Plag

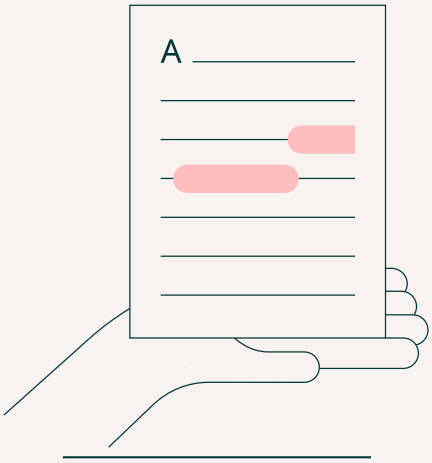
Звіт про оригінальність

● Оцінка схожості 20%

● Ризик плагіату НАЙВИЩИЙ

Olga Kagalo 2025-06-19 23:10

Посилання на звіт: 10mDK / Посилання користувача: qEAc



Ось вона –
Ваша звіт про оригінальність!

Ми раді повідомити, що перевірка вашого документа завершена, і результати вже готові! Наші алгоритми старанно працювали, щоб знайти збіги в наших базах даних.

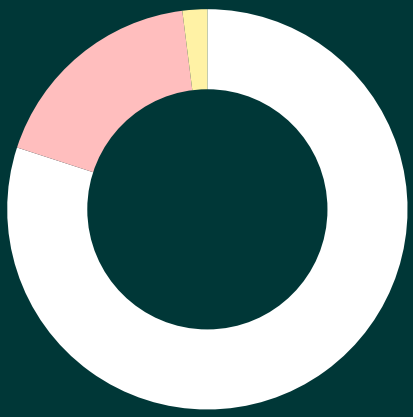
На наступних сторінках ви знайдете результати перевірки:

Бали
Збіги
Посилання

Ваш документ було перевірено за такими джерелами:

- ✓ База даних інтернет-джерел
- ✓ База даних наукових статей
- ○ Глибока перевірка (наш вдосконалений алгоритм)

Бали



Збіги тексту	18%
Перефразування	2%
Цитований текст	0%
Неправильне цитування	0%
Збігів не знайдено	80%

Ризик плагіату — НАЙВИЩИЙ

Ризик плагіату вказує, як збіги тексту розподілені по документу. Вищий ризик виникає, коли збіги з'являються близько один до одного, наприклад, у тому самому абзаці або розділі.

Оцінка схожості — % 20

Оцінка схожості показує, скільки слів або символів у вашому документі збігаються з текстами інших документів, включаючи перефразовані тексти або неправильні цитати.

Збіги

1 АНАЛІЗ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ У КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ТРАНСПОРТНОМУ РІВНІ

1.1 Еволюція та застосування мережевої моделі OSI

Однак, хоча модель OSI мала амбітні цілі, її реалізація ніколи не була повністю завершена через складність і великий обсяг роботи, що потрібен для її впровадження.

Незважаючи на те, що модель OSI не стала домінуючим стандартом, її вплив на розвиток мережевих технологій був значним. У 1984 році вона була прийнята.

У моделі OSI сім рівнів розташовані вертикально, кожен виконує свої функції та взаємодіє зі своїми сусідами. Наприклад, прикладний рівень (Application layer), що є верхнім рівнем, забезпечує взаємодію мережі та користувача, надаючи доступ до мережних служб та обробника запитів до баз даних.

Таблиця 1.1– Компоненти мережевої моделі OSI

Рівень моделі OSI

Функції

7. Прикладний

Забезпечує взаємодію мережі та користувача.

6. Представлення

Відповідає за перетворення даних в зручний для обробки формат та шифрування і дешифрування інформації.

5. Сеансовий

Контролює встановлення, управління та завершення сеансів між програмами на різних комп'ютерах.

4. Транспортний

Забезпечує безперервну передачу даних між комп'ютерами, відповідаючи за розбиття та збірку повідомлень.

Продовження таблиці 1.1

3. Мережевий

Відповідає за маршрутизацію даних в мережі, визначає найкращий шлях для доставки інформації.

2. Канальний

Організовує безпосередню передачу даних між пристроями на мережевому рівні, відповідає за адаптацію до фізичної мережі.

1. Фізичний

Відповідає за фізичне з'єднання між пристроями, передачу бітів через мережеве середовище.

Функції рівня представлення включають обробку протоколів та кодування/декодування даних. Цей рівень відповідає за перетворення запитів програм, отриманих з прикладного рівня, у формат для передачі по мережі, а також за перетворення отриманих з мережі даних у формат, зрозумілий застосункам. Тут може відбуватися стиснення/розпакування, кодування/декодування даних та перенаправлення запитів іншому мережевому ресурсу, якщо це необхідно.

Сеансовий 15 рівень відповідає за керування сеансами зв'язку між програмами, забезпечуючи можливість взаємодії тривалий час. Він контролює створення/завершення сеансів, обмін інформацією, синхронізацію завдань і визначення прав доступу до даних. Сеансовий рівень також забезпечує синхронізацію передачі даних шляхом розміщення контрольних точок у потоці даних, що допомагає відновити процес у випадку виникнення проблем з взаємодією.

Рівень транспорту 11 (Transport Layer) – це 11 четвертий 11 рівень мережевої моделі OSI, який 11 забезпечує надійну доставку 11 даних без помилок, втрати або дублювання у відповідній послідовності. Цей рівень відповідає за передачу блоків даних, що можуть бути розділені на фрагменти чи об'єднані в один, залежно від протоколу.

Мережевий рівень (Network Layer) – третій 11 рівень мережевої моделі OSI, який визначає шлях передачі даних через мережу. Він здійснює трансляцію логічних адрес в

фізичні, визначає найкоротші маршрути, здійснює комутацію та маршрутизацію пакетів, а також відслідковує помилки та затори у мережі.

Канальний рівень (Data Link Layer) – це другий рівень мережевої моделі OSI, що забезпечує взаємодію мереж на фізичному рівні та контроль за можливими помилками. Він упаковує отримані дані у кадри, перевіряє їх на цілісність та виправляє помилки, якщо це необхідно, передаючи їх на мережевий рівень. Цей рівень також взаємодіє з фізичними рівнями, регулюючи і керуючи цією взаємодією.

Фізичний рівень (Physical layer) – це нижчий рівень моделі OSI, що забезпечує безпосередню передачу потоку даних через мережу.

У сучасних мережах зазвичай використовуються три основних типи середовищ передачі: мідні кабелі, оптичні волокна та бездротове з'єднання. Тип сигналу, який використовується для передачі даних, залежить від обраного середовища передачі. Наприклад, для мідних кабелів сигнали зазвичай є електричними імпульсами, для оптичних волокон - світловими імпульсами, а для бездротових з'єднань - радіохвилями, що представляють собою електромагнітні хвилі.

Стандарти технологій фізичного рівня формуються і підтримуються провідними організаціями, такими як Міжнародна організація зі стандартизації (ISO), Інститут інженерів електротехніки та електроніки (IEEE), Американський національний інститут стандартів (ANSI), Міжнародний телекомунікаційний союз (ITU), Альянс електронної промисловості/Асоціація телекомунікаційної промисловості (EIA/TIA) та інші. Ці стандарти визначають параметри і вимоги до фізичних та електричних характеристик передавального середовища, механічні властивості, такі як матеріали та розміри конекторів, а також правила кодування бітів у сигнали та управління інформацією. Усі складові апаратного забезпечення, такі як мережеві адаптери (Network Interface Card, NIC), інтерфейси та конектори, а також матеріали та конструкції кабелів, повинні відповідати цим стандартам. Важливо відзначити, що функціональні можливості фізичного рівня вбудовані безпосередньо у апаратне забезпечення мережі.

Фізичний рівень забезпечує основні функції, необхідні для передачі даних через мережу. Він включає в себе фізичне обладнання, таке як кабелі, пристрої передачі сигналів та конектори, які використовуються для передачі бітів даних. Одна з важливих функцій - це кодування даних, яке перетворює потік бітів у певний код. Це необхідно для забезпечення правильного розпізнавання переданих даних як відправником, так і отримувачем. Крім того, методи кодування також допомагають виявити та виправити помилки, які можуть виникнути під час передачі. Фізичний рівень взаємодіє з іншими рівнями мережі через інтерфейси та протоколи, забезпечуючи ефективну передачу даних.

1.2 Дослідження принципів функціонування та використання технологій у мережах транспортного рівня

Основні завдання мережного рівня, відповідно до моделі взаємодії відкритих систем, включають передачу пакетів між різними вузлами у складних мережах, вибір оптимального маршруту для передачі пакетів та узгодження протоколів канального рівня, які використовуються в різних підмережах однієї комплексної мережі.

Зазвичай протоколи мережного рівня реалізовані у вигляді програмних модулів, що запускаються на кінцевих вузлах, таких як комп'ютери (хости), а також на проміжних вузлах, наприклад, маршрутизаторах або шлюзах. Здійснення функцій маршрутизації може здійснюватися як спеціалізованими пристроями, так і загальнопризначеними комп'ютерами з відповідним програмним забезпеченням.

Основна мета введення мережного рівня полягає у вирішенні проблем, пов'язаних з управлінням складеними мережами. Система мережі розглядається як сукупність декількох окремих мереж, що співпрацюють між собою, і отримує назву складеної мережі або інтермережі. Кожна окрема мережа в цій системі називається підмережею, складовою мережею або просто мережею рис. 1.1 [14].

