МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРАКОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 2020 р

На правах рукопису
УДК 004.056.5.51.22(043.3)

ДИПЛОМНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Удосконалений модуль багатофакторної аутентифікації на базі NGFW компанії

Автор: І. О. Мервінський

Науковий керівник: к.т.н., доц. Н. К. Гулак

Нормоконтролер: к.т.н., доц. Н. К. Гулак

Київ 2020

ВСТУП

Актуальність.

На сьогодення захист інформації, носів та систем є однією з основних складових, але методів не так багато і основними проблемами становить не тількі інстальовані віруси чи шифратори, а й крадіжка персональних паролей або їх зчитування за допомогою спеціальних систем, враховуючи людський фактор коли може людина проговоритись, пароль може основуватись на персональних даних або просто десь записаний.

Тому необхідні додаткові методи аутентифікації, не тільки для випадків втрати паролю або його скомпрементування, а також як альтернативний метод атеризації, якщо забутий основний пароль.

Дані методи становляться дуже популярними на сьогодення, коли велика кількість людей працює вдома.

Відомі підходи до вирішення поставленої задачі.

Існує наступна класифікація методів аутентифікації: Однофакторна або багатофакторна. Однафаткорний метод полягає в тому, що б використовувати один з наступних наведених методів авторизації: Парольний – Полягає в індентифікації за допомогою паролю персонального або спеціально виданого, Ідентифікаційний – коли ідентифікацію суб’єкта підтверджує спеціальна система чи пристрій, Біометричний – коли індетифікація відбувається на основі порівняння еталоних даних персональних характеристик суб’єкта з вхідними даними знятті за допомоги сканеру.

Метою роботи є вибір логічних методів для багатофакторної аутентифікації щоб підвисити захист інформації від несанкціонованого доступу за рахунок розробки коду та проведення розрахунок коефіцієнту можливості проникнення в систему.

Для досягнення поставленої мети вирішуються такі **задачі:**

- Аналіз нормативно-правової бази України в галузі інформаційної безпеки;

- Проведення аналізу загроз інформаційній безпеці, каналів витоку інформації та методів аутентифікації;
- Розробка та налаштування конфігурації віртуальної системи з використанням обладнання NGFW.
- Розробка програмного продукта для підвищення рівня захищеності від несанкціонованого доступу і проведення апробації та розрахунку коефіцієнта.

Галузь застосування. Розроблений програмний продукт використовується в інформаційних системах та мобільному зв'язку і відноситься до галузі інформаційних технологій для підвищення рівня захищеності від несанкціонованого доступу.

Об'єктом дослідження є процес захисту інформації від несанкціонованого доступу.

Предметом дослідження є методи аутентифікації в інформаційних системах.

Методи дослідження базуються на основі нечіткої логіки (для розробки методу аналізу та оцінки ризиків), та об'єктно-орієнтованого програмування (для програмної реалізації розробленого методу).

Новизна одержаних результатів полягає в наступному:

- на основі обладнання NGFW була розроблена та налаштована конфігурація віртуальної машини для практичної апробації розробленого нового програмного продукту який був використаний в багатофакторній аутентифікації для підвищення ступені захисту від несанкціонованого доступу.

Практична цінність отриманих результатів:

- розроблено та налаштовано конфігурацію віртуальної машини на основі обладнання NGFW;
- розроблено програмний продукт для багатофакторної аутентифікації який дає можливість отримати підвищення захисту інформації, за розрахунками, вірогідність отримання несанкціонованого доступу 2,7%.

ЗМІСТ

РОЗДІЛ 1. НОРМАТИВНО-ПРАВОВА БАЗА УКРАЇНИ В СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ

В законодавчій базі існує основні закони, які регулюють та дають визначення існуючим поняттям, принципам, галузі використання.

1.1. Закон України «Про інформацію» №-2657-XII

Даний закон визначає основні принципи інформаційних відносин та державної інформаційної політики; суб'єктів та об'єктів інформаційної політики; право та гарантії права на інформацію; основні види інформаційної діяльності; відповідальність за порушення законодавства про інформацію. [1]

Даний закон дає опис наступним термінам, згідно статті 1:

- Документ – основною функцією є її зберігання даних та передача її у часі та просторі. Являє собою фізичний носій, диск, матеріал , тощо.
- Захист інформації – комплекс адміністративних, технічних, правових, організаційних та інших заходів , які можуть забезпечити збереження цілісності інформації.
- Інформація – певна кількість знань, які зберігаються , або можуть бути збережені на фізичних носіях або відтворені в цифровому вигляді.
- Суб'єкт владних повноважень – суб'єкт або орган влади, який здійснює керувальні функції згідно законодавства, враховуючи виконання делегованих доручень.

Друга стаття визначає основні принципи інформаційних відносин:

- Гарантованість права на інформацію;
- Відкритість до інформації з її свободою до обміну;
- Повнота інформації з достовірніст'ю;
- Свобода в виражені переконань та поглядів;
- законне отримання, зберігання з його поширенням, та захисту даних;
- захист особи від вторгнення в її особисте та сімейне життя.

Стаття третя вказує нам основні напрямки державної інформаційної політики.

- Забезпечення можливістю отриманні інформації для кожного громадянина;
- Забезпечення рівноцінних можливостей для утримання, створення, поширення, передачі, захисту, отримання інформації;
- Створення обставин для створення в Україні інформаційного суспільства;
- Гарантування відкритості та прозорості діяльності суб'єктів вище урядових повноважень.
- Створення та забезпечення інформаційних систем та мереж даних з його подальшим розвитком електронної держави.
- Забезпечення можливості регулярного оновлення, розширення та підтримка здатності роботоздатності національних інформаційних ресурсів.
- Забезпечення інформаційної безпеки України.
- Колоборація з міжнародними органами і інформаційній сфері та інтеграція України до світового інформаційного простору.

Стаття четверта нам розповідає про суб'єкти і об'єкти інформаційних відносин.

- Фізичні особи;
- Юридичні особи;
- Об'єднання громадян;
- Суб'єкти владних повноважень.

Об'єктом інформаційних відносин є інформація.

Стаття п'ята надає визначення щодо право на інформацію.

Кожен об'єкт має право доступу до інформації, що має на меті можливість вільного отримання, використання, передача, зберігання та захист даних(інформації), необхідної для втілення свої прав, законних інтересів та свободи.

Втілення права на інформацію не має права порушувати політичні, соціальні, громадські, економічні, духовні, екологічні, соціальні та інші права та законних інтересів та інтересів громадян та інтересів юридичних осіб.

Стаття шоста дає опис гарантії права на інформацію.

Право на інформацію забезпечується:

- Створенням механізму реалізації права на інформацію;
- Створенням нагод для вільного доступу до статистичних даних, архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів;
- Суб'єкти владних повноважень повинні інформувати громадськість та засоби масової інформації про свою діяльність з прийнятими рішеннями;
- Суб'єкти владних повноважень зобов’язані визначити спеціальні служби або відповідальних осіб для гарантованого доступу пошукачів (запитувачів) за інформацією;
- Втілення державного і громадського контролю за дотриманням законодавства про інформацію;
- Врегулювання відповідальності за порушення законодавства про інформацію.

Право на інформацію може обмежуватись законом в інтересах національної безпеки, громадського порядку та територіальної цілісності з метою запобігання правопорушень, криміналу, охорони здоров’я мешканців, захисту репутації або прав інших людей для запобігання розголошення інформації, яка може нанести шкоди або підтримки авторитету та безстороннього правосуддя.

В статті сьомій вказується основні принципи охорони права на інформацію.

1. Право на дані та інформацію охороняється законом. Держава забезпечує рівноправність всім суб’єктам інформаційних відносин і методи отримання інформації з його доступом до неї.

2. Ніхто не має право обмежувати права суб’єкта у виборі джерел отримання інформації, за винятком випадків, які передбачені законом.

3. Забороняється знищення та вилучення друкованих документів, експонатів, видань, інформаційних банків, інформаційних архівів з бібліотечних та музейних фондів, крім підстав, встановлених законом або рішенням суду.

4. Право на інформацію, створену в процесі діяльності фізичної чи юридичної особи, суб'єкта владних повноважень або за рахунок фізичної чи юридичної особи, Державного бюджету України, місцевого бюджету, охороняється в порядку, визначеному законом.

Стаття восьма описує мову інформації.

Мова даних формується законом про мови або іншими законами в цій сфері, міжнародними угодами або домовленостями, згодою на обов'язковість яких надана Верховною Радою України.

1.2. Закон України «Про державну таємницю» №- 3855-XII

Даний закон в першій статті дає опис наступним термінам,основні теміни будуть описані

- Державна таємниця або секретна інформація – клас (вид) таємної інформації, даних, що обсягає дані у сфері оборони, науки, державної безпеки ,економіки, техніки, зовнішніх відносин, охорони правопорядку, розголошення яких може завдати збитків національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою[2];
- Гриф секретності ;
- Криптографічний захист секретної інформації – вид захисту, що відбувається шляхом трансформація інформації з використанням спеціальних даних (ключових даних) з метою кодування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

- Технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та не сприяють блокуванню інформації.

Стаття друга описує законодавчі органи України про державну таємницю.

Відносини в галузі охорони державної таємниці встановлюються Конституцією України, законами України "Про інформацію" та "Про доступ до публічної інформації", цим Законом, міжнародним договорами згода на обов'язковість яких надана Верховною Радою України та іншими нормативно-правовими актами.

Стаття третя свідчить про сферу дії закону.

Дія цього Закону розглядається на законодавчі, виконавчі та судовоі органи влади, органи прокуратури України, інші урядові органи, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян (далі - державні органи, органи місцевого самоврядування, підприємства, установи та організації), що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці.

1.3. Положення про порядок здійснення криптографічного захисту інформації в Україні №-505/98

Цей документ визначає порядок здійснення криптографічногозахисту інформації з обмеженим доступом, розголошення якої завдає ,може завдати шкоди державі, уряду, суспільству або особі. Також дає опис наступним термінам, основні темніти будуть розтлумачені[3]:

- Криптографічний захист – вид технічного захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою кодування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

- Засіб криптографічного захисту інформації – програмний, апаратно-програмний, апаратний або інший засіб, який призначений для криптографічного захисту інформації;
- Криптографічна система (криптосистема) – сукупність засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої спеціалізованої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує необхідний рівень захищеності інформації, що передається, зберігається та обробляється;
- Система криптографічного захисту інформації – сукупність органів, методів, підрозділів, груп, діяльність яких спрямована на забезпечення криптографічного захисту інформації, та підприємств, установ і організацій, що розробляють, забезпечують, виробляють, експлуатують та розповсюджують криптосистеми і засоби криптографічного захисту інформації.

