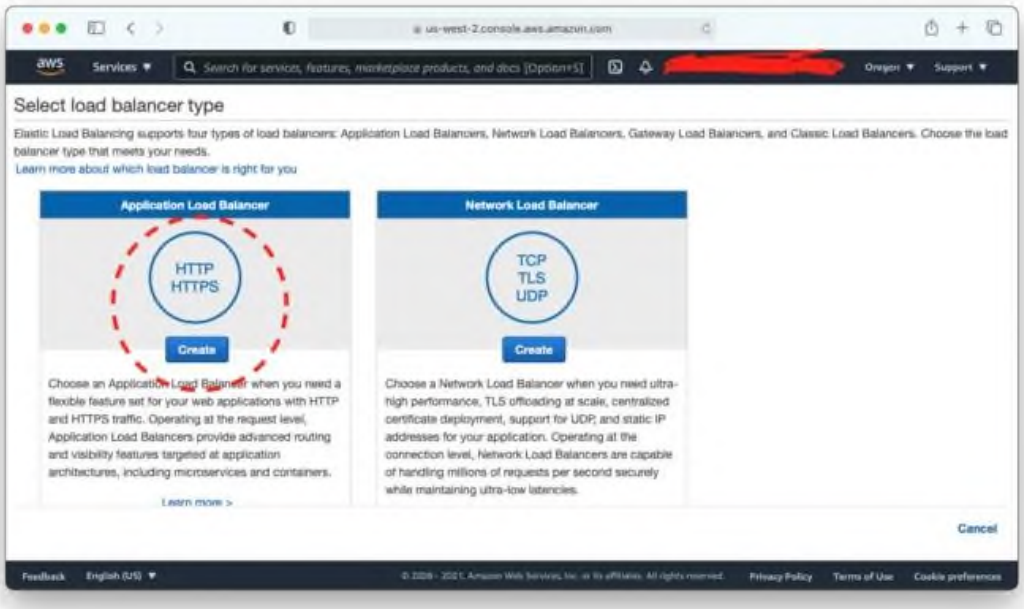


Рис 3.5 Створення https ELB

Після цього нам треба додати прослуховувач подій на 443 порт, так як HTTPS працює через цей порт. Обираємо «Вибрати сертифікат із ACM», та щойно отриманий сертифікат і натискаємо «Далі».

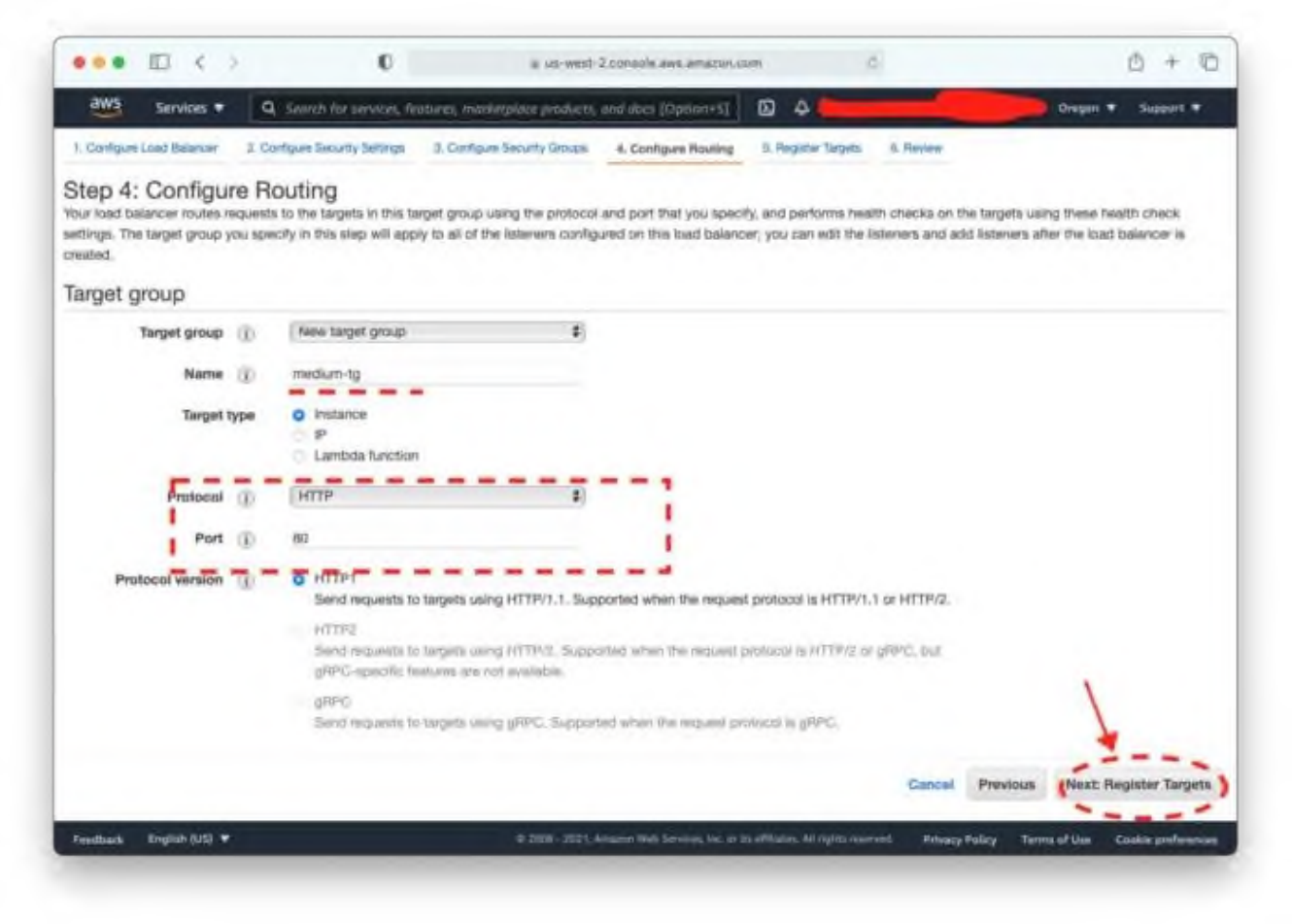


Рис 3.6 додавання сертифікату на ELB

Після цих кроків наш веб-сервер повинен працювати з використанням SSL/TLS, забезпечуючи зашифровану передачу даних між клієнтами та вашим сервером EC2.

2.4 Впровадження шифрування на основі протоколу SSL/TLS на базі Google Cloud

Ви можете створити сертифікат, яким керує Google, до, під час або після створення балансувальника навантаження. У процесі створення балансувальника навантаження в консолі Google Cloud ви можете використовувати консоль Google Cloud, щоб створити свій сертифікат. Крім того, ви можете створити сертифікат до або після створення балансувальника навантаження.

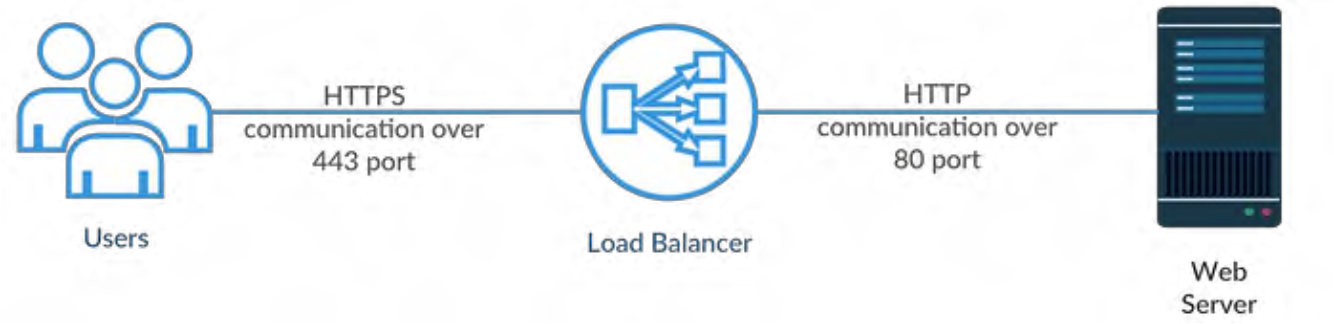


Рис 3.7 Схема побудови мережі на основі Google Cloud

Ви можете працювати з глобальними сертифікатами SSL на вкладці Classic Certificates на сторінці Certificate Manager:

- Перейдіть на вкладку Classic Certificates на консолі Google Cloud.
- Перейдіть до класичних сертифікатів
- Натисніть Створити сертифікат SSL.
- Введіть назву та необов'язковий опис сертифіката.
- Виберіть Створити сертифікат, керований Google.
- Додайте домени.
- Натисніть Створити.