Рисунок 1.1 – Структура складеної мережі

Взаємозв'язок підмереж через маршрутизатори є ключовим аспектом складеної мережі. У такій мережі можуть бути представлені як локальні, так і глобальні мережі, кожна з яких має свою внутрішню структуру, що не відображена на діаграмі, оскільки не впливає на роботу мережного протоколу. Взаємодія вузлів у межах кожної підмережі забезпечується використанням відповідних технологій, таких як Ethernet, Fast 22 Ethernet, Token Ring, FDDI для локальних мереж і Frame Relay, X.25, ISDN для глобальних. Однак для забезпечення зв'язку між вузлами різних підмереж необхідні додаткові засоби, що надає мережний рівень.

Роль мережного рівня полягає в організації спільної роботи всіх підмереж у складеній мережі для ефективного переміщення пакетів даних. Для використання технологій, що домінують у підмережах, мережний рівень взаємодіє з їх системами адресації.

Хоча деякі технології локальних мереж (наприклад, 22 Ethernet, Token Ring, FDDI, Fast Ethernet) використовують спільну систему MAC-адрес для ідентифікації вузлів, інші технології (такі як X.25, ATM, Frame Relay) мають свої власні схеми адресації. Адреси, призначені вузлам згідно з технологіями підмереж, вважаються локальними. Щоб мережний рівень міг ефективно працювати, йому потрібна власна система адресації, яка б не залежала від адресації вузлів у окремих підмережах, і дозволяла однозначно ідентифікувати будь-який вузол складеної мережі. Один із способів формування

мережної адреси - це унікальне присвоєння номерів усім підмережам у складеній мережі та номерів вузлів у межах кожної підмережі. Отже, мережна адреса складається з номера мережі (підмережі) і номера вузла в цій мережі (підмережі).

Мережний рівень відповідає за передачу даних через складену мережу, забезпечуючи їхнє упаковування у пакети з заголовками мережного рівня. Уніфікований формат заголовка пакета мережного рівня дозволяє незалежно від типу мережі включати інформацію про призначення пакета. Мережний рівень обирає маршрут та керує переміщенням пакетів між підмережами.

16 Коли дві або більше мережі об'єднуються для спільної транспортної служби, цей вид взаємодії часто називається 16 міжмережною взаємодією (internetworking).

16 Протоколи маршрутизації відрізняються від звичайних мережних протоколів, таких як SP і IPX, оскільки вони спеціалізовані на передачі маршрутної інформації, а не користувацьких даних. Хоча обидва види протоколів 20 виконують функції мережного рівня моделі OSI, протоколи 20 маршрутизації використовуються для 20 обміну маршрутною інформацією та включають дані у пакети мережного рівня або транспортного рівня. З цього погляду, протоколи маршрутизації 16 можна було б формально віднести до рівнів вище за мережний.

Протоколи маршрутизації допомагають маршрутизаторам побудувати карту зв'язків у мережі, визначити оптимальні маршрути для передачі пакетів і заповнити таблиці маршрутизації. Ця інформація допомагає визначити, куди направляти пакети для кожної мережі, забезпечуючи ефективну доставку.

Протоколи маршрутизації важливі для підтримки оптимального маршруту у мережі, особливо при зміні конфігурації мережі. Однак, неефективне використання цих протоколів може призвести до зациклення пакетів і втрати даних.

Транспортний рівень забезпечує передачу даних між вузлами мережі з необхідним рівнем надійності. Протоколи на цьому рівні відповідають за встановлення з’єднання, нумерацію, буферизацію та упорядкування пакетів, забезпечуючи ефективний обмін інформацією між процесами користувача.

Два ключові протоколи на транспортному рівні – це 13 UDP (User Datagram Protocol), який забезпечує надсилання датаграм без встановлення з'єднання, та 24 TCP (Transmission Control Protocol), який керує передачею даних з установленням з'єднання та перевіркою доставки.

При надходженні пакетів на транспортний рівень, операційна система організовує їх у черги до відповідних прикладних процесів. Ці черги в термінології TCP/IP відомі як

порти. Кожен порт ідентифікує певний прикладний процес і має 16-бітний номер, що знаходиться у діапазоні від 1 до 65535. Комбінація номера порту, номера мережі та номера вузла однозначно визначає призначений процес у мережі. Цей набір параметрів називається сокетом.

1.3 Основні протоколи інформаційно-комунікаційних систем

13 Сучасний етап розвитку телекомунікацій характеризується новими напрямами, які відображають перехід від простого росту кількості до покращення якості послуг. Це означає розширення асортименту телекомунікаційних послуг, які тепер інтегруються з різними інформаційними сервісами.

Крім того, мережі телекомунікацій починають інтегруватися, стають більш функціональними і отримують глобальний охоплюючий характер, аналогічно комп'ютерним мережам.

Давайте оглянемо ключові особливості телекомунікаційних систем та мереж, що важливі для 13 переходу від традиційних мереж до мереж нового покоління NGN (Next Generation Networks):

– Використання програмних комутаторів Softswitch для управління послугами та потоками інформації, що дозволяє зробити мережу набагато більш гнучкою.

– Застосування надійних та безпечних протоколів, спеціально розроблених для верхніх рівнів телекомунікаційних мереж.

– Перехід до нової архітектури мережі NGN, яка орієнтована на гнучку та ефективну систему створення та надання різноманітних послуг, як телекомунікаційних, так і інформаційних.

Кожен тип трафіку потребує відповідного рівня пропускної здатності, гарантованої затримки та стандартної рівня варіацій. Забезпечення цих вимог від трафіку вимагає відповідних технологій передачі даних. Оскільки абстрактний трафік може бути різноманітним і нестабільним, виникає необхідність у його класифікації за номером або типом. Однак індивідуальна обробка кожного типу трафіку може бути витратною. Вирішення цієї проблеми може полягати в групуванні трафіку за номером або типом, що спрощує обробку та може зменшити витрати.

Індивідуальне або групове обслуговування передбачає введення управління затримками та може бути застосоване лише у випадку стабільного маршруту передачі. Проте для ефективного використання цих методів необхідно, щоб усі групи в мережі були однаковими. У випадку зміни маршруту передачі потрібно передавати параметри обслуговування разом з трафіком, що може стати викликом у складних мережах з

багатьма підмережами.

У зв'язку з ростом використання вузькосмугових каналів виникла потреба встановлювати та підтримувати з'єднання (логічні канали) всередині мережі. У минулому, коли вузькосмугові канали не були настільки завантаженими, не виникало потреби передавати через них велику кількість потоків. Оскільки кожен користувач намагався використовувати максимальну доступну пропускну здатність, це призводило до конфліктів і хаосу в мережі. Для управління цим хаосом були розроблені методи чергування, які визначали, які потоки мають перевагу. Проте виникала проблема, коли великі блоки даних переміщувалися через канал, а раптово приходили маленькі, але дуже швидкі пакети, які вимагали негайного перевезення без черги.

Протоколи маршрутизації стають основними місцями збоїв у сучасних мережах зв'язку через використання так званих "таблиць маршрутів" для навігації. В разі неполадок у обладнанні, розривів або перевантажень на лініях зв'язку потрібно динамічно змінювати ці таблиці, проте це може бути вкрай складно та навіть неможливо через унікальність ситуації. Це призводить до невідповідності результатів обчислень протоколів маршрутизації та виникнення інерції, що додатково ускладнює ситуацію [6].

Ще одним негативним явищем у мережі передачі даних є резонанс. Виникнення цього ефекту пов'язане з методом транспортування даних через канали зв'язку. У режимі негарантованої доставки, для стабільних з'єднань транспортний рівень використовує механізм повторних запитів. Коли користувачі використовують подібні правила повторних запитів, це створює аналогію з багатьма майже ідентичними генераторами, що може призвести до ефекту резонансу в системах з великою кількістю джерел сигналів. Це може призвести до перенавантаження каналів зв'язку та ускладнити задачу підтримки коректного стану маршрутних таблиць. Одержання необхідної службової інформації та її передача тими ж каналами робить завдання забезпечення збіжності та стабільності ще більш складним.

Для підтримки ефективного впровадження нових технологій активно розробляються, уніфікуються та стандартизуються нові пристрої мережевого обладнання, такі як мости, комутатори (як апаратні, так і програмні), маршрутизатори, міжмережні екрани, шлюзи, а також вузли управління та комутації послуг. Один із таких типових пристроїв – це Softswitch, або програмний комутатор [7].

Програмний комутатор – це комплексне програмно-апаратне забезпечення, що стає головним інтелектуальним центром мережі. Він відповідає за керування обробкою телефонних викликів у різних мережах, включаючи мережі з комутацією пакетів. Softswitch надає мережі інтелектуальну основу, здатну керувати і координувати роботу інших елементів мережі, забезпечуючи кращу керованість та масштабованість всієї

інфраструктури.

Термін Softswitch наразі охоплює широке різноманіття пристроїв, включаючи програмні комутатори, пристрої для розділення функцій управління з'єднаннями і комутації, а також високошвидкісні маршрутизатори.

Softswitch виконує різноманітні завдання, включаючи:

– функцію універсального конвертора протоколів сигналізації і контролю для забезпечення взаємодії між мережами з комутацією каналів та мережами з комутацією пакетів;

– розвантаження операторських мереж від Інтернет-трафіку та його обліку, маршрутизації телефонного трафіку через IP-мережі, та обробки трафіку комутованого доступу з міських мереж;

– доставку інтелектуальних послуг та транзит телефонного трафіку через IP-мережі;

– забезпечення доступу, включаючи широкосмуговий доступ та передачу великих обсягів даних через вузькосмугові абонентські лінії;

– оптимізацію транзиту на мережах мегаполісів та організацію єдиного білінгу для абонентів телефонних мереж загального користування та IP-мережі.