З метою визначення ступеня захищеності від несанкціонованого доступу до інформації з обмеженим доступом проводяться сертифікаційні випробування криптосистем з засобами криптографічного захисту.

Для криптографічного захисту інформації, що становить державну таємницю, службову інформацію, створену на замовлення державних органів або яка є власністю держави, використовуються криптосистеми і засобами криптографічного захисту, допущені до експлуатації.

Зазначені криптосистеми і методи перебувають у державній власності. Засоби криптографічного захисту службової інформації та криптосистеми з відповідного дозволу можуть перебувати також в недержавній власності.

1.4. НД ТЗІ 1.1-002-99 “Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу”.

Цей нормативний документ технічного захисту інформації , надалі НД ТЗІ визначає методологічну методику вирішення завдань захисту інформації в

комп'ютерних системах з створенням нормативних та методологічних документів, регламентуючих питань [4]:

- Визначення вимог захисту комп'ютерних систем від несанкціонованого доступу;
- Створення захищених комп'ютерних систем з засобами їх захисту від несанкціонованого доступу;
- Оцінки захищеності комп'ютерних систем , їх придатність для вирішення завдань кінцевого замовника.

Документ призначено для розробників, користувачів комп'ютерних систем, які використовуються для обробки важливо-критичної інформації, також для державних органів, що здійснюють функції контролю за обробкою такої інформації.

1.5. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

Терміни, що описуються цим документом, обов’язкові для застосування в усіх видах документації та літератури, що входять до системи технічного захисту інформації(надалі ТЗІ).

Для кожного поняття встановлено один термін. Застосування синонімів до термінів не допускається. Будуть розтлумачені тільки основні поняття [5].

- Автоматизована система, надалі АС — організаційно-технічна система, що реалізує інформаційну технологію і об’єднує ОС, фізичне середовище, персонал і інформацію, яка обробляється;
- Комп’ютерна система;
- Політика безпеки інформації— сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації;
- Загроза— будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС;
- Безпека інформації

- Захист інформації в АС— діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.
- Комплексна система захисту інформації, надалі КСЗІ — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.
- Комплекс засобів захисту, надалі КЗЗ— сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.
- Захищена комп'ютерна система — комп'ютерна система, яка здатна забезпечувати захист оброблюваної інформації від певних загроз;
- Користувач ;
- Доступ до інформації— вид взаємодії двох об'єктів КС, внаслідок якого створюється потік інформації від одного об'єкта до іншого і/або відбувається зміна стану системи.
- Несанкціонований доступ до інформації, надалі НСД до інформації — доступ до інформації, здійснюваний з порушенням ПРД.
- Захист від несанкціонованого доступу — запобігання або істотне утруднення несанкціонованого доступу до інформації.
- Авторизація;
- Авторизований користувач — користувач, що володіє певними повноваженнями;
- Порушник;
- Ознайомлення ;
- Модифікація ;
- Конфіденційність інформації— властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем або процесом;

- Цілісність інформації— властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем або процесом;
- Доступність — властивість ресурсу системи (КС, послуги, об’єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний;
- Спостереженість — властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.
- Атака;
- Проникнення ;
- Вразливість системи ;
- Втрата інформації ;
- Прихований канал — спосіб одержання інформації за рахунок використання шляхів передачі інформації, існуючих у КС, але не керованих КЗЗ, або спостереження за існуючими потоками інформації.
- Пропускна здатність прихованого ;
- Відмова ;
- Комп’ютерний вірус ;
- Модель загроз (model of threats) — абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.
- Модель порушника;

- Ризик;
- Аналіз ризику— процес визначення загроз безпеці інформації та їх характеристик, слабких сторін КСЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеню їх прийнятності для експлуатації АС.
- Засоби захисту ;
- Експорт інформації — виведення інформації з-під керування КЗЗ назовні;
- Ідентифікація— процедура присвоєння ідентифікатора об’єкту КС або встановлення відповідності між об’єктом і його ідентифікатором; впізнання;
- Автентифікація— процедура перевірки відповідності пред’явленого ідентифікатора об’єкта КС на предмет належності його цьому об’єкту; встановлення або підтвердження автентичності;
- Пароль— секретна інформація автентифікації, що являє собою послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж йому буде надано доступ до КС або до інформації;
- Персональний ідентифікаційний номер— вид паролю, що звичайно складається тільки із цифр, і який, як правило, має бути пред’явлений нарівні з носимим ідентифікатором;
- Достовірний канал — захищений шлях передачі інформації між користувачем і КЗЗ, що не може бути імітований, а інформація, що передається ним, не може бути отримана або модифікована стороннім користувачем або процесом;
- Криптографічне перетворення — перетворення даних, яке полягає в їх шифруванні, вироблення цифрового підпису;
- Шифрування даних ;
- Зашифрування даних ;
- Розшифрування даних ;
- Відкритий текст ; .

- Шифртекст (cipher text) — дані, отримані у результаті зашифрування відкритого тексту.
- Ключ (key) — конкретний стан деяких параметрів алгоритму криптографічного перетворення, що забезпечує вибір одного перетворення із сукупності можливих для даного алгоритму.

1.6. Захист персональних даних з використанням криптографії

Шифрування даних - це тільки один з важливих елементів системи інформаційної безпеки, але абсолютно не достатній в окремому вигляді. Система шифрування ефективна лише тоді, коли грамотно налаштовані системи розмежування доступу та ролей, контролю цілісності операційного середовища, засобів виявлення проникнень або захвату антивірусного та антитроянского захисту.

Використання шифрування при передачі даних призводить до зниження ризику втрати конфіденційних даних через так "людський фактор", як кажуть в побуті, особливо проявляється при виникненні екстремальних ситуацій, коли зловмисники можуть отримати фізичний або віртуальний доступ до серверів або до зашифрованих носіїв, заволодіти адміністраторським доступом (прав).

Дані на захищених дисках завжди зберігаються в зашифрованому вигляді. Тому використовувати їх, навіть зробивши копію, наприклад, при транспортуванні сервера, ремонті, крадіжці або вилучення дисків, неможливо;

Найвища надійність - в процесі шифрування реалізований захист даних від збоїв, в тому числі і в результаті збоїв живлення комп'ютера;

Отримати доступ до даних і розшифрувати їх неможливо, навіть якщо під примусом спробують змусити це зробити адміністратора або власників.

1.7. ISO /IEC 27005 — міжнародний стандарт інформаційної безпеки, в Україні має назву ДСТУ ISO/IEC 27005:2015: «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки»

Прийнятий 18 грудня 2015 року, набув чинності на початку 2017 року

Міжнародна організація по стандартизації (ISO) і Міжнародна електротехнічна комісія (IEC) разом утворили спеціалізовану систему міжнародної стандартизації.

Державні організації, які є членами ISO або IEC, беруть участь в розробці міжнародних стандартів за допомогою технічних комітетів, які створені відповідними організаціями для роботи в певних технічних сферах.

Міжнародні технічні комітети ISO разом з IEC співпрацюють в областях, що представляють інтерес для обох організацій.

Крім того, спільно з ISO і IEC в роботі беруть участь інші державні та недержавні міжнародні організації та групи.

Розроблені варіанти міжнародних стандартів, прийняті об'єднаним технічним комітетом, передаються організаціям-учасникам для затвердження.

Для прийняття стандарту в якості міжнародного, необхідне схвалення не менше 75% національних органів, які мають право на голосування.

Цей перший випуск ISO / IEC 27005 представляє технічний перегляд

Стандартів на заміну старих стандартів ISO / IEC TR 13335-3: 1998 з ISO / IEC TR 13335-4: 2000.

Даний стандарт забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, що включає в себе інформацію (данні) та менеджмент ризиків безпеки технологій телекомунікації.

Методи, описані в цьому стандарті, відповідають загальним поняттям, моделям та процесам, описаними в ISO / IEC 27001. Ці рекомендації націлені, щоб допомогти реалізувати надійну інформаційну безпеку, основуючись на підході менеджменту ризиками.

Для кінцевого розуміння цього стандарту необхідно знайомство з поняттями, моделями, процесами і термінологією, описаної в ISO / IEC 27001 разом з ISO / IEC 27002 [6].

Передумови:

Для менеджменту ризиків інформаційної безпеки необхідний системний підхід, для ідентифікації організаційних потреб щодо вимог інформаційної безпеки та створити ефективну систему менеджменту інформаційної безпеки (надалі СМІБ). Цей підхід повинен відповідати до організації та також повинен бути урівноважений підхід повного менеджменту ризиків підприємства. Всі зусилля з безпеки повинні бути ефективним і своєчасним способом звернутися до ризиків, де і коли вони необхідні.

Менеджмент ризиком інформаційної безпеки повинен бути невід'ємною частиною усіх дій менеджменту інформаційною безпекою і це необхідно бути реалізовано як до інтеграції, так і до безперервності операції СМІБ.

Менеджмент ризиків інформаційної безпеки повинен стати безперервним процесом. Процес повинен враховувати навколишнє оточення, оцінювати ризики, обробляти ризики, використовуючи план обробки ризику, здійснити рекомендації та рішення. Менеджмент ризиків аналізує то, що імовірно може трапитися з його наслідками можуть бути перші, ніж вирішити те, що повинно бути зроблено й коли, щоб зменшити ризик до прийнятного рішення або процедури.

Менеджмент ризиків інформаційної безпеки повинен сприяти наступному:

- Ідентифікації ризиків;
- Оцінюванню ризиків в термінах їх наслідків щодо бізнесу і імовірності їх в інцидентах;
- Імовірність з наслідками цих ризиків повинні бути доведені і зрозумілі;
- Пріоритету для дій, щоб знизити появу ризиків;
- Залучення причетних сторін, коли рішення менеджменту ризиків прийняті і тримаються в курсі статусу менеджменту ризиком;
- Ефективність контролю обробки ризику;
- Ризики з процесом менеджменту ризиків мають бути вимірюваними і регулярно переглядатися;
- Зафіксовувати інформацію, щоб покращити підходи менеджменту ризиків;

- Фахівцям, обробляючих інформацію про риски зі зробленими діями, щоб пом'якшити їх.

Процес менеджменту ризиків інформаційних безпеки може прийматись для організацій в цілому чи для будь-якої окремої дискретної частини підприємства, або існуючої.

Процес менеджменту ризиків інформаційної безпеки складає з :

- Встановлення навколишнього оточення;
- Оцінка ризиків;
- Обробка ризиків;
- Прийняття рішення ризику;
- Комунікація ризику;
- Контроль ризику з його наступним переглядом.