Створюємо балансир навантаження. Щоб стати активним, сертифікат SSL, яким керує Google, має бути пов'язано з балансувальником навантаження, зокрема з цільовим проксі-сервером балансувальника навантаження.

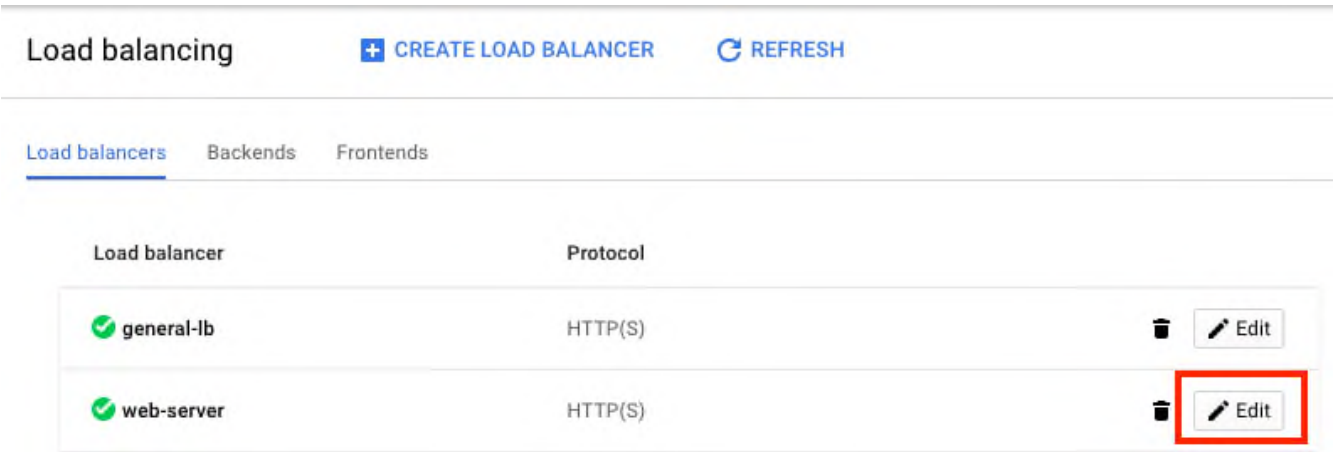


Рис 3.8 налаштування балансувальника навантажень

Після цього слід виконати кроки зазначені нижче:

- Переходимо до конфігурації інтерфейсу
- Додаємо IP-адресу та порт інтерфейсу
- Обираємо протокол як HTTPS
- Розкриваємо список «Сертифікат» і натискаємо «Створити новий сертифікат».

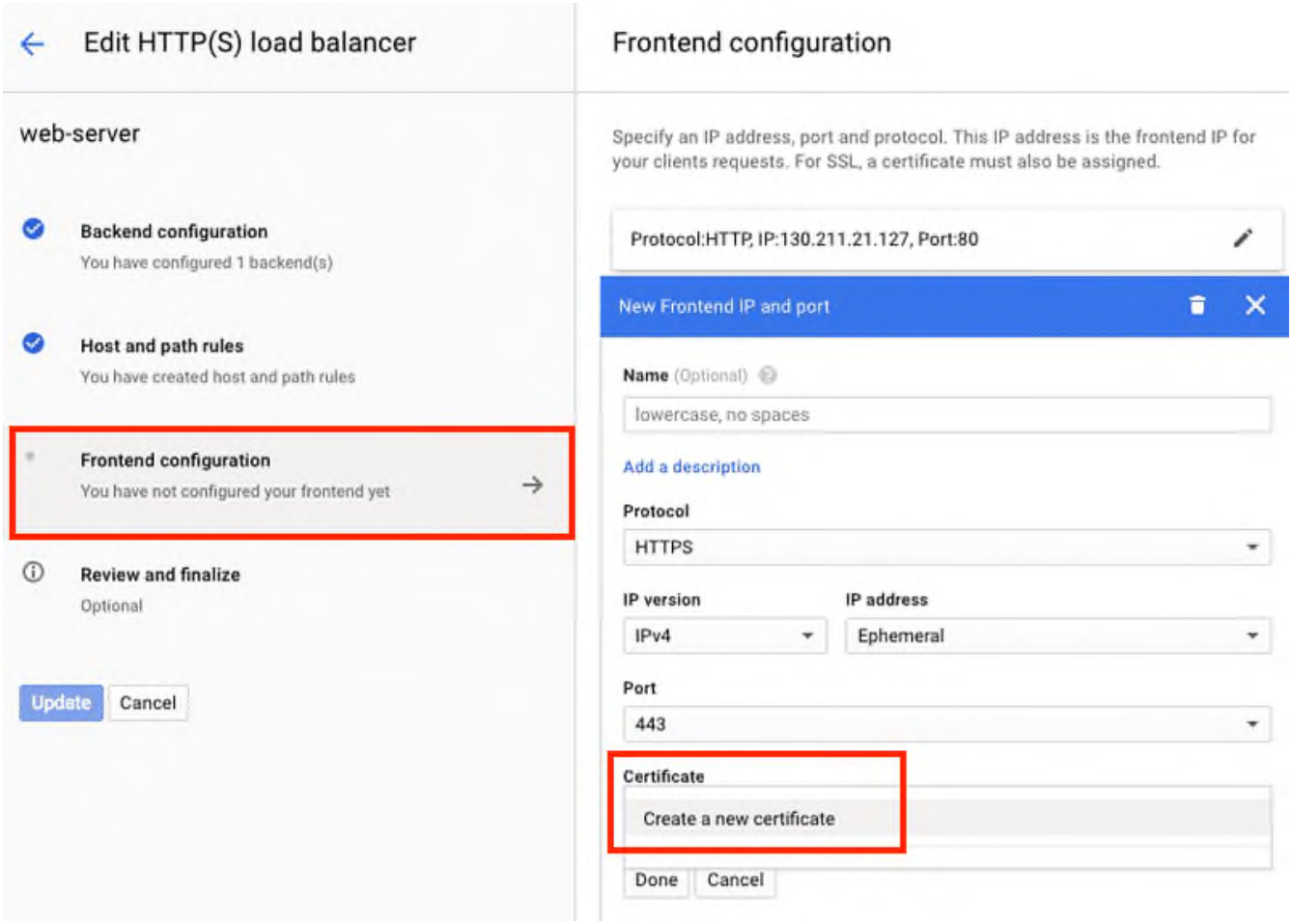


Рис 3.9 Створення SSL сертифікату

Після цього нам потрібно отримати CSR (запит на підписання сертифіката). Тепер нам потрібно надіслати CSR до центру сертифікації, щоб підписати його. Я використовую Let’s Encrypt, щоб підписати свій сертифікат, увівши ці дані та натиснувши «створити».

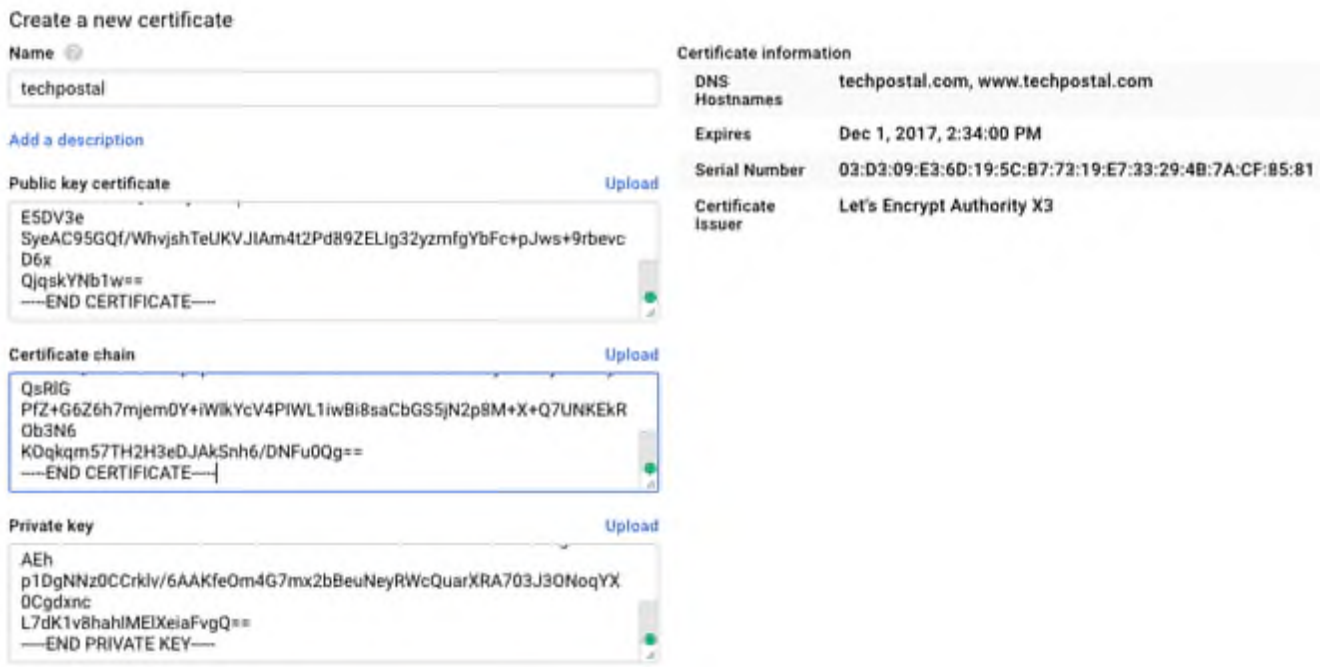


Рис 3.11 Підписання сертифікату

У наступному вікні натискаємо «Готово», а потім «Оновити».