Початковий стандарт для протоколів, що визначають взаємодії вузлів у сфері IP-телефонії, був вироблений Комітетом зі стандартизації телекомунікаційного сектору Міжнародного телекомунікаційного союзу (ITU-T) у 1996 році. Цей стандарт, відомий як H.323, регулює такі взаємодії. Початкові рекомендації, які стосувалися передачі голосового та відеотрафіку, були розроблені на початку 90-х років, проте вони спрямовані на використання ISDN замість IP-мереж для транспорту цього трафіку.

Стек протоколів, який використовується для взаємодії за допомогою протоколу SIP, включає такі компоненти:

– протокол ініціювання сесійного зв'язку (Session Initiating Protocol) на рівні прикладного програмного забезпечення;

– протоколи TCP/UDP на рівні транспортного забезпечення;

– протоколи IPv4 і IPv6 на рівні мережевого забезпечення;

– кадри Ethernet та ATM на рівні канального забезпечення;

– фізичні середовища передачі, такі як UTPS та оптичний кабель, на рівні фізичного

забезпечення.

2 СУТНІСТЬ 17 ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНИХ УМОВАХ

2.1 Аналіз заходів захисту даних в корпоративних мережах

Оцінка інформаційної безпеки є важливим аспектом в управлінні інформаційними технологіями. Ця область залучає значну увагу з моменту народження інформаційних технологій. Однією з ключових складових оцінки є нормативні документи, які встановлюють стандарти і критерії безпеки інформаційних систем. До найважливіших таких документів можна віднести: стандарт ISO/IEC 27001, який встановлює вимоги до 27 систем управління інформаційною безпекою; стандарт NIST SP 800-53, що містить керівні принципи та вимоги до захисту інформації в федеральних системах США; та інші національні та міжнародні стандарти, які визначають методики оцінки та вдосконалення безпеки інформаційних технологій [1].

Нормативні документи, що розглянуті, визначають фундаментальні принципи та методики для 17 забезпечення інформаційної безпеки у різних сферах. Проте, для успішного досягнення цієї мети необхідно застосовувати широкий спектр підходів та методів. Це включає в себе формальні методи моделювання процесів та оцінки ефективності, а також неформальні методи декомпозиції та структуризації компонентів систем і процесів.

При впровадженні заходів захисту, важливо збалансувати можливий збиток 17 від несанкціонованого доступу до інформації з розміром витрат на забезпечення безпеки. Ефективність захисту можна підвищити шляхом 26 дослідження різних підходів до оцінки рівня захисту та вибору відповідних систем захисту. Ця оцінка завжди є індивідуальною і залежить від різних факторів, таких як вартість інформації, статус організації, важливість даних, існуючі технології та ресурси.

Інформаційні ресурси неможливо уявити без доступу до них, і в сучасному світі доступність інформації є ключовою складовою успішного функціонування. Забезпечення доступності означає збереження нормальної взаємодії між користувачем та інформаційним ресурсом.

Для забезпечення конфіденційності інформації важливо встановити ефективний режим доступу до неї. Конфіденційність означає, що інформація залишається недоступною для тих, хто не має на це права. Це досягається через адекватність режиму доступу.

Сьогодні діяльність більшості організацій неможлива без мережі Інтернет. Однак разом з можливостями, які надає Інтернет, зростає і ризик збитку. Тому проблема забезпечення безпеки в інформаційних системах є дуже актуальною. Цей сегмент

постійно розвивається і вдосконалюється для забезпечення найвищого рівня захисту від мережевих загроз.

На сьогоднішній день мережеві екрани (брандмауери, файерволи, фільтруючі маршрутизатори і т. д.) залишаються одними з основних інструментів захисту комп'ютерних інформаційних систем. Вони служать не лише засобом реалізації політики безпеки на мережевому рівні, але й надають певний рівень захисту.

Рівень безпеки, який забезпечується мережевим екраном, може варіюватися в залежності від потреб і вимог безпеки конкретної системи. Традиційно існує компроміс між безпекою, простотою використання, вартістю і складністю.

Одним з ефективних засобів забезпечення безпеки інформаційних систем в мережі Інтернет є використання VPN (віртуальних приватних мереж). VPN дозволяє об'єднувати різні локальні мережі в єдину віртуальну мережу, що забезпечує захищений канал передачі даних між ними. Це досягається за допомогою криптографічних методів, що забезпечують конфіденційність, цілісність та аутентифікацію даних.

Оцінка рівня захисту інформаційних ресурсів вимагає визначення їх поточного стану, що може бути здійснено двома різними підходами: «дослідженням знизу догори» та «дослідженням згори донизу».

При використанні першого підходу адміністратори проводять аналіз захисту, спрямований на виявлення різних видів можливих атак, які можуть бути спробами порушення безпеки інформаційного ресурсу. Однак цей підхід може бути обмежений тим, що навіть найкращі адміністратори не можуть передбачити всі можливі методи атак та не завжди мають повну інформацію про програмно-апаратні засоби зловмисників.

Підхід «згори донизу» передбачає докладний аналіз схем зберігання та обробки даних. Спочатку визначаються всі інформаційні об’єкти та потоки захисту, а потім досліджується стан системи інформаційного захисту для визначення реалізованих методів захисту інформаційних ресурсів та їх рівня. Подальша класифікація всіх інформаційних об’єктів за рівнем конфіденційності, вимогами до доступності та цілісності допомагає забезпечити ефективний рівень захисту.

Останнім етапом є проведення оцінки ризиків, що передбачає визначення потенційних збитків для компанії внаслідок можливих порушень захисту інформаційних ресурсів. Наближений ризик обчислюється як добуток «потенційного збитку від атаки» на «ймовірність такої атаки». Зазвичай, оцінка ризиків включає аналіз ризиків та оцінку потенційного збитку.

Загальна методологія оцінки інформаційної безпеки передбачає три етапи: підготовчий, основний та завершальний.

На завершальному етапі основної процедури розробляється технічний звіт з оцінки, який експерт передає для подальшого аналізу. Під час цього етапу експерт вивчає надані матеріали та досліджує профіль захисту або об’єкт оцінки. Він готує цілу низку звітів, в яких враховані вимоги органу контролю, виявлені недоліки та інша інформація про процес оцінки. У той же час контролюючий орган здійснює безперервний моніторинг процесу відповідно до схеми оцінки.

Під час заключного етапу проводиться всебічний аналіз технічного звіту оцінки з боку контролюючого органу з урахуванням загальних критеріїв методології та вимог схем оцінки безпеки. На основі цього технічного звіту складається підсумковий звіт з оцінки, який містить рішення про відповідність необхідним вимогам. Усі учасники процесу оцінки мають право ознайомитися з підсумковим звітом і вимагати відповідних пояснень.

Багато компаній з різних причин часто не можуть провести повноцінну оцінку захисту своїх інформаційних ресурсів. Тому пропонується використовувати кількісну оцінку рівня захищеності, особливо на етапі впровадження. Застосування кількісної оцінки дозволяє точніше порівняти різні варіанти захисту та обрати найбільш ефективний. Для цього враховують ймовірність виникнення загроз і вразливостей, вартість захищених ресурсів (оцінка втрат при їх втраті) та частоту загроз кожного типу. Необхідно також встановити обмеження на вартість захисної системи та оцінити вплив на продуктивність.

2.2 Застосування відмовних модулів у якості засобу забезпечення інформаційної безпеки

Приманка Honeypot – це інноваційний інструмент у сфері мережевої безпеки, спрямований на виявлення та відстеження зловмисників, які намагаються зламати систему. Ця технологія відрізняється від звичайних методів захисту тим, що не виконує конкретних завдань, а замість цього створює ідеальне середовище для виявлення потенційних загроз. Назва 'Honeypot' відображає концепцію пристрою, який приваблює зловмисників, як мед приваблює бджіл. Протистояти приманкам може бути важко, проте це зовсім не неможливо.

Приманки можуть бути використані для виявлення незаконних дій, коли традиційні методи безпеки генерують багато записів журналу, більшість з яких не мають значення. В таких випадках Honeypot забезпечує точне виявлення реальних атак або досліджень. Крім того, не всі технології можуть ефективно виявляти невідомі атаки, що

робить Honeypot незамінним інструментом у цьому плані.

Пастки також можуть використовуватися для реагування на спроби зловмисників вторгнутися в мережу. Якщо атака виявляється, і одна з атакованих систем є пасткою, отримана корисна інформація дозволяє оперативно реагувати на зловмисника. Використання приманок Honeypot має безліч переваг, але важливо розуміти їхні обмеження і не переоцінювати їхню роль в системі безпеки [2].

Використання технології Honeypot дарує аналітикам безліч переваг. Вона дозволяє збирати цінну інформацію про хакерів, вимоги до системних ресурсів, при цьому маючи простоту управління та чіткість використання. У порівнянні з системами IDS (виявлення вторгнень), які можуть генерувати величезні обсяги інформації щоденно, Honeypot реєструє менші обсяги даних, проте цілком зосереджені на неправомірних діях. Це робить процес аналізу ефективнішим та менш витратним, оскільки інформація, яка потрапляє в Honeypot, має велику цінність та точність.