Рисунок 1.1. зображує , що процеси менеджменту ризиків є ітераційними для оцінки ризику та діями обробки ризиків.

Ітераційний підхід до проведення оцінки ризику може збільшити глибину з деталями оцінки при кожній ітерації. Ітераційний підхід забезпечує хорошу рівновагу між зменшенням часу і зусиллям, витраченим в ідентифікації контролю все ще гарантуючи, що високі ризики оцінені відповідно

Рис 1.1 Процес керування ризиком інформаційної безпеки

Встановлюється спочатку контекст. Після цього проводиться оцінка ризику. Якщо надано достатньо інформації, щоб визначити ефективні дії, необхідні для зміни

ризиків до прийнятного рівня, тоді завдання закінчена і слід обробка ризику. Якщо інформації буде недостатньо, то слід інша ітерація оцінки ризику з переглянутим контекстом та можливо буде проводитися на обмежених частинах повної області застосування.

Ефективність обробки ризику залежить від результатів оцінки ризику. Можливо, що обробка ризику не буде негайно приводити до прийнятного рівня залишкового ризику. У цій ситуації, інша ітерація оцінки ризику зі змінними контекстними параметрами, може в разі потреби турбуватися і супроводжуватися подальшою обробкою ризику

ISO / IEC 27001 визначає, що менеджмент, реалізований в межах області видимості, кородонів і контексту СМІБ повинен бути заснованим на ризики. Додаток процесу менеджменту ризиком інформаційної безпеки може задовольнити цю вимогу. Є багато підходів, якими може бути успішно здійснений процес в організації. Організація повинна використовувати кращі набори будь-яких підходів їх обставини для кожного певного додатка процесу.

На етапі «планування» СМІБ визначає стану, проводить оцінку ризику, розробляє план обробки ризику і прийняття ризику - це є всій частиною фази "Плану". В "здійсненні" СМІБ поетапно здійснює дії і регулювання, необхідні щоб зменшувати ризик до прийнятного рівня, необхідних згідно з планом обробки ризику. У фазі "перевірки" СМІБ визначає потребу менеджерам в переглядах оцінки ризику і їх обробки в світлі інцидентів і змін обстановки. В фазі "виконання" виконуються будь-які необхідні дії, включаючи додаткове застосування процесів менеджменту ризиком інформаційної безпеки.

Наступна таблиця підсумовує дії менеджменту ризиком інформаційної безпеки, які стосуються чотирьох фаз процесу СМІБ:

Табл. 1.1.

Регулювання СМІБ та процес менеджменту ризиком інформаційної безпеки.

Процес СМІБ	Процес менеджменту ризиків інформаційної безпеки
Планування (Plan)	Встановлення контексту Оцінки ризику Розробка плану обробки ризику Прийняття ризику
Реалізація (Do)	Реалізація плану обробки ризику
Перевірка (Check)	Безупинний контроль і розгляд ризиків
Виконання (Act)	Підтримка і поліпшення ризиків інформаційної безпеки Процес менеджменту

Надалі цей міжнародний стандарт описує і дає значення наступним темам:

- Встановлення контексту

Вхідна інформація: Вся інформація про організацію, що відноситься до встановлення контексту менеджменту ризиків інформаційної безпеки.

Дія: Має бути встановлено стан для менеджменту ризиком

інформаційної безпеки, яке здійснює установку основних критеріїв, необхідних для управління ризиками інформаційної безпеки, визначення області застосування і меж, встановлення відповідної організації, що здійснює менеджмент ризиків інформаційної безпеки.

Керівництво реалізації: Це є основним, щоб визначити мету менеджменту ризиків інформаційного безпеки, оскільки це зачіпає весь процес і область застосування установа зокрема.

Вихідна продукція: Специфікація основних критеріїв, області застосування і меж, і організації для процесу менеджменту ризиком інформаційної безпеки.

- Оцінка ризиків інформаційної безпеки

Вхідна інформація: Основні критерії, сфера застосування, межі та організація для встановлюваного процесу менеджменту ризиків інформаційної безпеки.

Дія: Ризики повинні бути ідентифіковані, визначені і описані кількісно або якісно, розташовані за пріоритетами проти критеріїв оцінки ризику і реальнощів, що належать до організації.

Керівництво реалізації: Ризик - комбінація наслідків, які слід було б від виникнення небажаного випадку і ймовірності виникнення випадку. Оцінка ризику визначається кількісними або якісними описами ризику і надає можливість менеджерам розташувати по пріоритетах ризики згідно їх важливості сприйняття або іншим встановленим критеріям.

Оцінка ризику визначає цінність інформаційних активів, ідентифікує відповідні загрози і вразливість, які існують (або можуть існувати), ідентифікує існуючі контролі і їх ефект на ідентифікований ризик, визначає потенційні наслідки і нарешті має за пріоритетами отримані ризики і ранжирує їх проти набору критеріїв оцінки ризику в навколишньому середовищі організації.

Оцінка ризику часто проводиться за дві (або більше) ітерації. Спочатку виконується оцінка високого рівня, щоб в подальшому гарантувати оцінку ідентифікованих потенційно високі ризики. Наступна ітерація може залучити подальший всебічний розгляд потенційно високі ризики, показаних в початковій ітерації. Якщо надано недостатньо інформації для оцінки ризику, тоді далі проводяться дослідження деталізуються, ймовірно, і можливе використання різних методів на частинах повної області застосування.

Вищевказане відноситься до організації, щоб вибрати власний підхід до оцінки ризику, заснованої на прагненні і цілі оцінки ризику.

Вихідна продукція: Список оцінених ризиків розташованих по пріоритетам відповідно до критеріїв оцінки ризику.

- Обробка ризиків інформаційної безпеки

Вхідна інформація: Список ризиків розташованих по пріоритетам відповідно до критеріїв оцінки ризику щодо інцідентних сценаріїв, які призводять до цих ризиків.

Дія: Повинні бути обрані контролі, щоб знизити, зберегти, запобігти або передати ризики і визначається план обробки ризику.

Керівництво реалізації: Є чотири опції, доступні для обробки ризику: зниження ризику, збереження ризику, запобігання ризику і передача ризику.

Рисунок 1.2. зображує діяльність обробки ризику в межах процесу менеджменту ризику інформаційній безпеці, як було зазначено на рисунку 1.1.

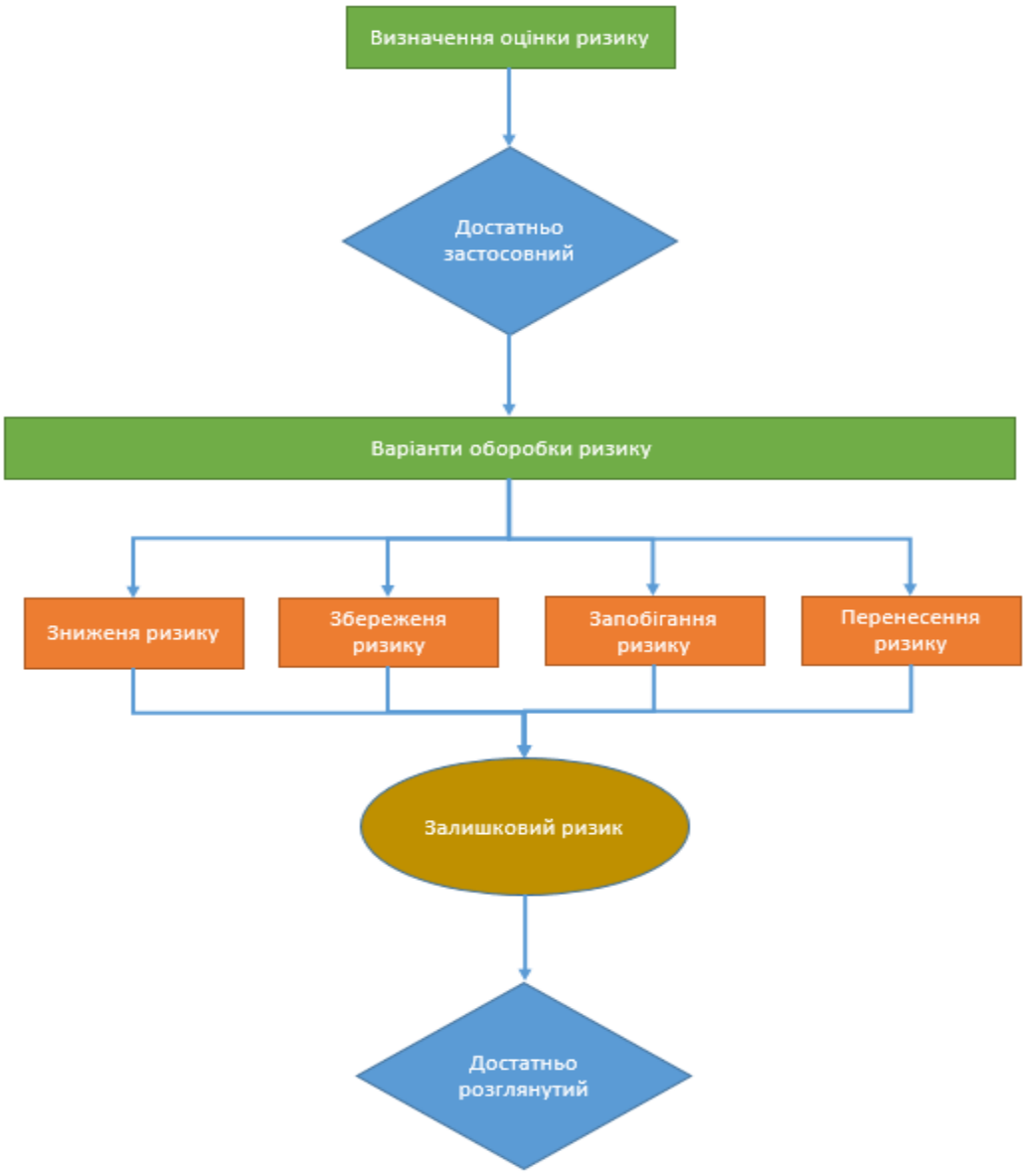


Рисунок.1.2. Діяльність обробки ризику

Повинні бути обрані варіанти обробки ризику, засновані на результаті оцінки ризику, очікувані витрати для того, щоб здійснити цей предмет вибору і очікувані пільги від цих варіантів.

Повинні бути здійснені такі варіанти, коли може бути отримано значне зниження ризиків з відносно низькими витратами. Подальші вибори варіантів для удосконалень можуть бути неекономними і має бути прийнято рішення щодо того, чи припустимі вони.