Використовуючи Google Cloud Load Balancer із підтримкою SSL, ми гарантуємо безпеку та конфіденційність передачі даних між клієнтами та нашими віртуальними машинами. Застосування такого заходу безпеки є ключовим для відповіді на сучасні виклики в галузі кібербезпеки та створення довіри серед користувачів.

2.4 Впровадження шифрування на основі протоколу SSL/TLS на базі Microsoft Azure

Ви можете додати цифрові сертифікати безпеки для використання в коді програми або для захисту настроюваних DNS-імен у службі додатків Azure, яка надає високомасштабовану послугу веб-хостингу з самовиправленням. Ці приватні або загальнодоступні сертифікати, які зараз називаються сертифікатами безпеки транспортного рівня (TLS), також раніше відомими як сертифікати рівня захищених сокетів (SSL), допомагають захистити підключення до Інтернету шляхом шифрування даних, що надсилаються між вашим браузером, веб-сайтами, які ви відвідуєте, і сервером веб-сайтів.

Безкоштовний керований сертифікат App Service — це готове рішення для захисту вашого власного імені DNS у App Service. Без будь-яких дій з вашої сторони цим сертифікатом сервера TLS/SSL повністю керує Служба додатків і він автоматично поновлюється з кроком у шість місяців, за 45 днів до закінчення терміну дії, якщо попередні умови, які ви налаштували, залишаються незмінними. Усі пов’язані прив’язки оновлюються разом із оновленим сертифікатом. Ви створюєте та прив’язуєте сертифікат до спеціального домену, а служба додатків зробить все інше.

Для створення та додавання сертифікату нам потрібно На порталі Azure у меню ліворуч вибрати пункт “Служби програм” та обрати назву програми. У навігаційному меню програми обираємо Сертифікати. На панелі Керовані сертифікати обираємо “додати сертифікат”.

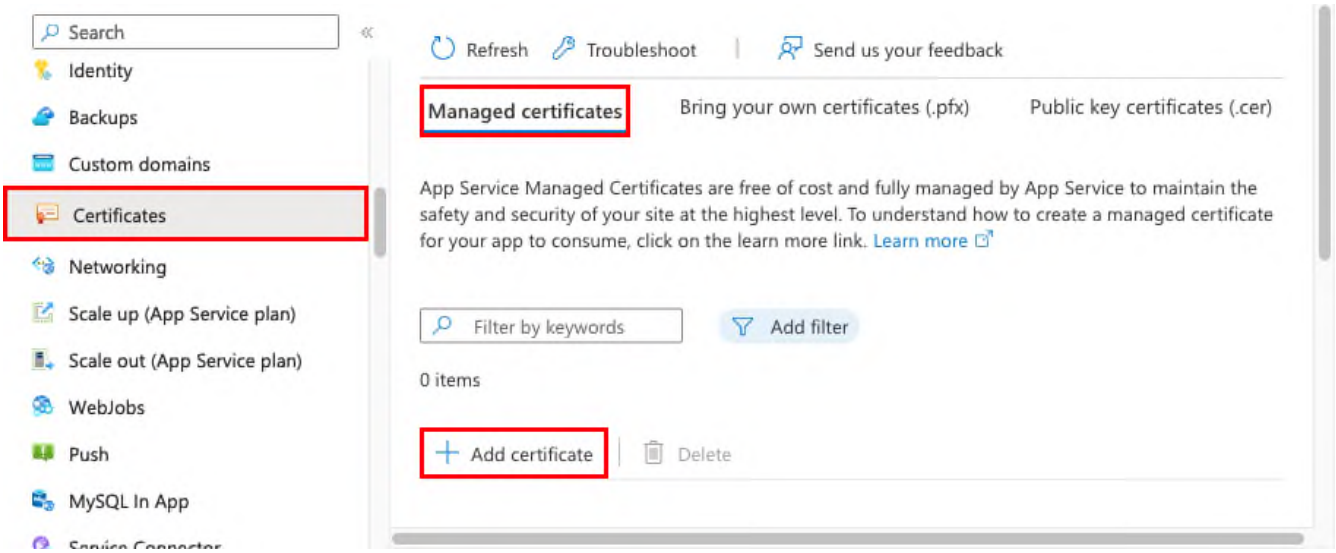


Рис 3.12 Додавання сертифікату

Обираємо домен для безкоштовного сертифіката, а потім натискаємо кнопку “перевірити”. Після завершення перевірки оберіть “додати”. Ви можете створити лише один керований сертифікат для кожного підтримуваного спеціального домену. Після завершення операції сертифікат з’явиться у списку керованих сертифікатів.

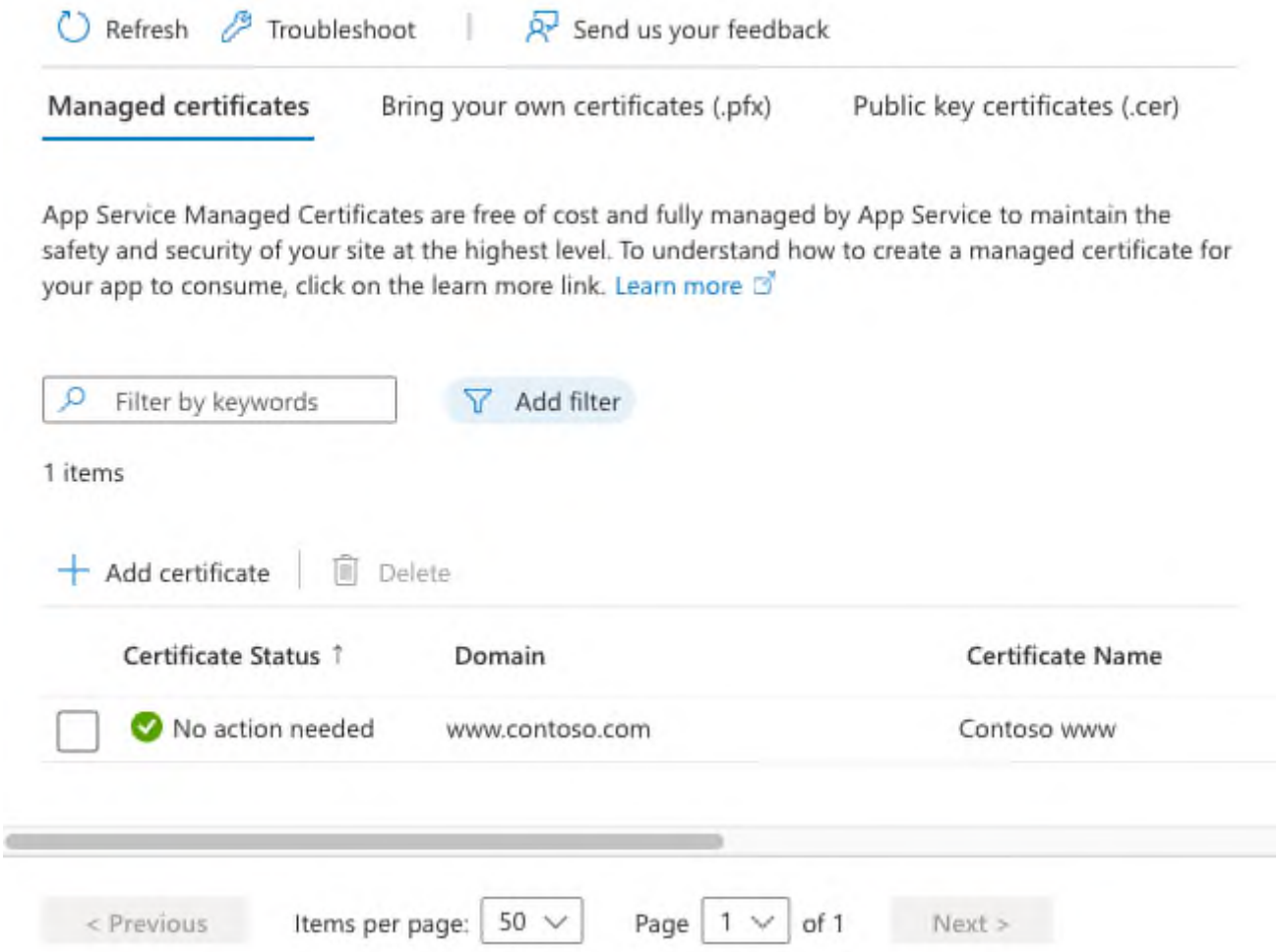


Рис 3.13 Список керованих сертифікатів

Щоб захистити власний домен за допомогою цього сертифіката, нам все одно потрібно створити прив’язку сертифіката. Щоб імпортувати сертифікат App Service, спочатку налаштуємо сертифікат App Service:

- На порталі Azure у меню ліворуч обира Служби програм.
- У навігаційному меню програми обираємо сертифікати.
- У «Джерело» обрали «Імпортувати сертифікат служби програми».
- У сертифікаті служби додатків виберемо щойно створений сертифікат.
- У розділі «Зрозуміле ім’я сертифіката» даємо сертифікату ім’я у своїй програмі.
- Обираємо Перевірити. Коли перевірка пройде успішно, натискаємо “додати”.

Коли операцію буде завершено, сертифікат з’явиться у списку власних сертифікатів.

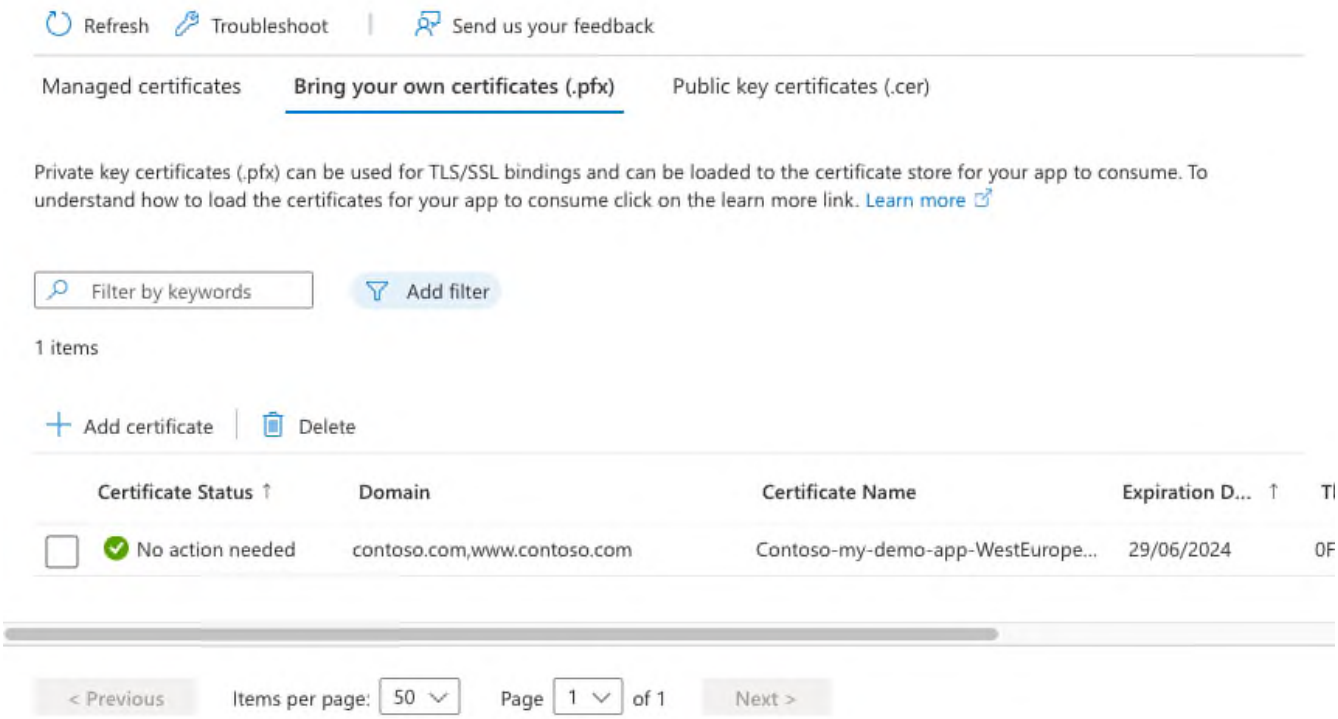


Рис 3.14 Список власних сертифікатів

Додавання SSL/TLS сертифікату до веб-додатку на Microsoft Azure — це важливий етап для забезпечення безпеки передачі даних. Використання Azure Key Vault для зберігання та управління сертифікатами сприяє безпеці та ефективності. Налаштування веб-додатку в Azure App Service дозволяє вам легко інтегрувати SSL/TLS сертифікат та активувати підтримку безпечного протоколу на вашому веб-сайті. Додаткові опції, такі як використання Azure Application Gateway чи Azure Front Door, дозволяють додатково керувати розподіленим трафіком та застосовувати SSL/TLS для оптимізації продуктивності. Важливо регулярно оновлювати сертифікати та вчасно оновлювати їх в Azure Key Vault для забезпечення безпеки та дійсності. Загальний підхід дозволяє ефективно і безпечно впроваджувати заходи забезпечення на Microsoft Azure.

2.5 Тестування та оцінка ефективності

Ефективна оцінка шифрування SSL/TLS включає в себе ряд кроків та аспектів, щоб переконатися, що ваші шифри та налаштування відповідають високим стандартам безпеки. Нижче наведено деякі рекомендації для ефективної оцінки шифрування SSL/TLS:

- Перевірка версії протоколу. Перегляньте, які використовуються найновіші версії протоколу TLS (наприклад, TLS 1.2 або TLS 1.3), оскільки вони мають більшу стійкість і безпеку разом зі старішими версіями SSL/TLS.
- Вибір Сильних Шифрів. Використовуйте сильні шифри, які відповідають сучасним стандартам безпеки. Виключіть застарілі та вразливі шифри.
- Сертифікат та Ключовий Обмін. Використовуйте сертифікати від надійних постачальників та переконайтеся, що ваш приватний ключ захищений та не піддавався компрометації.
- Вимкнення Застарілих Протоколів. Вимкніть старі версії протоколів SSL та старі шифри, такі як DES чи RC4, які можуть бути вразливими до атаки.
- HTTP Strict Transport Security (HSTS). Встановіть HTTP Strict Transport Security, щоб дозволити клієнтам використовувати захищене з'єднання в течії фіксованого періоду часу
- Ідеальна передня секретність (PFS). Щоб забезпечити PFS, якщо навіть у разі компрометації приватного ключа минулого сеансу, інші активи залишаються безпечними.
- Оцінка Відкритих Уразливостей. Використовуйте інструменти сканування безпеки, такі як Qualys SSL Labs чи SSLyze, щоб перевірити ваш сервер на наявність вразливостей та параметрів оптимізації.
- Регулярні Оновлення та Перевірки. Регулярно оновлюйте SSL/TLS бібліотеки та перевіряйте налаштування для врахування нових вразливостей та стандартів безпеки.

- Логування та Моніторинг. Забезпечте належне логування подій, пов’язаних із SSL/TLS, та встановіть систему моніторингу для часового виявлення аномалій чи атак
- Документація та Внутрішня Політика. Здійсніть налаштування документа SSL/TLS та визначте внутрішню політику безпеки для їх впровадження та моніторингу.

ВИСНОВКИ

У світлі нестримного розвитку телекомунікаційних технологій та постійного зростання кількості кіберзагроз, створення та впровадження ефективних систем безпеки в телекомунікаційних мережах стає надзвичайно важливим завданням.

У магістерській роботі виконано аналіз сучасних кіберзагроз, а також методи забезпечення безпеки в телекомунікаційних мережах. Основним методом безпеки було обрано шифрування, а саме впровадження безпеки на основі протоколу SSL, була виконана побудова мережі на основі провайдерів хмарних обчислень таких як AWS та Google Cloud.