Одна з головних переваг Honeypot полягає в його ефективності та економічності. Він не потребує значних ресурсів на підтримку та оновлення, оскільки практично автономний після налаштування. Крім того, використання Honeypot демонструє доцільність витрат на безпеку, навіть у випадку, коли вороги не намагаються проникнути в мережу. Він слугує ефективним і доказовим засобом для показу та підтвердження необхідності безпекових витрат.

Програмні приманки можуть бути налаштовані відповідно до різних цілей, включаючи широкий спектр параметрів конфігурації. Від програмних рівнів, які не потребують складних налаштувань, до складних апаратних комплексів, можна виділити різні рівні складності і можливостей програмних приманок. Залежно від їх функціональних характеристик та рівня взаємодії з потенційними загрозами, програмні приманки можуть бути класифіковані на рівні слабкої, середньої та високої інтеграції.

Honeypot з низьким рівнем складності використання є дуже надійними засобами. Вони імітують лише обмежену частину функціоналу служб, що обмежує взаємодію зловмисників з ними. Наприклад, такі приманки можуть імітувати систему UNIX із запущеним сервісом telnet. При спробі підключення до такої приманки зловмисник отримає запит на введення і намагатиметься отримати доступ до системи. Також може бути імітований FTP-сервер з анонімним доступом і файликом, який містить надійно засховані дані, такі як номери кредитних карток. Будь-яка спроба отримати доступ до цього файлика буде зарахована як спроба несанкціонованого доступу. Система веде журнал інцидентів, включаючи час, IP-адресу та порт зловмисника, а також порт, яким він намагався скористатися. Основне завдання таких програмних приманок полягає у мінімізації ризику. Хоча ризик використання таких приманок мінімальний, він присутній через можливість вразливості програмного забезпечення. Проте, сила цих

простих приманок полягає в їхній простоті, яка робить їх більш надійними. Такий підхід допомагає мінімізувати ризик, пов'язаний з можливими вразливостями та забезпечує більш високий рівень безпеки системи.

Приманки з високим рівнем взаємодії є найбільш складними та ризикованими, проте вони надають максимальну кількість інформації про зловмисника. Ці приманки моделюють реальні системи, до яких зловмисник може отримати доступ. Вони складаються з вузла приманки, мережевого датчика та сховища інформації. Часто такі приманки розташовуються у мережі за брандмауером, що дозволяє здійснювати фактичний контроль за доступом через брандмауер. Проте неправильна настройка таких вузлів або непередбачені ситуації можуть призвести до ризику доступу зловмисника до мережі. Однак, недоліки такого підходу включають складність реалізації та високі витрати на підтримку.

Проте ізольований вузол може також викликати підозру та бажання швидше його залишити. Крім того, якщо у приманки немає іншого трафіку, крім спроб злому, це також може бути підозрілим. Тому важливо створювати віртуальне середовище, яке виглядає як реальна мережа з різними рівнями складності злому, а також налаштовувати мережеві датчики належним чином для надійної реєстрації. Потрібно також бути обережним при роботі з віртуальними машинами, оскільки шкідливий код може вийти з-під контролю та спричинити непередбачені наслідки. Детальний аналіз і належне налаштування приманки на різних рівнях взаємодії є ключовими для успішного виявлення та аналізу потенційних загроз.

Взагалі, при використанні різних стратегій для зламу дуже серйозних ресурсів, таких як державні сайти або банківські системи, зловмисники можуть приховати свою ідентичність шляхом використання проксі-серверів. У такому випадку IP-адреса не є надійним показником, оскільки вона може бути адресою проксі-сервера. Таким чином, відстеження може бути ускладненим, оскільки потрібно робити заміщення на проксі-серверах. Деякі зловмисники використовують мережу з декількох комп'ютерів, 19 щоб отримати доступ до мережі через модем GPRS/EDGE у мобільному телефоні. Це дозволяє їм віддалено здійснювати атаки, уникнувши виявлення та відстеження їх місцеперебування. Крім того, якщо комп'ютер зловмисника є вразливим, приманка може відповісти контратакою, встановивши вірус або збираючи 19 конфіденційну інформацію, таку як файли cookie [2].

Під час вибору потенційної жертви, зловмиснику необхідно детально вивчити топологію мережі. Важливо переконатися, що цей вузол обробляє зовнішній трафік, має відмінну конфігурацію від конфігурації за замовчуванням та активно використовується іншими учасниками мережі. Після цього зловмисник може провести докладне дослідження протягом кількох днів, скануючи порти та спробуючи викликати

переповнення буфера. Він також може атакувати саму систему, використовуючи атаки, які маскують його IP-адресу, такі як DDoS, SYN або ECHO-death.

Honeypot може не вирішити всі проблеми безпеки, тому доведеться або дослідити рівень безпеки окремих частин інфраструктури, або використовувати кілька приманок. Існує певний ризик того, що зловмисник впізнає пастку як фіктивну. Це часто стається через недостатньо ретельну або неправильну постановку приманки, що свідчить про людський фактор в більшості випадків.

2.3 Стратегії забезпечення безпеки для критичної інформаційної інфраструктури

Сучасні виклики у сфері кібербезпеки відзначаються складністю та постійним еволюційним характером. Кібератаки вже давно перетворилися на інструмент для досягнення різноманітних цілей, які можуть бути пов'язані з порушенням конфіденційності, цілісності або доступності інформації. Об'єктами в цьому контексті є критична інфраструктура та інформаційні системи, що мають важливе значення для функціонування держави та суспільства.

– аналіз та визначення переліку інформаційних, програмних та апаратних ресурсів об’єкта критичної інформаційної інфраструктури, оцінка їх критичності та потенційних наслідків у разі порушення КЦД;

– здійснення передачі даних через бездротові мережі лише захищеними з'єднаннями з метою забезпечення конфіденційності та цілісності інформації. Використання технологій Wi-Fi та Bluetooth на об’єктах критичної інформаційної інфраструктури забороняється;

– використання захищених з'єднань для захисту даних, що передаються між віддаленими користувачами, адміністраторами та об’єктом критичної інформаційної інфраструктури, а також між різними компонентами об’єкта та іншими (зовнішніми) інформаційно-технічними системами.

Забезпечення конфіденційності та безпеки інформації, що стосується конфліктів, є важливою складовою безпеки країни. Для цього розглянемо деякі методи та рішення, які можуть бути застосовані:

1. Перевірка на допуск та достовірність. Для забезпечення безпеки інформації держава може регулювати доступ до конфіденційної інформації, що стосується конфліктів. Це може включати видання дозволів на доступ до секретної інформації для ключових учасників, а також встановлення критеріїв для нових учасників, наприклад, на основі згоди існуючих учасників або вимагати перевірку відповідності з державними органами.

1 2. Системи класифікації. Для контролю за поширенням інформації використовуються системи класифікації, які вказують ступінь доступності. Наприклад, 1 Протокол світлофора (TLP) має чотири кольори, які позначають рівень конфіденційності: червоний, бурштиновий, зелений та білий.

3. Використання електронних інструментів. 1 Деякі платформи використовують електронні інструменти, наприклад, екстранет, для 7 обміну даними між сторонами, які знаходяться на відстані. Ці інструменти дозволяють проводити обмін даними 4 в безпечному середовищі, забезпечуючи аутентифікацію учасників та захист інформації.

Різноманітні країни використовують різні підходи до 1 захисту конфіденційної 4 інформації, що стосується конфліктів [5]:

– Австралія. Уряд Австралії у 2003 році створив довірену мережу 6 обміну інформацією (TISN), яка є основним механізмом взаємодії між бізнесом і урядом. TISN забезпечує безпечне середовище для власників та операторів KBOI, дозволяючи їм обмінюватися інформацією та співпрацювати 6 для вирішення проблем безпеки та 1 безперервності бізнесу. 6 Крім того, існують спеціалізовані форуми та експертно-консультативна група, що допомагають вивчати складні питання та організовувати стабільність.

– Франція. В рамках національної системи забезпечення безпеки життєдіяльності (SAIV) приймаються директиви та плани, класифіковані за рівнями конфіденційного захисту. Оператори KBOI мають забезпечити знищення секретних документів, які більше не потрібні, зокрема тоді, коли вони переглянуті, скасовані або втрачається їхній статус «життєво важливого оператора.

– Канада. Визначила своєю однією з головних мет цілісний обмін інформацією та захист між учасниками 1 критично важливої інфраструктури (KBI). Для досягнення цієї мети уряд Канади пропонує створення Інформаційного центру критично важливої інфраструктури (CI Gateway), який буде розміщений на платформі громадської безпеки Канади. Мета CI Gateway полягає в забезпеченні участі ключових секторів KBI та інших зацікавлених сторін, стимулюючи їх до приєднання та сприяючи 6 обміну інформацією та передовим практикам через галузеві мережі. На що стосується доступу до конфіденційної інформації для приватного сектора, то більшість інформації, зібраної у співтоваристві безпеки та розвідки, є конфіденційною та доступною лише особам із відповідним допуском. Державна безпека Канади активно співпрацює з провідними федеральними департаментами та агентствами для залучення більшої кількості зацікавлених сторін із приватного сектора.

Один із ключових інструментів регулювання кібербезпеки в Європейському Союзі (ЄС) - Директива (ЄС) 2016/1148 Європарламенту та Ради 25 від 6 липня 23 2016 року про

заходи 25 для 25 встановлення 25 високого загального рівня безпеки мереж 9 та інформаційних систем в усій Союзі (NISD). Однак ця директива - лише один з інструментів регулювання кібербезпеки в ЄС, адже інші директиви та регламенти, такі як GDPR, також впливають на захист критичної інформаційної інфраструктури (KII).