Всі чотири варіанти для обробки ризику не є взаємовиключними. Іноді організація може істотно отримати вигоду комбінацією варіантів, таких як зниження ймовірності ризиків, зниження їх наслідків і передача або збереження будь-яких залишкових ризиків.

Вихідна продукція: План обробки ризику і менеджери організації, що призводять залишкові ризики до приймального результату.

- Збереження ризику інформаційної безпеки.

Вхідна інформація: План обробки ризику і залишкова оцінка ризику піддається приймального рішенням менеджерів організації.

Дія: Рішення зберегти ризики і обов'язки за рішення повинно бути прийнято і формально зареєстровано.

Керівництво реалізації: Важливо робити перегляд відповідальними менеджерами і здійснювати схвалення запропонованих планів обробки ризику, які утворюються залишкових ризиків і робити записи будь-яких станів, пов'язаних з таким схваленням.

У деяких випадках рівень залишкового ризику, можливо, не зустрічає прийомні критерії ризику, тому що застосовувані критерії не беруть до уваги переважаючі обставини. Наприклад, можна було б стверджувати, що необхідно прийняти ризики, тому що вартість зниження ризику занадто висока, а збиток, який супроводжує ризики дуже привабливий. Такі обставини вказують, що прийомні критерії ризику неадекватні і повинні бути, якщо можливо, переглянуті. Однак, це не завжди

можливо, щоб своєчасним способом переглянути приймальні критерії ризику. У таких випадках особам, які приймають рішення, ймовірно, доведеться зберегти ризики, що не зустрічають нормальні прийомні критерії. Якщо це необхідно, особа, яка приймає рішення, має явно прокоментувати ризики і внести виправдання для вирішення скасувати нормальні прийомні критерії ризику.

Вихідна продукція: Список збережених ризиків з обґрунтуванням того, що зустрічає нормальні прийомні критерії ризику організації.

- Комунікація ризику інформаційної безпеки

Вхідна інформація: Всі ризики інформації, отримані від дій менеджменту ризиками, згідно рисунку 1.1.

Дія: Інформація про ризик повинна обмінюватися або розділятися між особою, яка приймає рішення і іншими зацікавленими сторонами.

Керівництво реалізації: Комунікації ризику - діяльність, щоб досягти угоди по тому, як управляти ризиками, обмінюючись або ділячись інформацією про ризик між особами, що приймають рішення та іншими причетними сторонами. Інформація включає, але не обмежена існуванням, природою, формою, ймовірністю, серйозністю, обробкою і прийнятність ризиків.

Ефективна комунікація серед причетних сторін важлива, так як це може зробити істотний вплив на рішення, які повинні бути прийняті. Комунікації гарантує, що відповідальні за здійснення менеджменту ризиком і зацікавлені кола розуміють основний принцип, на якому прийнято рішення і чому потрібні специфічні дії. Комунікації двонаправлені.

Повинні бути виконані комунікації ризиків, щоб досягти наступного:

1. Забезпечити гарантування менеджментом організації результату ризику;
2. Зібрати інформацію про ризик;
3. Спільно використовувати слідства оцінки ризику і представити план обробки ризику;

4. Уникати і зменшувати поширення наслідків порушень правил інформаційної безпеки через брак взаємного розуміння серед осіб,

5. Які приймають рішення і причетних сторін;

6. Підтримувати прийняття рішень;

7. Отримати нові знання інформаційної безпеки;

8. Координувати з іншими сторонами і планами реакцій зменшення наслідки будь-якого інциденту;

9. Докласти зміст відповідальності щодо ризиків особам, які приймають рішення і причетним сторонам;

10. Поліпшити розуміння.

Організація повинна розробити плани комунікації ризику щодо нормальної експлуатації так само як щодо надзвичайних ситуацій. Тому, діяльність комунікації ризику повинна виконуватися безперервно.

Вихідна продукція: Розуміння безперервності процесу менеджменту ризиком інформаційної безпеки організації і їх результатів.

- Моніторинг та перегляд

Вхідна інформація: інформація повного ризику, отримана з дій менеджменту ризиком.

Дія: Повинні бути перевірені і переглядатися ризики і їх фактори, щоб в ранній стадії ідентифікувати будь-які зміни в оточенні і підтримувати короткий аналіз кінцевої картини ризику.

Керівництво реалізації: Ризики не є статичними. Загрози, вразливість, ймовірність або наслідки можуть змінитися різко без будь-індикації. Тому необхідний моніторинг, який контролює виявлення цих змін. Це може бути підтримано зовнішніми службами, які надають інформацію щодо нових загроз або уразливості.

Організації повинні гарантувати, що безперервно перевіряється наступне:

1. Нові активи, які були включені в область дії менеджменту ризиком;

2. Необхідна модифікація значень активу, наприклад через змінених бізнес вимог;

3. Нові загрози, які не були оцінені і можливо активні всередині і зовні організації;

4. можлива нова або збільшена вразливість, що дозволяє загрозам експлуатувати цю нову або модифіковану вразливість;

5. Ідентифікована вразливість, щоб визначити ті, які піддаються новим або повторно з'являються загрозам;

6. збільшене вплив або наслідки оцінених загроз, вразливостей і ризиків в агрегації, що призводять до неприпустимого рівня ризику;

7. Інциденти інформаційної безпеки.

Результатом від моніторингу ризику може бути вступна до інших дій з перегляду ризику. Коли відбуваються ключові зміни, організація повинна регулярно робити перегляд всіх ризиків

Вихідна продукція: Постійне регулювання менеджментом ризиків відповідно до бізнес цілями організації і з прийомними критеріями ризику.

1.8. Інформаційна політика держави

Інформаційна політика держави – під цим терміном розуміється бачення та план розвитку держави і інформаційній сфері, вектором якої становиться задоволення інформаційних потреб громадянина та гостей країни через створення відкритого та доступного інформаційного суспільства, беручи за основу розвиток єдиного інформаційного простору , враховуючи національні особливості , інтересів при створенні інформаційної безпеки(ІБ) на внутрішній стороні держави та міжнарожного рівня [7].

Основною складовою політик ІБ держави являється керування теперішніми та майбутніми (потенційними) небезпеками та загрозами, цілю якої є створенням

потрібних умов для задоволення інформаційних потреб суб’єктів, а також атілення національних інтересів та бачення.

Основні вектори державної інформаційної політики:

- Забезпечення доступу до інформації кого завгодно, хто побажає.
- Забезпечення рівноправних прав для створення , пошуку, отримання, збереження, захисту, зберігання, користування, розповсюдження даних.
- Забезпечення можливості для створення на території України інформаційного суспільства.
- Забезпечення прозорої діяльності суб'єктів владних повноважень;
- Створити інформаційні системи з мережами інформації, еволюцію електронного урядування.
- Регулярне оновлення, удосконалення зі зберіганням національних інформаційних ресурсів.
- Забезпечення інформаційної безпеки України;
- Підтримувати та просувати міжнародну співпрацю і інформаційній сфері та інтеграції України до світового інформаційного простору [7]

Таблиця 1.2

Суб'єкти і об'єкт інформаційних відносин

Суб'єкти інформаційних відносин				Об'єкти інформаційних відносин
фізичні особи	об'єднання громадян	юридичні особи	суб'єкти владних повноважень	Інформація

Право на інформацію має кожен, що розуміє під собою можливість вільного його зберігання, одержання, поширення, використання з захистом інформації , яка необхідна для реалізації своїх потреб з законними інтересами.

Утворення права на інформацію не може порушувати громадянські, економічні, духовні, політичні, екологічні взагалі будь-які права свободи з законними інтересами не тільки свасних громадян,а й інтересів інших громадян , прав, інтересів, тощо.

1.9.Висновок до розділу

Переглянувши вище вказані заеонотоворчі закони та укази презедента України можна цілком зрозуміло винести для себе розуміння нових слів, в основному запозичених із зарубіжних та їх тлумачення. Ця інформація нам необхідна для того, що б бути в одній течії з нашою країною та допомнати їй з новими течіями, які приходять з закордону, як стандарти ISO, та модифіковувати їх на локальні нормативи та чини.

Без цього буде важко будувати та взагалі зрозуміти що вібувається та в якому напрямку розвиватись без баз, які нам опизують законодавчі документи. Пізніше з них зороджуються інши закони до різних сфер використання, до банкових, до державних структур і так далі.

РОЗДІЛ 2 АВТЕНТИФІКАЦІЯ

На сьогодні інформаційні системи , надалі ІС, різноманітного масштабу стали частиною, яка є невід'ємною в локальних та віртуальних інфраструктурах будь то бізнесу або навіть державної складової. З кожним днем велика кількість захищеної інформації переноситься в ІС. Можливість сучасних технологій забезпечують не лише нові можливості діяльності, але також створюють значні проблеми в забезпеченні захисту власної інформації та її конфіденційності.

Більше 25% зловживань користуванням інформацією в ІС відбуваються локальними кінцевими користувачами або третіми особами, наприклад партнери з постачальниками послуг або сервісні компанії, що мають прямий доступ до ІС. Біля 70% з них, це випадки несанкціонованого отримання прав і прерогативів , крадіжки з передачею облікових даних користувачів ІС, що стає можливим через недосконаліть технологій розмежування доступу і автентифікації користувачів ІС. Модифікація та покращення методів управління реєстрації користувачів та доступу до корпоративних документів, папок, тощо, є одним з найважливішим напрямком розвитку ІС.

Кожен в сучасних інформаційно-комунікаційних систем постійно стикається з поцедурами ідентифікації та автентифікації. Ці процедури виконуються постійно, при введені паролю користувачем для доступу до ІС мережі або при відкритті програм. В результаті цього людина отримує доступ до потрібних ресурсів ІС, або система блокує його.

Ідентифікацію та автентифікацію треба вважати основою програмно-апаратних засобів безпеки, оскільки інші сервіси або послуги розраховуються на обслуговування спеціально найменіованих суб'єктів. Ідентифікація та автентифікація можна описати ,Як першу лінію оборони, так званий “ контрольно пропускний пункт» інформаційно-складової частини організації.

2.1 Класифікація інформаційних загроз

Заходи забезпечення захищеності у розподілених обчислюваних мережах великою мірою залежать від прогнозування моделей загроз. Слід цього необхідно проробити певні варіанти заходів з попередньо проведеним оцінюванням та класифікацією інформаційних загроз [8,9].

Описана ситуація показує нам цілісну картину реальних загроз, які існують для певної розподіленої обчислюваної мережі.