Актуальність даного дослідження визначається не лише наявністю загроз, але й швидким темпом змін у кіберпросторі, які вимагають постійного оновлення та вдосконалення методів захисту. Створення безпеки в телекомунікаційних системах залежить від вивчення та впровадження передових методів шифрування. Використання сучасних стандартів, таких як Advanced Encryption Standard (AES), та асиметричних алгоритмів гарантує високий рівень стійкості та конфіденційності даних. Методика створення та впровадження систем безпеки передбачає широкий спектр заходів, включаючи аудит існуючих систем, вибір оптимальних засобів шифрування, встановлення інтегрованих систем моніторингу та постійне оновлення технічної інфраструктури. Здійснене дослідження спрямоване на визначення найефективніших стратегій безпеки в телекомунікаційних мережах та встановлення фундаментальних принципів для їх впровадження. Невпинний аналіз та вдосконалення систем безпеки є крайньою необхідністю для забезпечення надійності та стабільності телекомунікаційних середовищ у світлі сучасних викликів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. П.Н. Девянин. - М.: Радио и связь, 2006. - 176 с.
2. Информатика. Новый систематизированный толковый словарь. Ф.С. Воройский. 2003. - 365 с.
3. Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. Cryptography Engineering: Design Principles and Practical Application Cryptography Engineering: Design Principles and Practical Applications, 2010 - 384 с.
4. William Stallings. Network Security Essentials. 2017 - 560 с.
5. Rolf Oppliger. SSL and TLS: Theory and Practice. 2009 - 424 с.
6. Jean-Philippe Aumasson. Serious Cryptography: A Practical Introduction to Modern Encryption. 2017 - 336 с.
7. Christof Paar, Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. 2009 - 368 с.
8. Основы построения виртуальных частных сетей. Запечников С.В., Милославская Н.Г., Толстой А.И. 2011
9. Nortel Guide to VPN Routing for Security and VoIP. Джеймс Єдвардс і Річард Браманте. 2006.
10. Виртуальные частные сети VPN. Александр Росляков. 2011.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

МАГІСТЕРСЬКА РОБОТА

на тему:

МЕТОДИКА СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ СИСТЕМ БЕЗПЕКИ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ НА ОСНОВІ СУЧАСНИХ МЕТОДІВ ШИФРУВАННЯ

Виконав: студент групи ТСДМ-63
Іщенко І.Є.
Керівник роботи: к.т.н., доцент, директор ННІТ
Кравченко В.І.

Мета та завдання

Мета роботи – визначення та дослідження основних типів кіберзагроз та методика та методика створення систем безпеки в телекомунікаційних мережах.

Об'єкт дослідження – системи безпеки в телекомунікаційних мережах.

Предмет дослідження – сучасні методи шифрування та їх впровадження.

Завдання до дипломної роботи:

1. Аналіз перспектив та особливостей застосування сучасних методів шифрування
2. Дослідження сучасних типів кіберзагроз;
3. Дослідження сучасних методів шифрування;
4. Реалізація захищеної мережі на основі протоколу SSL;

Захист Мережі

У сучасному інформаційному суспільстві, де телекомунікаційні мережі стали невід'ємною частиною нашого повсякденного життя, питання забезпечення безпеки цих мереж виявляється крайньою актуальністю. З кожним днем обсяги передачі даних у мережах та їх важливість для функціонування суспільства зростають, а це робить сучасні телекомунікаційні системи метою для різноманітних кіберзагроз. За таких обставин, розробка та впровадження ефективних систем безпеки в телекомунікаційних мережах стає необхідністю. Одним із ключових елементів таких систем є сучасні методи шифрування, які вирішують завдання надійного захисту конфіденційності, цілісності та доступності переданих даних.



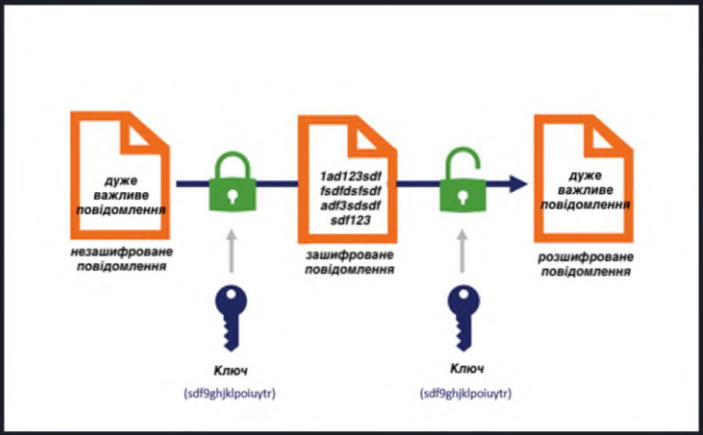
Огляд сучасних методів шифрування

За своєю суттю шифрування — це процес, який перетворює читабельні дані, відомі як відкритий текст, у нечитабельний формат, який називається зашифрованим текстом. Це перетворення досягається за допомогою складних алгоритмів і ключа. Ключ, який може бути рядком випадкових чисел і літер, використовується для дешифрування зашифрованого тексту назад у відкритий текст. Це гарантує, що навіть якщо дані перехоплено під час передачі, вони залишаються незрозумілими для будь-кого без ключа дешифрування.



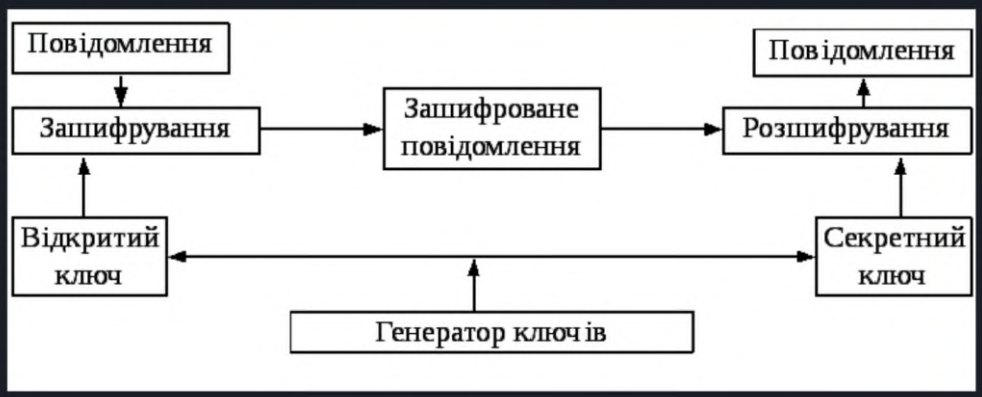
Симетричне шифрування

Симетричне шифрування — це тип шифрування, який використовує той самий ключ для шифрування та розшифрування даних. І відправник, і одержувач мають ідентичні копії ключа, які вони зберігають у секреті та нікому не діляться.
Прикладами алгоритмів з симетричним шифруванням є AES, Twofish, Serpent

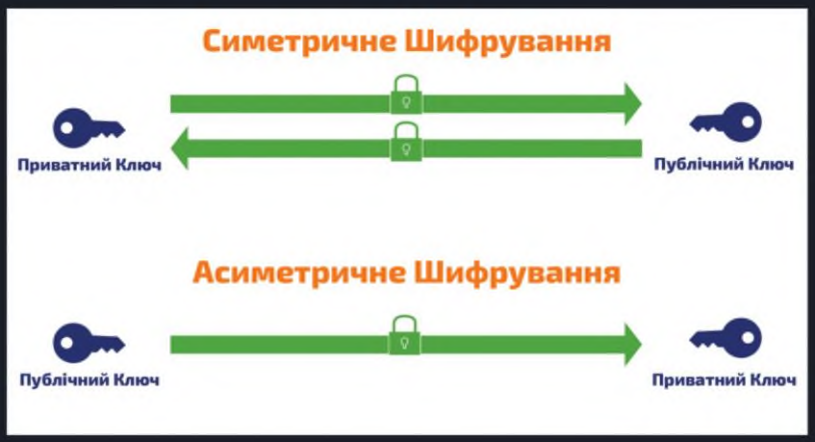


Асиметричне шифрування

Асиметричне шифрування - набір методів криптографічного шифрування, в яких використовують два ключі - таємний(приватний) і відкритий. Алгоритми асиметричного шифрування, так само як і симетричного, застосовують для шифрування масивів даних, але їхня швидкість значно нижча. Основне призначення асиметричних алгоритмів - забезпечення ефективного функціонування сучасних криптосистем. Алгоритми з асиметричним шифруванням: RSA, DSA, ECC, ElGamal

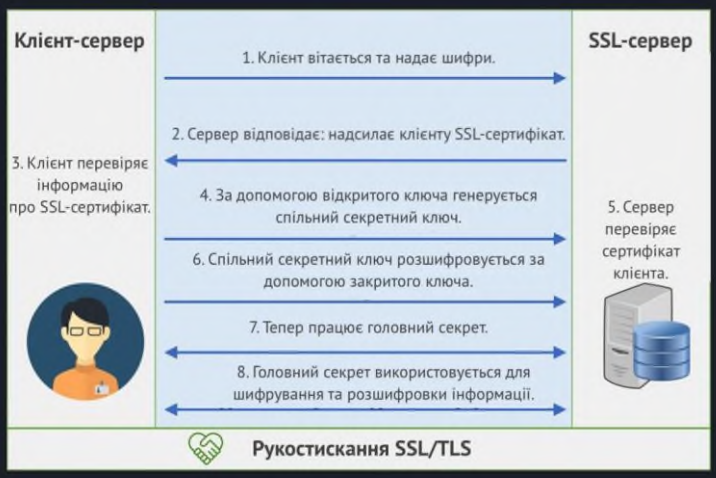


Симетричне шифрування зазвичай є швидшим, оскільки використовує менше обчислювальних ресурсів. Ідеально підходить для шифрування великих обсягів даних. Асиметричне шифрування зазвичай повільніше, оскільки використовує більше обчислювальних ресурсів. Зазвичай використовується для обміну ключами та підписів.