Згідно зі статтею 5 NISD, держави-члени мають широкі можливості в управлінні відповідно до власних обставин. Вони можуть встановлювати ще більш жорсткі стандарти безпеки, ніж ті, що передбачені у директиві. Навіть в пункті 6 Преамбули NISD зазначається, що 9 для операторів життєво важливих послуг та провайдерів цифрових послуг можуть бути застосовані ще більш суворі заходи захисту.

Різноманітні країни Європейського Союзу, такі як Німеччина та Великобританія, прийняли відповідні закони та стратегії для регулювання 4 захисту критичної інфраструктури. Наприклад, 9 в Німеччині це питання урегульоване Законом про 7 забезпечення безпеки інформації (BSIG) та відповідним указом щодо класифікації критичної інфраструктури. Схожий підхід має і Великобританія, яка взяла на озброєння 9 відповідний Статут № 506. Більшість країн ЄС також мають національні стратегії з кібербезпеки, в яких відводиться значна увага 4 захисту критичної інфраструктури. У цих стратегіях передбачені заходи для забезпечення безпеки як найбільш важливих організацій і компаній, так і органів державної влади, які беруть активну участь у цьому процесі.

У 2015 році постійний комітет загальнокитайських зборів народних представників прийняв ряд законів, спрямованих на 4 забезпечення національної безпеки та 4 захист інформаційної 4 інфраструктури. Закон про національну безпеку вперше визначив "захист національного суверенітету в кіберпросторі" як одну з важливих складових національної безпеки, а також створив систему перевірки для розгляду питань, пов'язаних з інформаційною безпекою. Закон про боротьбу з тероризмом, що набрав чинності у 2017 році, встановив механізми для боротьби з терористичною діяльністю, зокрема, зобов'язав телекомунікаційні та Інтернет-підприємства співпрацювати з державними органами у розслідуванні терористичних подій.

3 4 ЗАХИСТ ІНФОРМАЦІЇ В КОНТЕКСТІ ТЕХНОЛОГІЇ VOICE OVER INTERNET PROTOCOL

3.1 Принципи технології голосового передачі через Інтернет VoIP та використання IP-телефонії

Перспективи телефонії варто розглядати з двох позицій: для користувача це доступна послуга, для оператора – це технологічний аспект надання цієї послуги. Основна мета телефонії - забезпечити надійний голосовий зв'язок між віддаленими абонентами з мінімальною затримкою. Якість голосової передачі повинна бути максимально наближена до реального спілкування лице до лиця. Голосовий сигнал передається за

допомогою сучасних електронних засобів.

Ще однією важливою функцією телефонії є передача та обробка службової інформації або сигналізація. Для здійснення дзвінка до співрозмовника потрібно ввести його номер на телефоні. Обробка цього номера визначає маршрут передачі голосової інформації від одного абонента до іншого. Під час цього процесу звучить дзвінок на телефоні співрозмовника, а особа, що здійснює дзвінок, отримує інформацію про стан з'єднання (наприклад, зайнято чи недоступно). Типовий сценарій телефонної розмови відтворено на рис.3.1. Перший успішний випадок використання телефонії полягав у передачі голосу на великі відстані. У перших поколіннях телефонних систем голос людини перетворювався на електричний сигнал за допомогою мікрофону.

Рисунок 3.1 – Процес телефонного спілкування у традиційній телефонній системі

Для забезпечення безвтратної передачі електричного сигналу через дроти на великі відстані використовувалися електричні підсилювачі. На завершення передачі електричний сигнал перетворювався у звуковий за допомогою акустичного динаміка рис.3.2.

Рисунок 3.2 – Голосова комунікація через аналоговий електричний канал

Протягом розвитку технології телефонії, мікрофон та динамік залишалися сталими компонентами, не зазнаючи принципових змін. Проте інші елементи системи піддавались постійним вдосконаленням. Сигнал, що передавався через мережу, спочатку був аналоговим, і змінювався в залежності від сили акустичного тиску, генерованого голосом. Така технологія отримала назву "аналогова телефонія". На великі відстані якість передачі голосу погіршувалася через шуми та спотворення, а також через втрату сигналу від проміжних підсилювачів. Проблему вирішено за допомогою переходу до цифрового коду для передачі голосу рис.3.3 [8]. Голосовий сигнал перетворюється у цифровий код через аналогово-цифровий перетворювач (АЦП), а потім зворотно у звук через цифро-аналоговий перетворювач (ЦАП). Цифровий зв'язок значно покращив якість передачі голосу, оскільки цифровий сигнал не піддається впливу шумів та спотворень, які характерні для аналогових мереж. Сьогодні цифровий зв'язок переважає, замінюючи застарілі аналогові системи.

Рисунок 3.3 – Голосова комунікація з використанням цифрової технології передачі сигналу

Для забезпечення зв'язку між багатьма абонентами у телефонній мережі використовується комутація, що дозволяє операторові створювати шлях передачі голосу між абонентами, об'єднуючи ділянки мережі у єдиний канал. У цифровій формі голосовий сигнал передається як послідовність цифрових відліків замість неперервного

аналогового сигналу. Ця технологія, відома як часове мультиплексування (TDM), рис. 3.4 дозволяє передавати декілька розмов через один канал, оптимізуючи використання ресурсів мережі.

Рисунок 3.4 – Оптимізована передача голосових даних за допомогою технології TDM

Технологія голосової передачі по мережах IP, відома як Voice-over-IP (VoIP), є ключовою складовою сучасних IP-телефонних систем. Окрім голосової передачі, IP-телефонія включає також сигналізаційні функції.

IP-телефонія, що ґрунтується на технології VoIP, швидко стала популярною завдяки ряду переваг 7 у порівнянні з традиційною телефонією:

– ефективне використання ресурсів мережі: передача голосу через IP-пакети дозволяє оптимізувати використання каналів зв'язку та обладнання без потреби у спеціальному резервуванні ресурсів;

– зниження вартості міжнародних дзвінків: відміна резервування ресурсів на дорогих проміжних TDM-комутаторах дозволяє перейти до сплати за підключення до Інтернету, що зменшує витрати на дзвінки на великі відстані;

– єдина технологічна база: IP-телефонія дозволяє використовувати однакові комутатори, маршрутизатори та сервери для обробки як голосових, так і даних;

– розширені можливості для користувачів: інтеграція телефонії та Інтернету відкриває широкий спектр нових сервісів та додаткових послуг для абонентів.

Рисунок 3.5 – Взаємодія мереж традиційної телефонії та IP-телефонії

Рисунок 3.6 – Процес перетворення аналогового сигналу у цифрову форму

Рисунок 3.7 – Процес присвоєння цифрового коду кожному відліку

Для покращення якості кодування відліків потрібно використовувати більшу кількість розрядів. Наприклад, на цифрових аудіодисках відліки зазвичай кодуються за допомогою 16-бітних двійкових кодів. У телефонії для кодування голосу часто використовуються 8-бітні коди.

Компресія динамічного діапазону використовує нелінійну функцію кодування відліків. Замість лінійної функції, де кожне значення відповідає однаковому рівню кодування, застосовується нелінійна функція, яка ефективно використовує сітку можливих значень кодів. Оскільки більшість сигналів знаходиться в середньому діапазоні, а сплески менш часті, ця стратегія зберігає більше інформації про сигнал.

Ефективніше кодування можливе за допомогою нелінійної функції кодування, де для середнього діапазону сигналу використовується більш щільна сітка значень, ніж для сплесків. Це дозволяє оптимізувати використання значень кодів.

Цифрове перетворення аналогового сигналу, відоме як імпульсно-кодова модуляція (PCM), є ключовою процедурою у звуковій технології. У форматі PCM аналоговий сигнал представляється у вигляді 8-бітових цифрових кодів, які передаються з частотою 8000 за секунду.

Термін «кодек» походить від слів «кодування» та «декодування» і використовується для опису набору функцій, які забезпечують зменшення обсягу голосових даних, що передаються, шляхом кодування та декодування цих даних на різних кінцях передачі.

Існує широкий спектр кодеків, які відрізняються за рівнем стиснення даних, складністю обробки, впливом на якість сигналу та оптимальними умовами використання. Деякі з них мають стандартний статус і описані в документах Міжнародного Телекомунікаційного Союзу (ITU), що позначені кодами виду G.7xx (наприклад, G.711, G.726, G.729 та інші). Також існують пропрієтарні кодеки, які потребують використання обладнання певного виробника на обох кінцях передачі голосових даних. У табл. 3.1 наведені характеристики деяких поширених кодеків [13].

При передачі голосу через мережі VoIP важно враховувати, що окрім цифрових відліків передається також службова інформація, яка включає заголовки IP-пакетів і фреймів канального рівня. Для оцінки потрібної пропускної здатності мережі необхідно враховувати не лише значення, вказані в табл. 3.1, але й додаткову пропускну здатність для передачі цієї службової інформації.

Наприклад, можемо розглянути розрахунок потрібної пропускної здатності Ethernet мережі для передачі однієї голосової розмови з використанням кодеку G.711 [8].

Умови передачі:

– часовий інтервал фрагменту голосової розмови, що передається одним пакетом IP (визначає затримку голосового сигналу) – 20 мілісекунд;

– розмір заголовка контейнера протоколу RTP (Real-time Transport Protocol) - 12 байт;

– розмір заголовка датаграми UDP (User Datagram Protocol) – 8 байт;

– розмір заголовка пакета IP - 20 байт;

– розмір заголовка та контрольної інформації Ethernet-фрейму – 18 байт.