Таблиця 2.1

Класифікація інформаційних загроз

<table>
<tr><td rowspan="13">Загрози інформаційної безпеки</td><td>Характер загрози</td><td>Вид впливу загрози</td><td>Спрямування загрози</td><td>Джерело загрози</td></tr>
<tr><td rowspan="8">Технологічні загрози</td><td rowspan="4">Фізичний</td><td>зовнішня</td><td rowspan="2">Людина</td></tr>
<tr><td>внутрішня</td></tr>
<tr><td>зовнішня</td><td rowspan="2">Форс-мажор</td></tr>
<tr><td>внутрішня</td></tr>
<tr><td>зовнішня</td><td rowspan="2">Відмова обладнання і внутрішніх систем</td></tr>
<tr><td>внутрішня</td></tr>
<tr><td rowspan="3">Програмні (логічні)</td><td>внутрішня</td><td>Локальний порушник</td></tr>
<tr><td>зовнішня</td><td rowspan="2">Віддалений порушник</td></tr>
<tr><td>внутрішня</td></tr>
<tr><td rowspan="4">Організаційні загрози</td><td rowspan="2">Впливи на суб'єктів інформування</td><td>внутрішня</td><td>Фізичний вплив на суб'єктів інформування</td></tr>
<tr><td>внутрішня</td><td>Психологічний влив на суб'єкти інформування</td></tr>
<tr><td rowspan="2">Дії суб'єктів інформування</td><td>внутрішня</td><td>Умисні порушення</td></tr>
<tr><td>внутрішня</td><td>Випадкові порушення</td></tr>
</table>

Аналіз планувального документа відмобілізування зроблений з оглядом на типові характеристики та описи загроз може дати опис, що кількість загроз,які знаходяться в середині підприємства, важить значну складову та може перевищувати зовнішні. Оскільки випадки використання впливу на відповідальних суб’єктів ,

суб’єкти інформування з метою прегорнути іх на джерело загрози може дати вплив на джерело загрози , що свідчить практика веденя бойових дій в «гібридних» війнах.

Виходячи з попереднього треба передбачати можливість попередження зовнішнього впливу, засобами внутрішніх сил. В широкому розумінні контексту внутрішні загрози складають генеральну сукупність практично повністю пов'язану з користувачами обчислювальних мереж та суб'єктів інформування. Найбільні небезпечні внутрішні загрози порушення інформаційної безпеки наведені в табл. 2.2.

Таблиця 2.2

Внутрішні загрози порушення безпеки інформації

Загрози	Відстоткова складова
Втрата інформації	7
Крадіжка обладнання	6
Збої в роботі інформаційних систем	15
Спотворення інофрмації	62
Порушення конфідеційності інформації	98
Інше	28

Разом з цим у більшості рішень для забезпечення інформаційній безпеці, беручи за увагу існуючі засоби з методами захисту інформації, дають захист інформації тільки від зовнішніх загроз та проникнень. Треба зазначити , що з іншої сторони безпеки, де сосереджені способи забігання внутрішнім загрозам не приділяють увагу.

Базою для такої позиції відповідальних за планування осіб є думка про сумління та професійну компетентність користувачів. Необхідно розробляти методики для забеки, враховуючи, можливі типи злочинців, яких можна класифікувати таким чином, описано на таблиці 2.3.

Таблиця 2.3

Класифікація порушників

Зовнішні порушники	Внутрішні порушники
Представники імовірного супротивника	Посадові, відповідальні особи, начальники служб

Представники задіяних у відмобілізуванні організацій, громадяни	Співробітники відділів розробки і супроводу програмного забезпечення
Випадкові відвідувачі	Користувачі та адміністратори системи
Хакери	Керівники різних рівнів посадової ієрархії
Злочинні організації	Технічний персонал

Для підтвердження такого висновку можу навести результати дослідження агенства CNews Analytics (CNA) самими серйозними загрозами інформаційної безпеки є планомірний витік інформації (70%) разом з халатністю персоналу, які змогли доспустити витік інформації (теж 70%). Обмеження таких сучасних систем безпеки повязані з тим, як внутрішні слабкі місцянабагато важче виявити та діагностувати, ніж зовнішні чинники. Оскільки поведінку внутрішніх працівників та персоналу зачастую дуже непередбачуванні та посилюються перспективами несанкціонованим доступом з крадіжкою інформації. Рівень нанесеної шкоди може бути значно більше в порівнянні з діями зовнішніх порушників, хакерів.

Щодо методів застерігання вважається, що жорстке лімітування доступу штатних та найманих працівників не зовсім дієве та призводить до зупинки підприємства. Взагалі внутрішня, локальна безпека є завжди балансом між організаційними та технічними методами, прагненням до захищеності з потребами суб'єктів інформування. Але в цей же час цей процес є безперервним , що передбачає не тільки інтегрування програмних методів, а ще підвищення освіченості працівників. Цілком захиститись від внутрішніх небезпек неможливо, оскільки необхідно намагатись мінімізувати ризики їх реалізації.

Захиститись від внутрішніх загроз з кожним роком становиться все більшою проблемою. Вимоги з рекомендаціями з покращення захисту інформації стосується впровадженню комплексної системи підходу та посилення контролю , додатково передбачаючи наступне:

- Комплексну інтеграцію заходів з заходами захисту даних він несанкціонованого доступу;
- Постійний контроль за роботою засобів компютерної техніку;

Ці вимоги не головні, але вже вироблені практикою. Схожі формулювання є в британському стандарті BSS 7799 “Практичні правила керування інформацією”, в німецькому стандарті BS і в інших країнах.

2.2. Канали витоку інформації

На сьогодення технічна складова розіляється на велику кількість галузей. Звичайно прийняття новітніх технічних засобів впроваджує великому розповсюдженню різноманітної компютерної техніки в усіх різноматних сферах бізнесу чи державних установ з телекомунікаційними компаніями, які роблять повсякденні задачі більш простішими. Прикладом можна зазначити, що постійно і з кожним днем все збульшується кількість нових користувачів в глобальній мережі Internet, спеціальні структури вказують, що кожного місяця з’являється від 7 до 8 відсотків нових користувачів у світі. Як на мене ці данні мало що вказують,оскільки до інтернету ми підєднуємо не тільки наші роботі чи домашні станції з телефонами чи ноутбуками а й ще й цілі квартири, машини, будь-які електронні пристрої чи механізми. І всьому цьому є інша сторона медалі, з’ява комп’ютерної злочинності та різних махінацій.

Вже на локальному рівні можуть виникати загрози витоку інформації. Каналами витоку інформації можна вважати сукупністю джерел інформації з матеріальними носіями або джерел інформації, що містять дані.[10].

Існування фізичних чи віртуальних каналів передачі інформації потенційно може привертати інтерес зі сторони порушників для крадіжки, блокування, шифрування або видалення інформації або різноманітні інші маніпуляції. Різні канали зв’язку приводять до різних методів витоку інформації.

Найчастіше використовують спеціалізовані технічні засоби інформації для проведення розвідки або зчитування інформації:

- Мікрофони;
- Оптичні системи;
- Прилади перехоплення телефонних оповіщень;
- Відеопристрої запису або відеоспостереження;
- Девайси для визначення розташування об’єкта або суб’єкта;
- Пристрої впливу на персональні комп’ютери з мобільними робочими станціями та мережу їх підключення;
- Системи перехвату, керування, запису та інше.

Пряме включення в систему з лінією зв’язку або електронний пристрій є самим простим способом зчитування інформації. Безконтактне під'єднання можливе за допомогою електромагнітних наводок або за рахунок рішенню на скупченні індуктивності. Ще ж рішення, які реалізовані за допомогою маскування приладів зчитування інформації в навколишнє середовище або імітації предметів. Такі технічні комплекси можуть працювати на відстані предечі від 50 і майже до 1 кілометру в залежності від потужності передавача та носія електроживлення. Усі ці пристрої являються не самими дорогими в цій сфері викрадення інформації.

Для зразку нижче наведу варіанти таких пристроїв [11]:

Таблиця 2.1

Традиційні канали витоку інформації

Традиційні канали витоку аудіо- та відеоінформації
Контактна або безконтактний підключення до електронних пристроїв. Вбудовані мікрофони, відео-і радіозакладки в стінах, меблях предметах.
Знімання акустичної інформації за допомогою лазерних пристроїв з відображають поверхонь.
Оптичний дистанційний з'їм відеоінформації.

Застосування вузьконаправлених мікрофонів і диктофонів.
Витоку інформації по ланцюгах заземлення, мереж гучномовного зв'язку, охоронно-пожежної сигналізації, ліній комунікацій і мереж електроживлення.
Високочастотні канали витоку інформації побутової та іншої техніки.
Витік за рахунок поганої звукоізоляції стін і перекриттів.
Дослідження зловмисником виробничих і технологічних відходів.
Витік інформації через телефонні і факсимільні апарати.
Обладнання віброканалов витоку інформації на мережах опалювання газо-і водопостачання.
Витік інформації через персонал.

Процес зчитування звукової інформації за допомоги лазерних девайсів з відображенням від поверхні. Алгоритм роботи даних пристроїв полягає в моделюванні по амплітуді і фазі відбитого лазерного променю від місць зчитування, надалі сигнал зчитується спеціальним зчитувачем або приймачем. Дальність роботи цих девайсів складає біля пари сотні метрів. Основною проблемою являється велика чутливість до погодних умов.

Оптично-дистанційне зчитування відеоданих. Метод роботи полягає в використанні оптичного довгофокусного обладнання і ручному або автоматичному режимі, направлені на вінка приміщень.

Для зчитування голосових даних в приміщеннях використовують мікрофони та диктофони з різноманітними модифікаціями. Прийнято використовувати прилади з вузьконаправленою діаграмою спрямованості. Дана діаграма дозволяє певним приладам уникнути завадам від сторонніх шумів або сигналів. Додатково ці мікрофони можуть використовуватись у парі з магнітофонами і диктофонами.

Витік інформації за рахунок гальванічного зв’язку провідників з землею. Можливі в наступних прикладах: Заземлення, мережі гучномовців, пожежної сигналізації, охоронної сигналізації, мереж електроживлення і т.д.

“Мікрофонний ефект” – властивості датчиків, які мають свою долю використання в витоці даних через сигналізації та системи оповіщення.

Такі канали витоку з часом здобули назву параметричні канали. Вони утворюються шляхом “високочастотної накачки” електронних приладів з наступним перевипроміненням електромагнітного поля, які пройшли модуляцію інформаційним сигналом. Модифіковані ВЧ-коливання мають властивість будти перехопленими і повернутись в оригінальний вид схожим технічним пристроєм.

Можливі варіанти витку інформації через погану звукоізоляцію стін та перекриттів. В цьому випадку можливі рішення варіанти зчитування інформації як самі звичайні мікрофони так і досить складних програмно-апаратних комплексів.