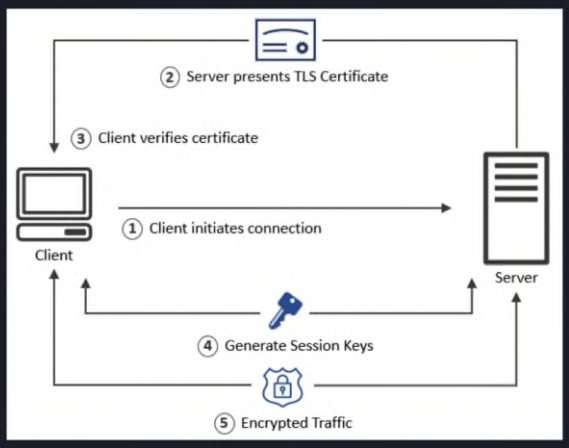


Забезпечення безпеки при передачі даних через інтернет за допомогою протоколу TLS/SSL

Шифрування/дешифрування SSL/TLS (Secure Sockets Layer/Transport Layer Security) — це метод, за допомогою якого захищено підключення до Інтернету, будь то клієнт-клієнт, сервер-сервер або клієнт-сервер. Це запобігає неавторизованим третім сторонам від перегляду або зміни будь-яких даних користувача, якими обмінюються через Інтернет.



SSL/TLS використовує як асиметричне, так і симетричне шифрування для захисту конфіденційності та цілісності даних, що передаються. Асиметричне шифрування використовується для встановлення безпечного сеансу між клієнтом і сервером, найбільш часто використовувані алгоритми шифрування з асиметричним ключем включають ELGamal, RSA, DSA, методи еліптичної кривої та PKCS, а симетричне шифрування використовується для обміну даними в межах захищеного сеансу, найпоширенішими симетричними алгоритмами є AES-128, AES-192 і AES-256.



Додавання SSL/TLS до вашого веб-сайту є важливим заходом для забезпечення безпеки передачі даних між клієнтами та сервером. Існує кілька рішень та підходів, які можна використовувати для цього:

- Використання Безкоштовних SSL/TLS Сертифікатів. Деякі сервіси надають безкоштовні SSL/TLS сертифікати та має простий інструментарій для їх автоматичного оновлення. Доцільно для більшості веб-сайтів.
- Платні SSL/TLS Сертифікати. Comodo, Symantec, DigiCert: Компанії, які надають комерційні SSL/TLS сертифікати. Придатно для корпоративних та великих проектів, де потрібен розширений набір функцій.
- Хмарні Постачальники SSL/TLS. Cloudflare, AWS Certificate Manager, Azure SSL, Google Cloud: Деякі хмарні постачальники пропонують свої сервіси SSL/TLS, що спрощує процес налаштування та оновлення.

Висновок

У світлі нестримного розвитку телекомунікаційних технологій та постійного зростання кількості кіберзагроз, створення та впровадження ефективних систем безпеки в телекомунікаційних мережах стає надзвичайно важливим завданням. У магістерській роботі виконано аналіз сучасних кіберзагроз, а також методи забезпечення безпеки в телекомунікаційних мережах.

Основним методом безпеки було обрано шифрування, а саме впровадження безпеки на основі протоколу SSL, була виконана побудова мережі на основі провайдерів хмарних обчислень таких як AWS та Google Cloud. Актуальність даного дослідження визначається не лише наявністю загроз, але й швидким темпом змін у кіберпросторі, які вимагають постійного оновлення та вдосконалення методів захисту. Створення безпеки в телекомунікаційних системах залежить від вивчення та впровадження передових методів шифрування. Використання сучасних стандартів, таких як Advanced Encryption Standard (AES), та асиметричних алгоритмів гарантує високий рівень стійкості та конфіденційності даних.

АПРОБАЦІЯ РОБОТИ:

1. Іщенко І.Є. «Роль шифрування в забезпеченні конфіденційності телекомунікаційних мереж». IV ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «TELECOMMUNICATION: PROBLEMS AND INNOVATION». Київ-2023р., с.35-36.
2. Іщенко І.Є. «Телекомунікаційна безпека: захист від кіберзагроз та інформаційних вторгнень». IV ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «TELECOMMUNICATION: PROBLEMS AND INNOVATION». Київ-2023р., с.216.


ДЯКУЮ ЗА УВАГУ
ДОПОВІДЬ ЗАВЕРШЕНО

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

МАГІСТЕРСЬКА РОБОТА

на тему:

ПОБУДОВА СИСТЕМ БЕЗПЕКИ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ НА ОСНОВІ СУЧАСНИХ МЕТОДІВ ШИФРУВАННЯ

Виконав: студент групи ТСДМ-63 Філіппов А.О.
Керівник роботи: к.т.н., доцент Малюженко М.В.

Київ-2025

Мета та завдання

Мета роботи – визначення та дослідження основних типів кіберзагроз та методика та методика створення систем безпеки в телекомунікаційних мережах.

Об'єкт дослідження – системи безпеки в телекомунікаційних мережах.

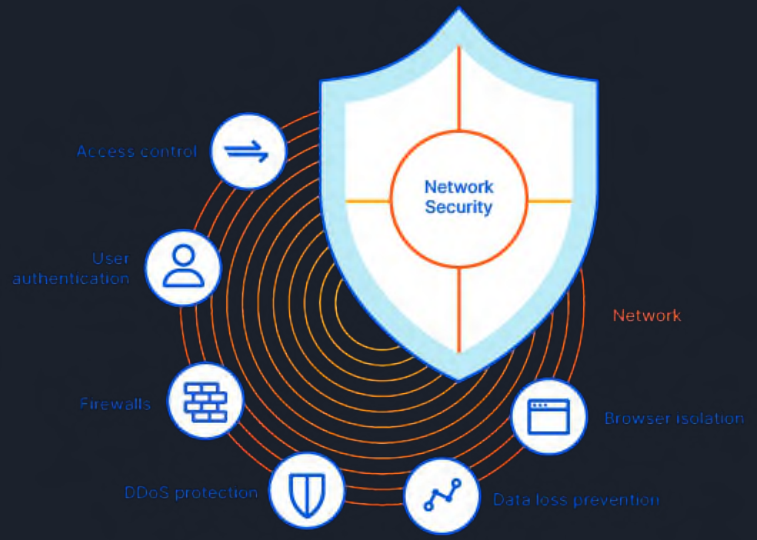
Предмет дослідження – сучасні методи шифрування та їх впровадження.

Завдання до дипломної роботи:

1. Аналіз перспектив та особливостей застосування сучасних методів шифрування
2. Дослідження сучасних типів кіберзагроз;
3. Дослідження сучасних методів шифрування;
4. Реалізація захищеної мережі на основі протоколу SSL;