3 Передача фрагментів кожні 20 мілісекунд вимагає їх відправки з частотою 1 / 0.02 = 50 пакетів на секунду. Таким чином, передача 50 пакетів 3 розміром 218 байт на секунду потребує пропускної здатності мережі 10900 байт/с або 87.2 Кбіт/с.

Як можна помітити, реальна потреба в пропускній здатності (87,2 Кбіт/с) перевищує швидкість, необхідну 3 для передачі лише голосових даних (64 Кбіт/с) на 36%. Це пояснюється тим, що крім голосових даних 3 також передаються пакети з додатковою інформацією через протокол RTCP (Real-Time Control Protocol), яка, однак, має невеликий 3 внесок в загальну пропускну здатність мережі.

3 При 3 використанні 3 кодеків з високим ступенем стиснення голосових даних, таких як G.729a, який передає голос із швидкістю 8 Кбіт/с, накладні витрати стають ще вищими. Наприклад, для фрагменту 3 тривалістю 20 мс пропускна здатність складе 31,2 Кбіт/с, що відповідає зростанню накладних витрат на 290%. Якщо тривалість фрагменту збільшити 3 до 30 мс, пропускна здатність зменшиться до 23,5 Кбіт/с, що все ще становить 193% від необхідної пропускної здатності. Незважаючи на це, в порівнянні з кодеком G.711, 21 який використовується для передачі голосових даних з швидкістю 64 Кбіт/с, економія все одно залишається значною – 23,5 Кбіт/с проти 87,2 Кбіт/с для кожного голосового з'єднання.

Важливо враховувати, що для ефективної комунікації між абонентами важливо, щоб їхні пристрої підтримували однакові кодеки. Відсутність відповідності кодеків вимагає перетворення між ними під час передачі голосових даних. Ця процедура може збільшити затримку сигналу і погіршити його якість. Зазвичай у телефонних мережах встановлюється єдиний базовий кодек для всіх розмов, що полегшує взаємодію. У випадку зв'язку між абонентами різних мереж із різними кодеками необхідно забезпечити підтримку обох кодеків кінцевими пристроями абонентів або виконати конвертацію кодеків на межі мережі. Для передачі голосу через мережевий протокол IP між VoIP-шлюзами абонентів використовуються раніше згадані протоколи RTP та RTCP.

Індустріальний стандарт ITU H.323 став першим широко використовуваним протоколом службової сигналізації. Початково розроблений для відеоконференцій в IP-мережах, протокол H.323 швидко став основою 1 для всіх типових сценаріїв IP-телефонії. Його гнучкість дозволяла використовувати його як у мережах з виділеними 1 контролерами зон, так і в універсальних 1 шлюзах, що поєднували 1 функції передачі голосу та сигналізації.

1 У простіших випадках SIP може забезпечувати взаємодію між двома кінцевими пристроями, наприклад, голосовими шлюзами, 1 без додаткових елементів керування. Також, за відміну від MGCP, SIP дозволяє більшу інтелектуальну взаємодію між кінцевими пристроями та може керувати передачею викликів через багато проміжних пристрої.

Порівняно з протоколом H.323, який також здатен підтримувати симетричну взаємодію, SIP пропонує додаткові можливості:

– знаходження фактичного місця підключення (реєстрації) користувача в телефонній мережі, що дозволяє підтримувати мобільних користувачів;

– обмін інформацією щодо підтримуваних функцій між пристроями, які беруть участь у сеансі зв'язку, що забезпечує ефективну взаємодію між пристроями різних виробників та узгоджене впровадження підтримки нових функцій;

– визначення готовності абонента, якого викликають, до початку сеансу взаємодії;

– можливість динамічної зміни параметрів виклику під час сеансу взаємодії, наприклад, додавання та вилучення учасників.

SIP володіє спрощеною системою службових повідомлень у порівнянні з H.323. Ці повідомлення передаються у вигляді простого тексту, аналогічно до протоколу передачі гіпертексту HTTP. В якості транспортного протоколу часто використовується UDP, що має менше накладних витрат порівняно з TCP.

Основними компонентами мережі на основі SIP є такі (рис. 3.8) [12]:

– Агент користувача (User Agent) – це модуль, що інтерактивно працює з агентами користувача інших пристроїв. Він може виступати як клієнт, що ініціює взаємодію, або сервер, що відповідає на запити.

– Сервер реєстрації (Registrar) – це компонент, який зберігає інформацію про доступні агенти користувача в мережі і надає можливість їхнього пошуку.

– Проксі-сервер (Proxy Server) – це посередник на шляху передачі виклику, який маршрутизує його і виконує різноманітні технологічні та безпекові функції.

– Сервер переадресації (Redirect Server) – це агент користувача, що вказує на необхідність перенаправлення запиту до іншого агента користувача, наприклад, в іншій мережі.

Рисунок 3.8 – Компоненти інфраструктури мережі, що базується на протоколі SIP

3.2 Аналіз ризику нелегітимного доступу до безпечної IP-телефонії

Оцінка загроз нелегітимного доступу до безпечної IP-телефонії. Аналіз ймовірності успішної атаки нелегітимним користувачем.

Рівень потенційних загроз для інформаційної безпеки враховується через 1 модель нелегітимного користувача. Розглянемо таку модель, де нелегітимні користувачі, такі як сторонні особи, представники 1 іноземних держав, агенти розвідувальних служб або злочинні організації, не мають відповідного доступу до послуг IP-телефонії."

1 Для аналізу моделі нелегітимного користувача ми спробуємо з'ясувати їхні цілі та мотивацію. Сформулюємо декілька потенційних цілей, які можуть переслідувати такі користувачі, проводячи 1 атаки для отримання несанкціонованого доступу до даних IP-телефонії. Зокрема, ми визначимо Ціль_О (отримання доступу 1 до обладнання оператора) та Ціль_М (отримання доступу до моніторингу абонентів). Усі цілі спрямовані на незаконне 1 отримання доступу до потоку даних IP-телефонії."

Після аналізу алгоритмів, які можуть бути використані нелегітимними користувачами, ми розробимо 1 модель порушника інформаційної безпеки для кожної з вищезазначених цілей."

Давайте розглянемо сценарій захоплення обладнання оператора нелегітимним користувачем. Цей користувач працює над активними атаками з метою 1 отримання несанкціонованого доступу до даних IP-телефонії. Успішний результат такої атаки означатиме 1 захоплення обладнання оператора.

1 Рисунок 3.9 1 – Можливий сценарій 1 дій нелегітимного користувача під 1 час 1 атаки на обладнання оператора з 1 метою захоплення контролю

1 Сценарій 1 дій нелегітимного користувача відображено на рис. 3.9. Для ініціювання атаки, зловмиснику потрібно спочатку визначити, 1 на який саме сервіс IP-телефонії 1 він планує здійснити 1 активну атаку. Один з можливих методів - використання команди tracert для отримання інформації про 1 проміжні вузли між об’єктом атаки та самим зловмисником. Ця інформація дозволить зловмиснику виявити вузли, які беруть участь у поточному обміні даними між абонентами.

Після вибору сервісу IP-телефонії зловмиснику слід спробувати отримати контроль над цим сервісом. Один з методів цього може включати активну атаку, таку як перебір паролю. Однак за наявності 1 списків доступу (ACL) у оператора, віддалене управління може бути технічно недоступним 1 для зловмисника. 1 Ймовірність проведення активної атаки на сервіси IP-телефонії при наявності ACL в оператора визначається як p12, а ймовірність наявності віддаленого 1 підключення до сервісів IP-телефонії визначається як p13, що є оберненою подією до 1 p12 [7].

1 Для виконання активної атаки віддаленого управління сервісами IP-телефонії, зловмиснику слід вибрати доступний протокол (наприклад, 1 telnet, http або https, 1 ssh, SNMP) для атак 1 типу «перебір пароля». Для визначення ймовірності успішного

завершення атаки «перебір пароля» за певний час, необхідно розрахувати формулу:

????34зх_о = ??????????????(????, ????, ????, ????),(3.1)

де L – кількість символів у логіні 1 чи паролі;

1 T – час, що 1 був відведений 1 для успішного завершення атаки, тобто для 1 перебору 1 пароля;

1 D – механізми, програмно-апаратні та технічні можливості порушника, а також обмеження IP-протоколу, які ускладнюють або унеможливлюють 1 успішне завершення атаки "перебір пароля" за відведений час;

1 C – швидкість каналу зв'язку Інтернет мережі, при виконанні атаки зловмисником;

1 p34зх_о – ймовірність успішного завершення активної атаки "перебір пароля" і надання нелегітимному користувачеві доступу 1 до обладнання оператора;

1 p32 – ймовірність того, що атака "перебір пароля" завершилася неуспішно протягом відведеного для неї часу.

1 Несанкціонований доступ до потоку даних IP-телефонії може бути отриманий зловмисником, якщо він успішно захопить віддалене управління сервісами. Це може статися через один із наступних способів:

1) здійснення атаки "перебір пароля" для доступу до медіатрафіку, що передається через Інтернет, та прослуховування цього трафіку;

2) атака на 1 механізм програмного розмоділу загальної секретної інформації, наприклад, ключів, для отримання можливості дешифрування трафіку.

Однак успішність таких атак може не завжди привести зловмисника до його основної мети. Якщо він не 1 може виконати атаку "Зустріч по середині" і налаштувати 1 обладнання оператора для пропуску трафіку 1 через своє обладнання, то ці атаки можуть виявитися малоефективними.