Існують навіть комплекси які здатні зчитувати дані з газо-та водопостачанні та мережі опалювання. Предметом витоку інформації є труби, Через які розповсюджуються акустичні хвилі. Акустичні хвилі можуть прийматись завдяки п'єзоелектричних датчиків, пізніше підсилюватись і сприймаються надалі магнітофоном або транслюються в ефір.

Але самим ймовірним витоком інформації буде через людський фактор. Велика кількість дослідів було проведено на території України та закордонними службами і висновки в усіх однакові, що людина є самою великою загрозою в розповсюдженні та “злитті” інформації. Тому треба бути обережним з власними співробітниками, які можуть розказати, знищити, модифікувати інформацію чи інсталювати випадково додаток шахрая чи зловмисника.

Таблиця 2.2

Канали витоку інформації

Канали витоку інформації з ЗКТ

Витік інформації за рахунок введення програмно-апаратних закладок
Витік за рахунок побічного електромагнітного випромінювання і наведення
Витік за рахунок знімання інформації з принтера і клавіатури з акустичного каналу
Витік, модифікація, знищення або блокування інформації з використанням комп'ютерних вірусів
Втрата носіїв інформації
Ініціалізація зловмисником каналів витоку, викликаних недосконалістю програмного або апаратного забезпечення, а також систем захисту

Програмні комплекси витоку інформації дуже часто використовуються в вигляді модифікованого програмного забезпечення. Тобто програмне забезпечення начебто працює в звичайному режимі, але паралельно можуть відбуватись різноманітні процеси чи в залежності від обставин.

Втрата інформації за допомоги побічного електромагнітного випромінювання і наведень (ППЕВН). Під час функціонування комп’ютерної техніки виникаються побічні електромагнітні випромінення, які собою несуть оброблюванну інформацію пристроєм. ППЕВН випромінює у простір за допомоги: клавіатури, монітора, мишки, будб-яким пристроем вводу-виведення інформації, принтером або пристоями збереження інформації з кабельними лініями. Зчитування за допомогою ППЕВН відбувається спеціальними радіоприймальними пристроями з засобами аналізу або реєстрації інформації. Відстань роботи таких рішень може досягати до полутора кілометрів за умови роботи цього пристрою зі спрямованою антеною.

За допомогою комп’ютерних вірусів дані на носіях можуть бути змінені, знищенні, заблоковані або просто скопійовані на носії грабіжника. Взагалі існує велика кількість різноманітних типів вірусів, які по своєму інтегруються в систему.

Згідно останніх досліджень можна зазначити, що віруси зараз не тільки спрямовані на модифікацію даних , а навіть на зміну програмних комплексів, доходячи аж до руйнування самого комп’ютера.[12] На рис.2.1 наведена класифікація комп’ютерних вірусів

Руйнування або втрата носіїв з інформацією може здійснитись у випадках розкрадання або частковим знищенням зони зберігання. Фізичного руйнування через цілеспрямовані дії персоналу або відвідувачів. Надзвичайних ситуацій таких як, пожежа, затоплення, стихійні лиха (землетрус, урагани, повінь і т.д.), обробка хімічними речовинами, впливу потужного електромагнітного поля або інші надзвичайні події (ЧП).

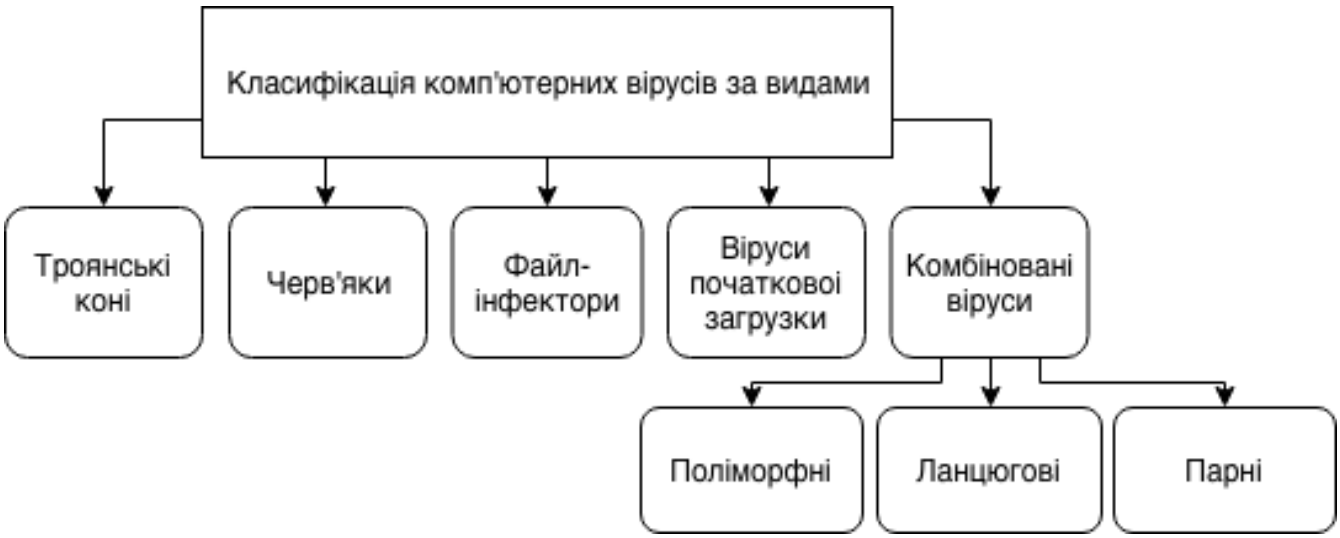


Рис.2.1. Класифікація комп'ютерних вірусів

Момент створення шахраєм каналів витоку даних, як правило виникає через недосконалість програмних, апаратних та програмно-апаратних комплексів. Зазвичай цілеспрямовано здійснюється крадіжка інформації з аналізом ситуації та слабких місць, ні ж коли це виникає під час якихсь випадкових махінацій. Зараз було описано так звані атаки на інформаційні системи (ІС). Під цим розуміється намір подолання будь-яких систем захисту.

2.3. Способи захисту інформації від несанкціонованого доступу.

Захист інформації – комплекс заходів, направлених на уникнення або стримування порушень цілісності даних або її модифікації. Під захистом розуміється інформація в будь-якому вигляді, формі, типу, об’ємі, які можуть нанести шкоди власнику або будь-якому суб’єкту. Також це розповсюджується на різні галузі в сферах науки, техніки, адміністративних підприємств, державі чи до корпорацій (комерційних організацій).

Сполучення методів з засобами захисту інформації може включати в себе програмні, апаратні, програмно-апаратні комплекси (засоби), захисні перетворення разом з організаційними заходами.

Рис.2.2. Методи й засоби захисту інформації.

Апаратні засоби передбачають, що в девайсах ЕОМ та інших технічних засобах опрацювання даних планується наявність спеціальних мікросхем або інтегрованих пристроїв, які можуть забезпечити захист та контроль витоку інформації чи схеми контролю на відповідність між різним обладнаннями чи пристроями.

Програмні методи захисту під собою розуміють певну кількість програмних засобів зі можуть забезпечити певне розділення ролей доступу та виключення несанкціонованого витоку інформації.

Ідеологія методів захисного перетворення в тому, що дані які зберігаються в якомусь середовищі та передається за допомогою каналів зв’язку передається в певному коді, що обмежує пряме його використання.

Організаційні заходи з захисту інформації являють собою певний набір дій з точковим підбором та перевірки персоналу, які беруть участь та мають доступ до роботи програм чи інформації, його експлуатацію з чітко визначеними правилами розробки процесів та життєдіяльності ІС.

Тільки використання комплексного підходу до використання заходів безпеки(Рис.2.3.) інформації, може забезпечити певний захист інформації, також треба враховувати всі сильні та слабкі місця заходів, які плануються у використанні.

Рис.2.3. Класифікація способів захисту інформації з обмеженим доступом.

Самі поширені практичні методи захисту даних та додатків.

Встановлення завад – спосіб фізичного перегороду шляхів шахраю до даних, які знаходяться під захистом, враховуючи технічні заходи зчитування інформації або впливання на неї.

Встановлення перешкод – спосіб фізичного перегороду шляху злочинцю до даних, які знаходяться під захистом , в тому рахунку намагання використовуючи технічні засоби інформації для знімання даних та дій на них.

Керування доступом – спосіб захисту даних шляхом обмежень використання тотальних даних, в тому числі автоматизованих інформаційних систем корпорації. Керування доступом повинно включати в себе наступні функції захисту:

- Ідентифікацію персоналу з ресурсами компанії;
- Аутентифікацію суб'єкта з об'єктом за допомоги наданого ідентифікатора;
- Перевірка компетенцій;
- Організація робочих умов в межах встановленого регламенту компанії;
- Реєстрація звертань до ресурсів, які знаходяться під захистом (Аудит сесій);
- Реагування під час спроб несанаційного доступу.

Маскування – тип захисту інформації , використовуючи інженерних технічних засобів, враховуючи криптографічне маскування інформації. Маскувальники, аналогово-цифрово статичні.

Скремблери – програмний чи апаратний пристрій або алгоритм, які виконують функцію скремблювання. Скремблювання це зворотне перетворення цифрового потоку без змін швидкостей передачі з метою роботи отримати властивість випадкової послідовності. Після скреблювання з'ява "1" з "0" на вихідній послідовності рівноймовірні. Скремблювання це оборотній процес, значить, що вихідне повідомлення може бути відновлене при використанні зворотного алгоритму.

Вокодери – технічні засоби, які передають мову в зашифрованому та цифровому виді.

2.4. Способи захисту від несанкціонованого доступу

- Ідентифікація – процедура розпізнавання системою за допомогою наперед присвоєного ім’я (ідентифікатора) або іншої зазначеної інформації про користувача, яка сприймається системою [13]. Це є першою ступеню в процедурі надання доступу до системи, після чого надається автентифікація з авторизацією.

- Аутентифікація – це процедура відповідності належності ідентифікатора об'єкта, іншими словами встановлення чи підтвердження об’єкта дійсним, і перевіряння чи є об'єкт або суб'єкт, що піддається перевірці, насправді тим, за кого він себе видає або намагається видати [14]. На теперішній час є пару основних методів автентифікації, які відрізняються своєю складністю та надійністю з вартістю (це основні показники). Будь-який метод має свої переваги та недоліки.

Використовуються наступні види автентифікації:

- Однобічна автентифікація, коли користувач системи для отримання доступу до даних підтверджує свою автентичність;

- Двобічна – це метод, коли система повинна підтвердити автентичність, окрім самого користувача;

- Трибічна –використання, так званої, “нотаріальної служби автентифікації” для підтвердження дійсності кожного з клієнтів при обміні чи передачі інформації.