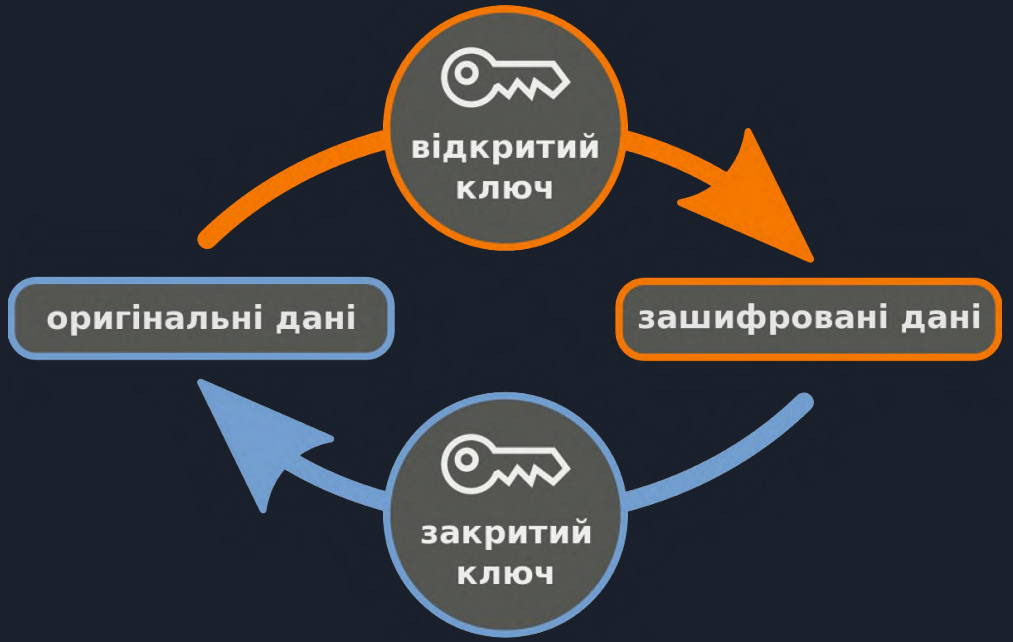
Захист Мережі

У сучасному інформаційному суспільстві, де телекомунікаційні мережі стали невід'ємною частиною нашого повсякденного життя, питання забезпечення безпеки цих мереж виявляється крайньою актуальністю. З кожним днем обсяги передачі даних у мережах та їх важливість для функціонування суспільства зростають, а це робить сучасні телекомунікаційні системи метою для різноманітних кіберзагроз. За таких обставин, розробка та впровадження ефективних систем безпеки в телекомунікаційних мережах стає необхідністю. Одним із ключових елементів таких систем є сучасні методи шифрування, які вирішують завдання надійного захисту конфіденційності, цілісності та доступності переданих даних.



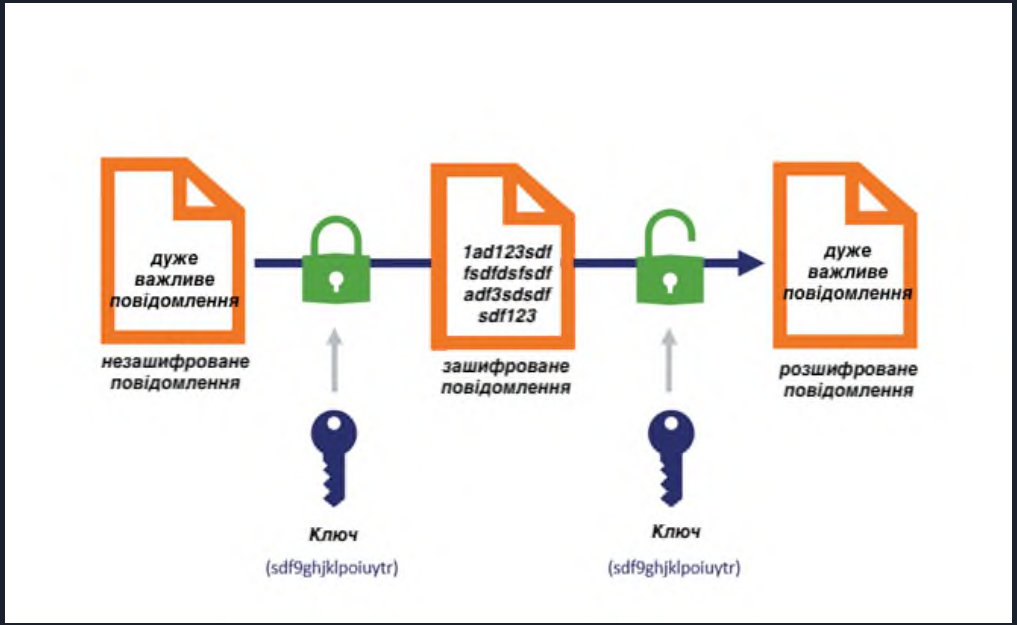
Огляд сучасних методів шифрування

За своєю суттю шифрування — це процес, який перетворює читабельні дані, відомі як відкритий текст, у нечитабельний формат, який називається зашифрованим текстом. Це перетворення досягається за допомогою складних алгоритмів і ключа. Ключ, який може бути рядком випадкових чисел і літер, використовується для дешифрування зашифрованого тексту назад у відкритий текст. Це гарантує, що навіть якщо дані перехоплено під час передачі, вони залишаються незрозумілими для будь-кого без ключа дешифрування.



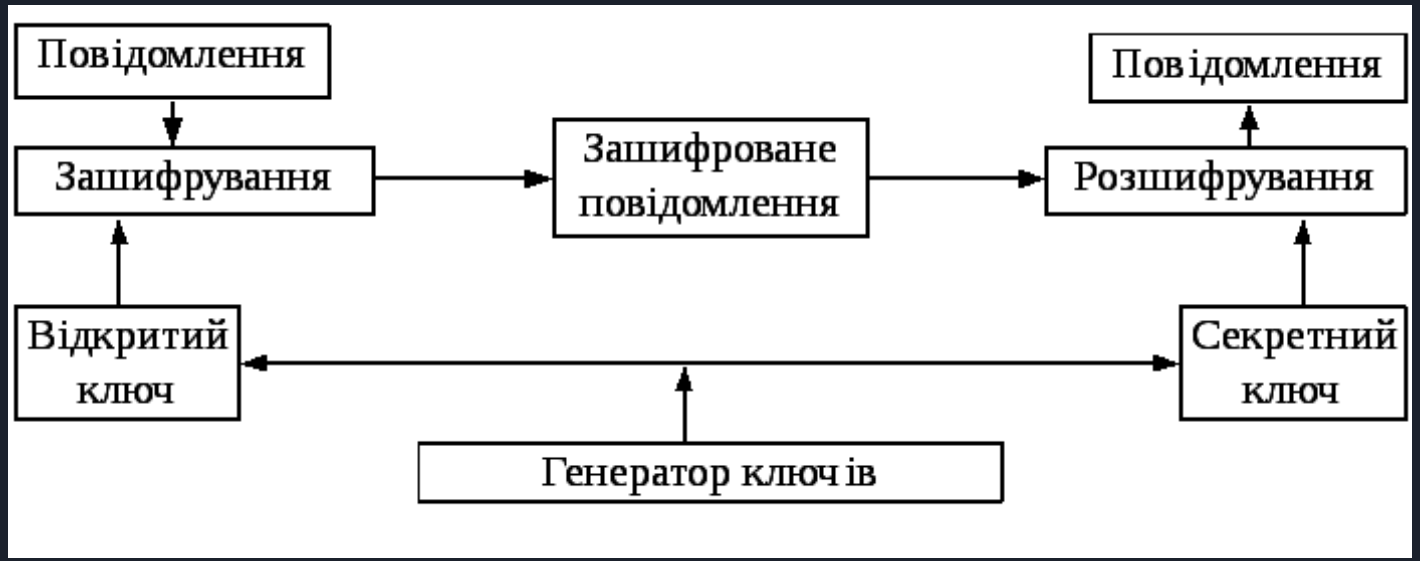
Симетричне шифрування

Симетричне шифрування — це тип шифрування, який використовує той самий ключ для шифрування та розшифрування даних. І відправник, і одержувач мають ідентичні копії ключа, які вони зберігають у секреті та нікому не діляться.
Прикладами алгоритмів з симетричним шифруванням є AES, Twofish, Serpent