Для визначення ймовірності 1 успішної атаки нелегітимним користувачем на медіа-трафік з 1 метою 1 отримання несанкціонованого доступу до потоку даних (для атаки "зустріч по середині" 1 або 1 організації проксінгу) можна скористатися наступною формулою:

(3.2)

Активна атака з боку несанкціонованого користувача включає у себе втручання у

маршрутизацію потоку даних, що передаються у вигляді 1 пакетів мультимедійних файлів. Це 1 дозволяє зловмиснику перенаправляти трафік 1 через своє обладнання.

1 Імовірність p57 – успішна атака «підбір пароля» несанкціонованого користувача до переданого медіатрафіку. Підступник отримує змогу перехоплювати потік даних IP-телефонії або 1 атакувати механізм програмного розподілу секретних ключів, що 1 дозволяє йому розшифрувати 1 трафік за допомогою цих ключів.

1 Імовірність p52 – спроба атаки на пароль, проведена над переданим через Інтернет медіа-трафіком, завершилася невдачею. Час збереження актуальності даних (Тзб_акт) визначається призначенням цих даних. Час, 1 необхідний для успішного підбору 1 пароля (Тпд), 1 залежить від технічних можливостей та ресурсів, які доступні атакуючому, включаючи потужність обладнання (Рот), застосовані криптографічні методи (Ркрипт), довжину ключа (Рдовж), а також додаткові заходи ускладнення, такі як використання додаткових лічильників і т.п. (Рдодат).

????57 = ??????????????(????злв_акт, ????злв_прл) =

=??????????????(????злв_акт, 1 ЗЛВпотуж, ЗЛВкрипт, ЗЛВдовж, ЗЛВптж)(3.3)

????52 = 1 - ????57(3.4)

Імовірність p67 відображає ймовірність успішної атаки 1 на механізм програмного розподілу секретних ключів, а 1 також дешифрації трафіку з використанням 1 отриманої секретної інформації через механізм розподілу ключів. У 1 випадку, коли зловмисник втручається 1 в канал зв’язку під 1 час 1 обміну секретною інформацією між користувачами IP-телефонії, ця ситуація розглядається як атака. Нелегітимний абонент має можливість створити по два секретних ключа 1 для обміну інформацією з кожним абонентом незалежно один від одного. Використовуючи 1 цю секретну інформацію, зловмисник 1 може шифрувати та дешифрувати потік 1 даних, включаючи 1 мультимедійні дані під час розмови двох користувачів IP-телефонії. 1 Ймовірність успішної атаки 1 "зустріч по середині" на протокол розподілу секретної інформації між користувачами IP-телефонії залежить від потужності технічних та програмних засобів, що використовуються зловмисником.

Необхідно 1 врахувати, що для проведення активної атаки зловмисник 1 мусить розробити 1 відповідне програмне забезпечення. Імовірність p62 визначається 1 як ймовірність неуспішної 1 атаки типу «зустріч по середині», що здійснюється нелегітимним абонентом:

????62 = 1 - ????67(3.5)

1 На рис. 3.3 наведено імовірнісний граф, який ілюструє можливий алгоритм дій

зловмисника під час 1 атаки типу «зустріч по середині». Для 1 аналізу цього алгоритму використовується 1 математичний апарат теорії імовірнісних графів. Він допомагає отримати інформацію, що сприяє оцінці часу, необхідного для 1 успішного завершення атаки, а також ймовірності її успішності. Імовірнісний граф у цьому випадку допомагає отримати утворюючу функцію і розв'язати задачу переходу системи від початкового стану до кінцевого. Кожна гілка графа відповідає певній утворюючій функції.

Після 1 аналізу можливих дій зловмисника 1 отримано результат, який дозволяє 1 оцінити ймовірність отримання несанкціонованого доступу до конфіденційної інформації. Відповідний граф 1 представлено на рис. 3.10. 1 У цьому графі для гілки, що відповідає успішному виконанню атаки з метою 1 отримання несанкціонованого доступу до потоку даних IP-телефонії, складено утворюючу функцію H(x). Для імовірнісного 1 графа, показаного на рис. 3.2, представлено Рнсд = H(x=1).

????нсдц = ????13????34(????45????57 + ????46????67),(3.6)

1 де Pij – ймовірність переходу з вершини і графу в вершину j.

1 Рисунок 3.10 – Граф імовірностей дій під час атаки на захоплення обладнання оператора, яку виконує незаконний користувач

1 Алгоритм можливих дій зловмисника 1 під час цієї атаки відображений 1 на рис. 3.11. Результати аналізу дозволили докладніше розглянути різновиди атак, які може здійснити нелегітимний абонент, залежно від того, чи має він доступ 1 до шлюзу чи персонального комп'ютера користувача. Якщо зловмисник має доступ до шлюзу, найбільш 1 ймовірним є здійснення 1 активної атаки з проксінгом всього трафіку за 1 допомогою обладнання зловмисника. Ця 1 атака виконується за схемою, показаною на рис. 3.12. На цій схемі зображені IP1 та IP2, 1 що є шлюзами користувача, а SH є сервером зловмисника, де встановлено спеціалізоване програмне забезпечення.

Рисунок 3.11 – Сценарій можливих дій у випадку атаки на захоплення монітора 1 користувача зловмисником

1 Для вдалого завершення цієї атаки, зловмиснику спочатку потрібно 1 отримати доступ до монітора користувача та отримати контроль над управлінням VoIP монітором. Після цього необхідно встановити та налаштувати відповідне спеціалізоване програмне забезпечення.

Рисунок 3.12 – Під час атаки на захоплення монітора, варіанти використання проксінгу включають: а) передача 1 загальної секретної інформації та б) налагодження захищеного каналу для голосової комунікації

1 Якщо зловмисник використовує VoIP монітор з програмним шлюзом IP-телефонії, найбільш імовірним варіантом 1 активної атаки є наступне:

Зловмисник може здійснити атаку з проксінгом, перенаправляючи потік 1 медіа-трафіку користувачів через свій сервер, позначений як SH. Використовуючи цю атаку, зловмисник може встановити спеціалізоване програмне забезпечення 1 на VoIP моніторі, що 1 дозволить передавати голосову інформацію 1 у відкритому вигляді з монітора 1 або перехоплювати пакети 1 з мережевого інтерфейсу IP-телефонії. Ці дані потім будуть відправлені на сервер зловмисника для подальшої маніпуляції. Для цього зловмиснику потрібно 1 вимкнути на VoIP моніторі IP-протоколи безпеки або змінити налаштування протокола IP-телефонії SRTP, а також 1 відключити опцію шифрування голосової 1 інформації.

1 Це показує, що успішність 1 атаки залежить від кількох факторів, включаючи рівень захисту IP-телефонії та потужність 1 спеціалізованого програмного забезпечення та методів взлому, використаних зловмисником. Ймовірність успішної атаки можна представити як наступне: P34зм_м = [1, 0], де 1 вказує на наявність віддаленого управління на терміналі користувача без 1 налаштованого списку ACL на всі віддалені протоколи, а 0 вказує на включене віддалене управління з налаштованими списками 1 ACL на всі віддалені протоколи або на відсутність віддаленого управління взагалі. Якщо віддалене управління доступне, зловмиснику потрібно використовувати спеціалізоване ПЗ для підбору логіну/пароля для доступу на монітор користувача VoIP. Імовірність успіху такої 1 атаки залежить від рівня захисту IP-телефонії та методів взлому, використаних зловмисником визачається за формулою:

????42зах_м = ??????????????(????, ????, ????, ????)(3.7)

де L – кількість символів у логіні/паролі;

T – максимальний час, який зловмисник може витратити на 1 перебір для успішної атаки;

1 D – 8 додаткові заходи та засоби, що ускладнюють атаку перебором пароля протягом виділеного часу, а також технічні можливості зловмисника;

C – швидкість передачі даних по каналу зв'язку Інтернету мережі IP-телефонії 8 під час виконання атаки.

8 У разі успішного перехоплення 8 пароля та 8 отримання доступу до VoIP монітора 8 користувача, зловмисник може незаконно звернутися 8 до потоку даних IP-телефонії через один із двох методів: внедрення програмної вразливості в спеціалізоване ПЗ користувача або 8 модифікація програмного забезпечення VoIP монітора; налаштування VoIP монітора користувача; проведення 1 атаки типу "зустріч

по середині" на всі 8 протоколи безпеки IP-телефонії. Можливість успішної 1 атаки залежить від рівня забезпечення технічними та програмними засобами зловмисника.

Перша атака дозволяє зловмиснику перехопити голосові дані, обходячи IP-протоколи або впливаючи на режим роботи або відключаючи їх. Друга атака дозволяє змінити налаштування VoIP монітора користувача для проведення атаки 1 "зустріч по середині". Під час цієї атаки зловмисник по черзі підключається до кожного абонента, використовуючи IP-протоколи безпеки IP-телефонії. Дана схема 1 зображена на рис. 3.13.

1 Рисунок 3.13 – Стратегія 1 виконання атаки 1 «зустріч по середині» на захищені протоколи IP-телефонії

При виборі будь-якої 1 з перерахованих атак, зловмисник може мати можливість незаконно отримати доступ 8 до потоку даних, якщо атака завершиться успішно. Проте існує ризик невдачі обраної атаки, який відображається ймовірностями p72 і p62 відповідно. Крім того, якщо користувач помітить зміни в налаштуваннях VoIP-монітора, змінить паролі доступу та відключить віддалене управління, відновивши налаштування, атака типу «модифікація налаштувань» також буде неуспішною. Згідно 1 аналізу можливих дій нелегітимного абонента, був 1 побудований ймовірнісний граф, який 1 зображено на рис. 3.14.