Методи аутентифікації умовно можна поділити на однофакторні (слабкі, з точки зору безпеки) та багатофакторні (потужні, з точки зору безпеки)

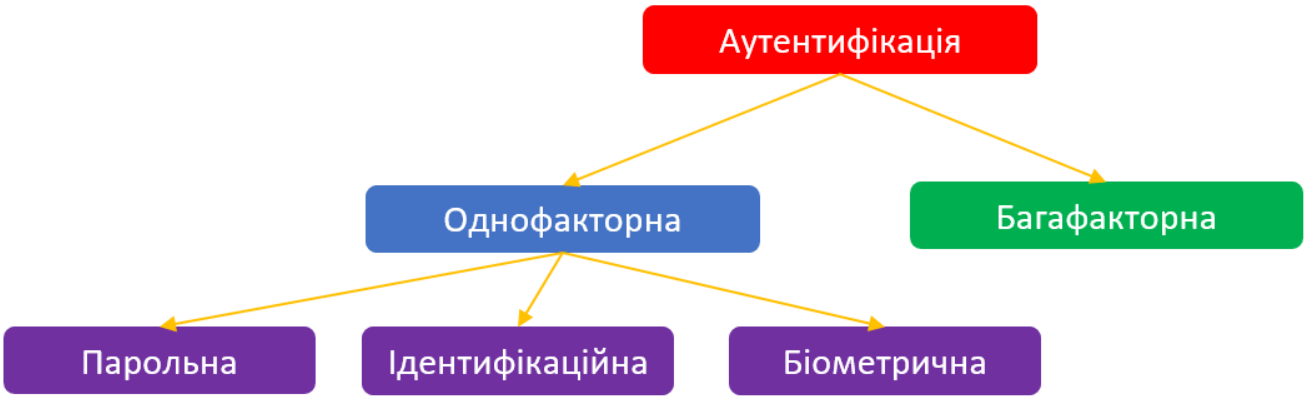


Рис. 2.4. Класифікація методів аутентифікації

2.4.1 Парольна аутентифікація

Парольна аутентифікація являється найбільш простим та поширеним методом на теперішній час. У цьому випадку при введенні абонента/клієнта персонального пароля система автентифікації порівнює його з паролем, який присвоєний в базі даних, які зберігаються в зашифрованому вигляді або середовищі. У разі співпадіння паролів підсистема відкриває доступ до мережі та сервісів. Парольні методи автентифікації поділяються ступенем зміни паролів:

- метод, що використовує постійний пароль, без змін;
- метод, при якому використовується одноразовий пароль, (пароль генерується системою або додатком)

Введення паролю, зазвичай виконується з клавіатури або за допомогою сенсорного екрана або панелі.

Основна перевага полягає в простоті реалізації та використані. Також цей метод не вимагає затрат. Цей процес реалізований у більшості програмних продуктах. Тому робимо висновок , що цей метод є самий доступний та простий.

Недоліки , нажаль їх багато. Почнем з основного – велика складова надійності лежить на самих користувачах, в основному від складності обраних ними паролів. Діло в тому, що більшість людей використовують ненадійні паролі, ключові слова, дати, які просто підібрати. Тому різні компанії генерують паролі у комбінацій

випадкових букв, цифр та різноманітних символів. Володіння достовірним паролем до конкретного користувача, майже стовідсотково гарантує зловмиснику доступ до системи або до інформації, яка зберігається на певних ресурсах. Атаки на парольні системи є самими поширеними для кіберзлочинів. Для реалізації цього злочинці звертаються до спеціальних програм, що цілеспрямовані на “злом” та “підбір” паролю.

Правильне використання паролю може забезпечити певний рівень безпеки для більшості організацій. Але в сукупності характеристик треба визнати цей метод найслабшою ідентифікацією. Саме слабкість даного методу є головною причиною вразливості комп’ютерних систем від несанкціонованого доступу.

Наступні заходи можуть підвищити ступінь парольного захисту [15]:

- Накладення технічного обмеження (Введення нормативів для паролю, тобто пароль повинен мати не менше певної кількості символів, складатись додатково з цифрами, знаками пунктуації і т.д.)
- Введення системи періодичної зміни паролів;
- Обмеження спроб введення паролів;
- Використання парольних генераторів.

2.4.2 Ідентифікаційний метод аутентифікації

При ідентифікаційній автентифікації унікальні предмети, як правило, забезпечують більш безпечний захист, ніж парольний метод. Ці предмети поділяють на дві частини:

- Пасивні предмети, котрі зберігають в собі автентифікаційну інформацію (якийсь згенерований пароль за допомогою системи) і передають це в модуль автентифікації за потребою або викликом. Також ця інформація ,як варіант, може зберігатися в предметі відкритого типу (наприклад: магнітні карти, смарт-карти з відкритою пам'яттю, електронні девайси «Touch Memory») і в захищеному середовищі (спеціальні картки з захищеною пам'яттю, флеш-токени);

- Активні предмети, які забезпечені достатнім обчислювальним ресурсам , беручи активну участь в проведені автентифікації (: мікропроцесорні карти або USB-токени і т.д.).

Далі хочу трохи більше розписати методи аутентифікації індентифікаційного типу:

- Токени

Являють собою тим, чим володіє заявник з елементами керування, які можуть використовуватися для аутентифікації особистості заявника. При електронної аутентифікації заявник аутентифікуючий в системі або додатку по мережі. Отож, токен, який використовується для електронної аутентифікації, є секретом, і токен має бути захищений. Маркер може, бути криптографічним ключем, який захищений шляхом його шифрування паролем. Самозванець повинен вкрасти зашифрований ключ і дізнатися пароль для використання токена.

Рис.2.5. Зображення токен ключа.

- Паролі та аутентифікація на базі PIN-коду.

Паролі та PIN-коди відносяться до категорії методів "щось, що ви знаєте". Комбінація цифр, символів і змішаних регістрів вважається більш надійною, ніж буквений пароль. Крім того, впровадження функцій Transport Layer Security (TLS) або Secure Socket Layer (SSL) в процесі передачі інформації також створить зашифрований канал для обміну даними і для додаткового захисту доставляється інформації. В даний час більшість атак на безпеку націлені на системи аутентифікації на основі паролів[16].

- Аутентифікація за допомогою відкритого ключа

Цей тип аутентифікації складається з двох частин. Один - відкритий ключ, інший - закритий. Відкритий ключ видається центром сертифікації і доступний будь-якому користувачеві або сервера. Секретний ключ відомий тільки користувачеві[17]

Цей метод будемо використувувати у якості другого методу підтвердження персони.

- Аутентифікація на базі семетричного ключа.

Користувач ділиться унікальним ключем з сервером аутентифікації. Коли користувач відправляє випадково сгенерированное повідомлення або запит, зашифроване секретним ключем, на сервер аутентифікації, якщо повідомлення можна порівнювати сервером з використанням його загального секретного ключа, користувач аутентифицирующей. При реалізації разом з аутентифікацією по паролю цей метод також забезпечує можливе рішення для систем двофакторної аутентифікації [18].

- Аутентифікація на базі SMS

Користувач отримує пароль, читаючи повідомлення в приватному стільниковому телефоні, за заданим номером, і вводить пароль назад для завершення аутентифікації. SMS метод дуже ефективний, коли стільникові телефони широко використовуються. SMS також підходить для захисту від атак типу «людина посередині» (man-in-the-middle MITM), оскільки використання SMS не пов'язано з Інтернетом. [19]

2.4.3 Біометрична аутентифікація

Біометрична аутентифікація базується на основі використання устаткування для обчислення вхідних даних з порівнянням з еталоном заданих персональних характеристик користувача. Біометрія – це комплекс автоматизованих засобів автентифікації персон , основуючись на їх фізіологічних і поведінкових характеристик , так званих динамічних. До фізіологічних характеристик відповідають

особливості відбитків пальців на руках або ногах, сітківки з рогівкою очей, геометрія рук з обличчя та т.д. До поведінкових характеристик відповідають дані по динаміці підпису, стилю роботи з клавіатурою, розпізнавання голосових хвиль [20]. Дані засоби дають можливість з високою точністю розпізнати власника за певною біометричною ознакою, фальсифікація цих параметрів практично виключно.

Існує наступні методи біометричної автентифікації:

- Автентифікація за малюнком папілярних ліній (відбиток пальця).

Одною з унікальних складових людини являється унікальні папілярні візерунки на пальцях особи та й не змінна протягом усього життя, не враховуючи отримання травм. В цьому і є основа даного методу. Відбиток, отриманий за допомогою спеціального сканера, перетвориться в цифровий вигляд або код, і зрівнюється з раніше заданим еталоном. Дана технологія є найпоширенішою в галузі, порівнюючи з іншими методами біометричної аутентифікації. Технологія сканування відбитків пальців - одна з найпоширеніших.

Рис.2.5. Вигляд відбитку пальця

На даний момент існує 3 типи сканерів відбитки пальців:

- Оптичні

В основі роботи оптичних сканерів є оптичний метод отримання зображення з носія. За видами використовуваних технологій можна виділити наступні групи оптичних сканерів:

1. FTIR-сканери - пристрої, в яких використовується ефект порушеного повного внутрішнього відбиття (Frustrated Total Internal Reflection, FTIR).

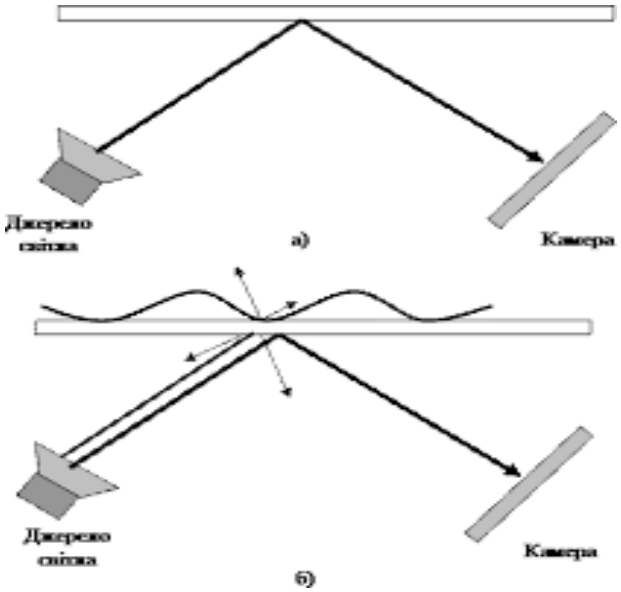


Рис.2.6.Принцип роботи FTIR-сканера

При падінні світла на кордон розділу двох середовищ світлова енергія ділиться на дві складові: одна відбивається від кордону, інша - проникає через кордон розділу в іншу середу. Доля відображеної енергії залежить від кута падіння луча. Починаючи з деякої його величини, вся світлова енергія відбивається від кордону розділу. Це явище називається повним внутрішнім віддзеркаленням. Однак при контакті більш щільною оптичного середовища (в нашому випадку поверхню пальця) з менш щільною (в практичній реалізації, як правило, поверхня призми) в точці повного внутрішнього відображення пучок світла проходить через цю межу. Таким чином, від кордону позначаться тільки пучки світла, що потрапили в такі точки повного внутрішнього відображення, до яких не було докладено борозенки папілярного візерунка поверхні пальця. Для фіксації отриманої світловий картинки поверхні пальця використовується спеціальна камера (залежить від реалізації сканера).