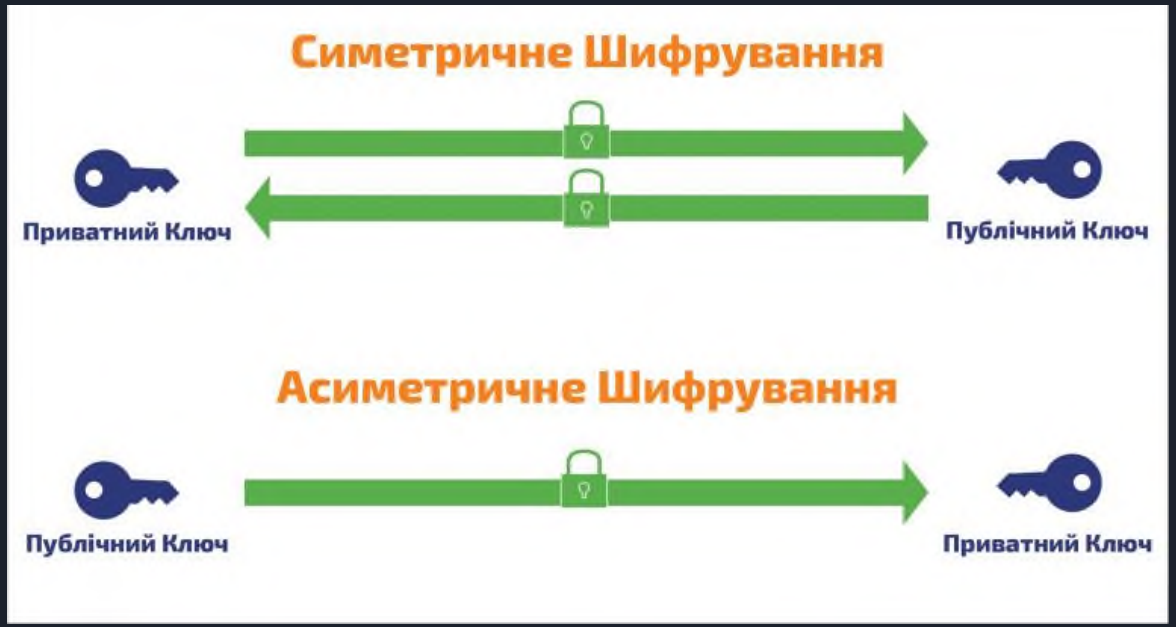


Асиметричне шифрування

Асиметричне шифрування - набір методів криптографічного шифрування, в яких використовують два ключі - таємний(приватний) і відкритий. Алгоритми асиметричного шифрування, так само як і симетричного, застосовують для шифрування масивів даних, але їхня швидкість значно нижча. Основне призначення асиметричних алгоритмів - забезпечення ефективного функціонування сучасних криптосистем. Алгоритми з асиметричним шифруванням: RSA, DSA, ECC, ElGamal

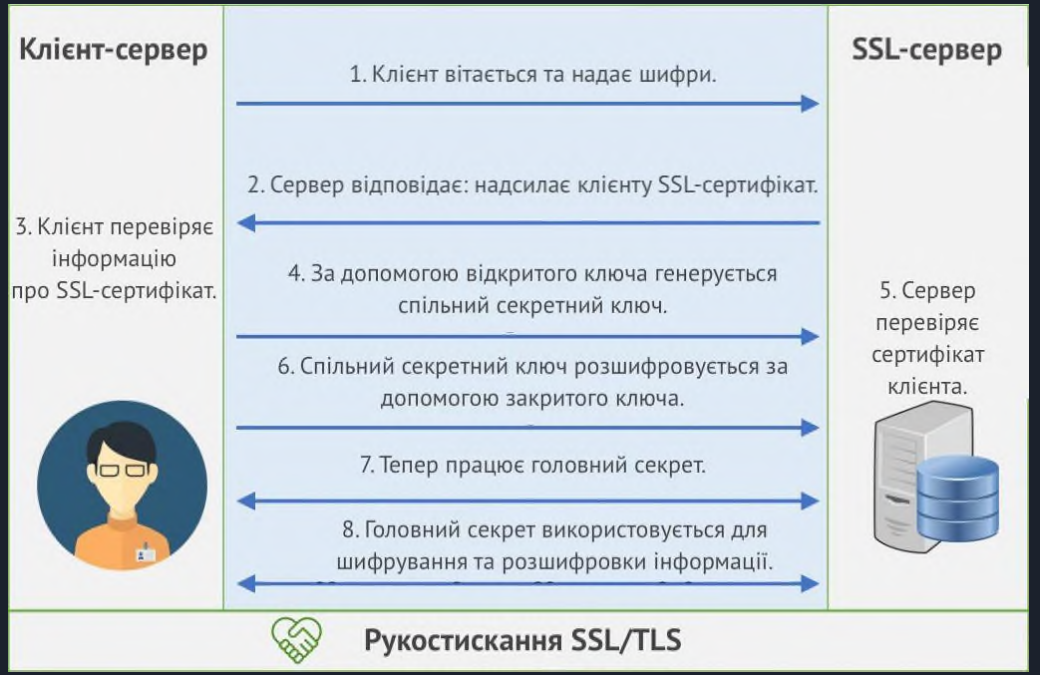


Симетричне шифрування зазвичай є швидшим, оскільки використовує менше обчислювальних ресурсів. Ідеально підходить для шифрування великих обсягів даних. Асиметричне шифрування зазвичай повільніше, оскільки використовує більше обчислювальних ресурсів. Зазвичай використовується для обміну ключами та підписів.

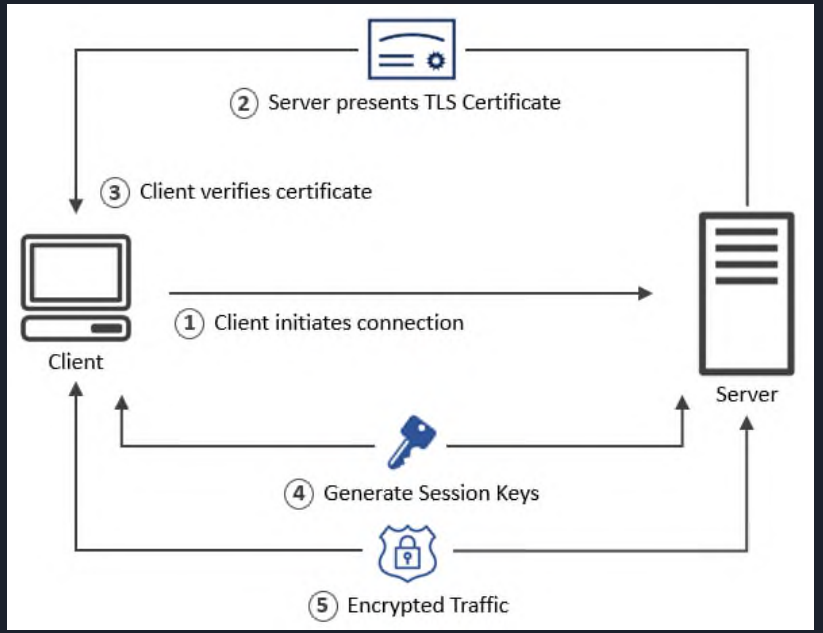


Забезпечення безпеки при передачі даних через інтернет за допомогою протоколу TLS/SSL

Шифрування/дешифрування SSL/TLS (Secure Sockets Layer/Transport Layer Security) — це метод, за допомогою якого захищено підключення до Інтернету, будь то клієнт-клієнт, сервер-сервер або клієнт-сервер. Це запобігає неавторизованим третім сторонам від перегляду або зміни будь-яких даних користувача, якими обмінюються через Інтернет.



SSL/TLS використовує як асиметричне, так і симетричне шифрування для захисту конфіденційності та цілісності даних, що передаються. Асиметричне шифрування використовується для встановлення безпечного сеансу між клієнтом і сервером, найбільш часто використовувані алгоритми шифрування з асиметричним ключем включають ELGamal, RSA, DSA, методи еліптичної кривої та PKCS, а симетричне шифрування використовується для обміну даними в межах захищеного сеансу, найпоширенішими симетричними алгоритмами є AES-128, AES-192 і AES-256.



Додавання SSL/TLS до вашого веб-сайту є важливим заходом для забезпечення безпеки передачі даних між клієнтами та сервером. Існує кілька рішень та підходів, які можна використовувати для цього:

- Використання Безкоштовних SSL/TLS Сертифікатів. Деякі сервіси надають безкоштовні SSL/TLS сертифікати та має простий інструментарій для їх автоматичного оновлення. Доцільно для більшості веб-сайтів.
- Платні SSL/TLS Сертифікати. Comodo, Symantec, DigiCert: Компанії, які надають комерційні SSL/TLS сертифікати. Придатно для корпоративних та великих проектів, де потрібен розширений набір функцій.
- Хмарні Постачальники SSL/TLS. Cloudflare, AWS Certificate Manager, Azure SSL, Google Cloud: Деякі хмарні постачальники пропонують свої сервіси SSL/TLS, що спрощує процес налаштування та оновлення.

Висновки

У світлі нестримного розвитку телекомунікаційних технологій та постійного зростання кількості кіберзагроз, створення та впровадження ефективних систем безпеки в телекомунікаційних мережах стає надзвичайно важливим завданням. У магістерській роботі виконано аналіз сучасних кіберзагроз, а також методи забезпечення безпеки в телекомунікаційних мережах.

Основним методом безпеки було обрано шифрування, а саме впровадження безпеки на основі протоколу SSL, була виконана побудова мережі на основі провайдерів хмарних обчислень таких як AWS та Google Cloud. Актуальність даного дослідження визначається не лише наявністю загроз, але й швидким темпом змін у кіберпросторі, які вимагають постійного оновлення та вдосконалення методів захисту. Створення безпеки в телекомунікаційних системах залежить від вивчення та впровадження передових методів шифрування. Використання сучасних стандартів, таких як Advanced Encryption Standard (AES), та асиметричних алгоритмів гарантує високий рівень стійкості та конфіденційності даних.