1 Рисунок 3.14 – Граф імовірностей можливих дій зловмисника під час здійснення атаки на захоплення VoIP-монітора

У цьому графі представлений шлях, що вказує на успішне завершення атаки для отримання несанкціонованого доступу до потоку даних. Для цієї гілки була розроблена функція H(x). Для графа імовірностей, показаного на рис. 3.14, ймовірність успішного завершення атаки позначається як Рнсд і обчислюється за значенням H(x=1):

Рнсдц(зх_м) = p13p34(p45p58 + p46p68 + p47p78)(3.8)

1 де Pij – ймовірність переходу з вершини і графа в вершину j.

1 Для аналізу ймовірносно-часових характеристик необхідно ретельно розглянути та оцінити протоколи, що використовуються 1 для розподілу загальної секретної інформації (ключів) у захищеній IP-телефонії. Вони повинні відповідати певним вимогам, а саме:

1 – протокол має підтримувати 1 різноманітні топології, такі як 1 клієнт-сервер та клієнт-клієнт, у 1 Інтернет-мережах IP-телефонії;

1 – протокол може функціонувати між абонентами без потреби 1 у використанні

додаткових IP-протоколів 1 для розподілу загальної секретної інформації (ключів);

1 – 1 протокол може 1 працювати без передачі секретної інформації у відкритому вигляді по 1 каналах зв'язку;

1 – протокол має вбудований механізм виявлення атак типу "зустріч по середині" без необхідності 1 передплати 1 секретних ключів між користувачами або 1 використання сертифікатів;

1 – протокол використовує TCP/UDP порти, що визначені у стеку протоколів для IP-телефонії, такі як SIP/RTP, або інші порти, які встановлюються в результаті узгодження при підключенні.

1 Порівняння IP - протоколів по вище вказаним критеріям зображено в табл. 3.2.

1 Фінальну оцінку нашого аналізу кожного з протоколів визначимо за формулою:

1 5

????ПРК: ????ПРК = □ ????????(3.9)

????=1

Враховуючи результати аналізу, представлені в табл. 3.2, можемо рекомендувати використання IP-протоколів ZRTP і DTLS. Ці протоколи мають найкращі показники QПРК. Проте, зауважимо, що найбільш поширені IP-протоколи 2 розподілу секретних ключів потребують покращень як у своїх базових характеристиках, так і у забезпеченні інформаційної безпеки IP-телефонії.

Для забезпечення безпеки IP-протоколу 2 розподілу секретних ключів рекомендується 2 вживання 2 кількох паралельних незалежних каналів сеансів зв'язку в Інтернет-мережах IP-телефонії. Ці канали мають бути повністю незалежними один від одного, щоб у разі захоплення зловмисником одного каналу не давали йому можливості одночасно атакувати інші.

3.3 Підвищення ефективності IP-протоколу 2 ZRTP за допомогою автоматизованої перевірки аутентифікаційного рядка

2 Для запобігання успішним атакам на асиметричний алгоритм 2 Діффі-Хелмана під час обміну секретною інформацією, необхідно 2 забезпечити захищені канали 2 передачі голосової інформації. Використання протоколу Діффі-Хелмана у захищених каналах дозволить уникнути несанкціонованого доступу, 2 модифікації чи заміни даних. Однак, може виникнути ситуація, коли два абоненти, які не мають 2 загальних сертифікатів або протоколів секретної інформації, спробують 2 встановити захищене

з’єднання без 2 захищеного каналу для встановлення зв’язку один з одним[15].

У ситуації, коли абоненти мають сертифікати від 2 різних центрів сертифікації, перевірка достовірності кожного сертифікату стає складною, оскільки кожен абонент може не довіряти 2 центру сертифікації іншого. Для встановлення захищеного зв’язку 2 між ними необхідно 2 згенерувати та розподілити секретну інформацію (ключі). У таких ситуаціях можуть застосовуватись як асиметричні, так і 2 симетричні алгоритми шифрування. Але 2 використання 2 симетричного шифрування має ризик, оскільки ключі потрібно передавати по відкритим каналам зв’язку, що може дозволити нелегітимному абоненту отримати доступ до голосової інформації. Використання асиметричного шифрування забезпечує безпеку переданої інформації, але при обміні відкритими ключами користувачі не можуть бути впевнені, що ключ передається між ними без модифікацій нелегітимним абонентом, як показано на рис. 3.15.

Рисунок 3.15 – Ситуація, коли атака «зустріч по середині» стає можливою під час використання асиметричного шифрування

Використання асиметричного шифрування має свої обмеження через великий розмір відкритого та секретного ключів, що ускладнює їх передавання через Інтернет. Для підвищення безпеки можна застосувати такі методи: перевірку аутентифікаційного рядка SAS абонентів за допомогою додаткового каналу зв'язку, використання декількох каналів зв'язку для передачі секретних ключів.

У сценарії клієнт-клієнт захист від зловмисника можна забезпечити за рахунок перевірки аутентифікаційного рядка абонентів із застосуванням додаткового каналу зв'язку. Однак автоматизація цього процесу на сьогодні не може гарантувати потрібного рівня безпеки, оскільки використовується лише один канал зв'язку між абонентами сесії IP-телефонії. Крім того, існують засоби аналізу і синтезу голосових даних, які можуть бути використані зловмисником для викрадення чи модифікації інформації в потоці даних.

В результаті аналізу і досліджень виявлено, що існує значна ймовірність наявності незалежних каналів зв'язку між абонентами, які не перетинаються. Дослідження показали перевагу легітимних абонентів над нелегітимними, оскільки вони мають доступ до голосових даних з кількох каналів одночасно. Пропонований метод покращення алгоритмів розподілу секретних ключів не забезпечує абсолютної безпеки, але сприятиме підвищенню захищеності даних. Для оцінки ефективності покращення алгоритму можна використовувати такі критерії ймовірності: ймовірність успішної атаки «зустріч по середині», ймовірність виявлення цієї атаки та ймовірність успішного генерування та розподілення секретного ключа.

Протокол ZRTP вбудовує механізм захисту від активних атак типу «зустріч по середині». Цей механізм використовує вербальну перевірку короткого аутентифікаційного рядка SAS через голосовий канал між абонентами сесії. Користувачі, що проводять сесію без сервера в топології клієнт-клієнт, отримують аутентифікаційний рядок SAS, який вимовляється одним із учасників і порівнюється з візуальною версією іншим учасником на екрані свого VoIP-пристрою. У разі збігу рядків, можна впевнено стверджувати відсутність активної атаки. Однак існує ризик підробки аутентифікаційного рядка через голосовий канал, і у випадку незбігу рядків може бути виявлена активна атака. При з’єднанні двох абонентів без сервера, автентифікація здійснюється на основі відомих голосових характеристик іншого абонента та немодифікованої передачі даних по двом каналам: для голосового зв’язку і передачі даних SRTP.

За допомогою сучасних технологій та програмно-апаратного забезпечення можна легко аналізувати голос учасників сесії зв’язку та проводити аналіз їх голосу. Проте важливо враховувати дві можливі ситуації. В першій, коли абоненти знають характеристики голосових даних один одного, вербальна перевірка аутентифікаційного рядка SAS може бути уразливою до атаки, оскільки голосова інформація може бути синтезована для модифікації рядка SAS. У другій ситуації, коли учасники сесії не мають інформації про голос один одного, синтез голосу може бути виконаний за умови наявності будь-яких голосових даних. Для покращення захисту протоколу ZRTP може бути використана автоматизована програмно-апаратна перевірка аутентифікаційного рядка SAS, особливо при використанні декількох каналів зв’язку, що дозволяє виявляти порушників інформаційної безпеки рис.3.16.

Рисунок 3.16 – Можливість заміни аутентифікаційного рядка зловмисником під час передачі через голосовий канал зв'язку

Посилання

Це джерела виділених збігів у вашому документі. Кожен збіг позначено темно-зеленим числом, яке відповідає вказаному тут джерелу. Джерела впорядковані за схожістю — чим вищий бал, тим сильніше збіг.

#	Джерело	%
1	ela.kpi.ua	11.0%
2	ela.kpi.ua	0.9%
3	ekmair.ukma.edu.ua	0.6%
4	conference.cyberspace.org.ua	0.5%
5	elar.khnu.km.ua	0.4%
6	ir.library.knu.ua	0.4%
7	repository.hneu.edu.ua	0.4%
8	elar.khnu.km.ua	0.3%
9	researchgate.net	0.3%
10	dspace.zsmu.edu.ua	0.3%
11	itcj.sethost.net	0.3%
12	csecurity.kubg.edu.ua	0.2%
13	ela.kpi.ua	0.2%
14	metod.suitt.edu.ua	0.2%
15	core.ac.uk	0.2%
16	zhu.edu.ua	0.2%
17	mil.univ.kiev.ua	0.2%
18	ekhnuir.karazin.ua	0.1%
19	cqr.company	0.1%
20	duikt.edu.ua	0.1%
21	lib.iitta.gov.ua	0.1%
22	dspace.wunu.edu.ua	0.1%
23	lviv-forum.inf.ua	0.1%

#	Джерело	%
24	lib.kart.edu.ua	0.1%
25	zakon.rada.gov.ua	0.1%
26	economy.in.ua	0.1%
27	dqsglobal.com	0.1%

Plag

Дякуємо, що перевірили
свій документ за допомогою
Plag!