2. Оптоволоконні сканери являють собою оптоволоконну матрицю, кожне з волокон якої закінчується фотоелементом.

Чутливість кожного фотоелемента дозволяє фіксувати залишковий світло, що проходить через палець, в точці дотику рельєфу пальця до поверхні сканера. Зображення відбитка пальця формується за даними кожного з елементів.

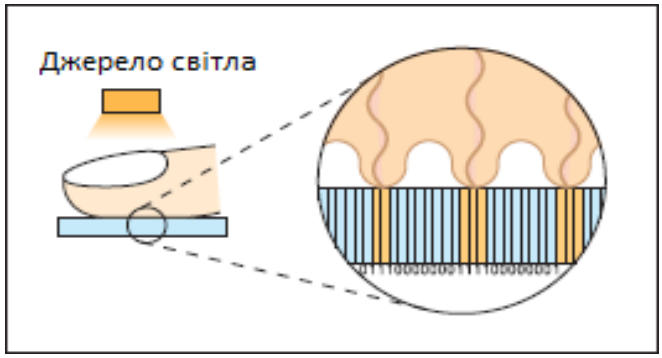


Рис.2.7. Принцип роботи оптоволоконного сканеру

3. Електрооптичні сканери (electro-optical scanners) засновані на використанні спеціального електрооптичних полімеру, до складу якого входить світловипромінювальний шар. При прикладанні пальця до сканера неоднорідність електричного поля у його поверхні (різниця потенціалів між горбками і западинами) відбивається на світінні цього шару так, що він висвічує відбиток пальця. Потім масив фотодіодів сканера перетворює це світіння в цифровий вигляд.

4. Оптичні протяжні сканери – в цілому аналогічні FTIR-пристроїв. Їх особливість в тому, що палець потрібно не просто прикладати до сканера, а проводити їм по вузькій смужці - зчитувача. При русі пальця по поверхні сканера робиться серія миттєвих знімків (кадрів). При цьому сусідні кадри знімаються з деяким накладенням, тобто перекривають один одного, що дозволяє значно зменшити розміри використовуваної призми й самого сканера. Для формування (точніше збірки) зображення відбитка пальця під час його руху по скануючої поверхні кадрам використовується спеціалізоване програмне забезпечення.

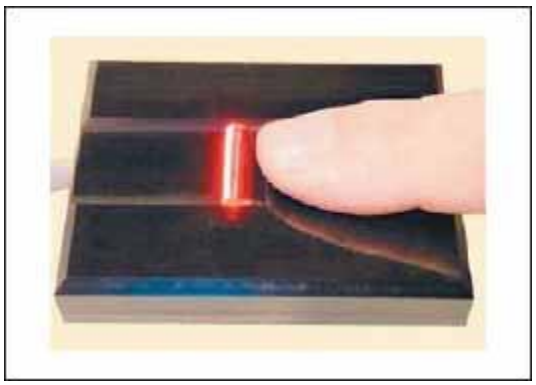


Рис.2.8. Використання оптичного протяжного сканеру.

5. Роликові сканери У цих компактних пристроях сканування пальця відбувається при прокочуванні пальцем прозорого тонкостінного циліндра, що обертається (ролика). Під час руху пальця по поверхні ролика робиться серія миттєвих знімків (кадрів) фрагмента папілярного візерунка, що стикається з поверхнею. Аналогічно протяжному сканера сусідні кадри знімаються з накладенням, що дозволяє без спотворень зібрати повне зображення відбитка пальця. При скануванні використовується найпростіша оптична технологія: всередині прозорого циліндричного ролика знаходяться статичний джерело світла, лінза і мініатюрна камера. Зображення освітлюваної ділянки пальця фокусується лінзою на чутливий елемент камери. Після повної «прокрутки» пальця, «збирається картинка» його відбитка.

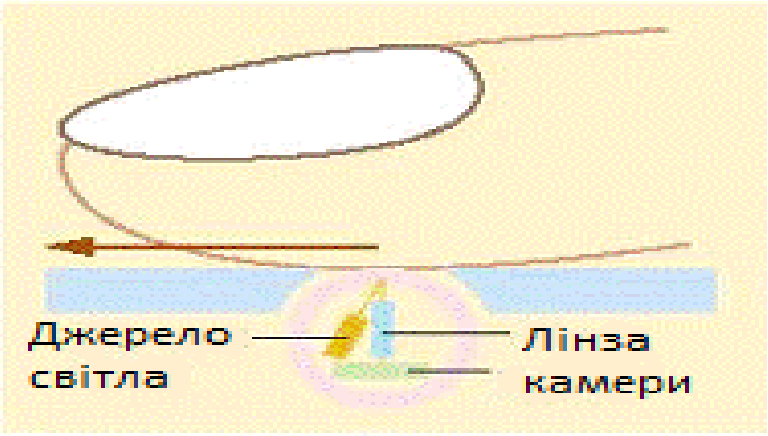


Рис.2.9. Схема роликового сканеру

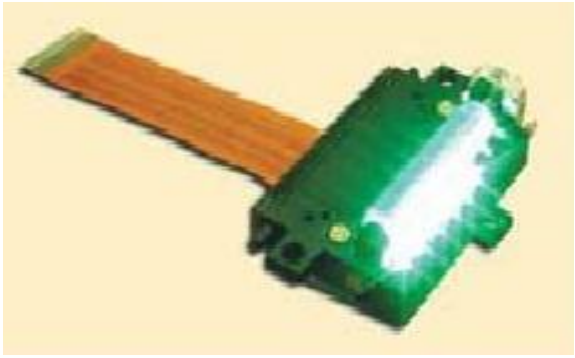


Рис.2.10. Реалізація роликового сканеру

6. Безконтактні сканери. У них не потрібно безпосереднього контакту пальця з поверхнею скануючого пристрою. Палець прикладається до отвору в сканері, кілька джерел світла підсвічують його знизу з різних сторін, в центрі сканера знаходиться лінза, через яку, зібрана інформація проектується на КМОП-камеру, що перетворює отримані дані в зображення відбитка пальця.

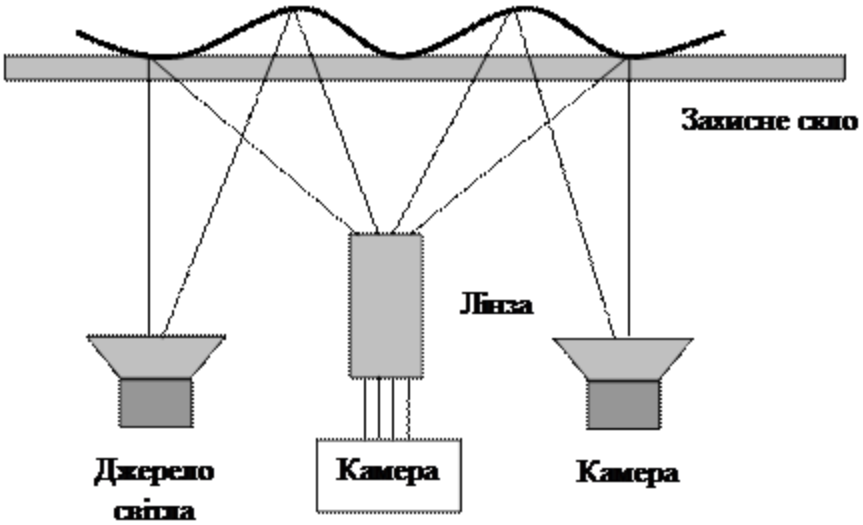


Рис.2.11. Узагальнена схема роботи безконтактного сканера

Всі вони працюють за різним принципом, але результат на виході отримуємо приблизно однаковий , з деякими відмінностями, які у відповідності з певними математичними алгоритмами перетворюються в контрольну суму.

- Напівпровідникові сканери

В основі цих сканерів використання для отримання зображення поверхні пальця властивостей напівпровідників, що змінюються в місцях контакту гребенів

папілярного візерунка з поверхнею сканера. В даний час існує декілька технологій реалізації напівпровідникових сканерів.

1. Ємнісні сканери – найбільш розповсюджені в напівпровідніковіх сканерів, у якіх для здобуття зображення відбитка пальця вікорістовується ефект Зміни ємності pn-переходу напівпровіднікового приладнати при зіткненні Гребеня папілярного малюнка з елементом напівпровіднікової матриці. Існують модіфікації описаного сканера, у якіх кожен напівпровідніковій елемент у матриці сканера Виступає в роли однієї пластини конденсатора, а палець - у роли Іншої. При прікладанні пальця до сенсора между шкірних чутлівім елементом и виступа-западинами папілярного малюнка утвориться якась Ємність, величина якої візначається відстанню между поверхні пальця й елементом. Матрицею ціх ємностей пеертворюється в зображення відбитка пальця.

2. Чутливі до тиску сканери – в цих девайсах використовуються сенсори, що складаються з матриці п'єзоелементів. При прикладанні пальця до скануючої поверхні виступи папілярного візерунка чинять тиск на деяку підмножину елементів поверхні, відповідно западини ніякого тиску не чинять. Матриця отриманих з п'єзоелементів напруг перетвориться в зображення поверхні пальця.

3. Термо-сканери – в них використовуються сенсори, які складаються з піроелектричних елементів, що дозволяють фіксувати різницю температури і перетворювати її в напругу. При прикладанні пальця до сенсора по температурі торкаються до піроелектричні елементів виступів папілярного візерунка і температурі повітря, що знаходиться в западинах, будується температурна карта поверхні пальця і перетворюється в цифрове зображення. Дані типи сканерів є найпоширенішими. У всіх наведених напівпровідникових сканерах використовуються матриця чутливих мікроелементів і перетворювач їх сигналів в цифрову форму.

Надалі хочу зобразити на рисунку 2.12 узагальнено схему роботи наведених напівпровідникових сканерів

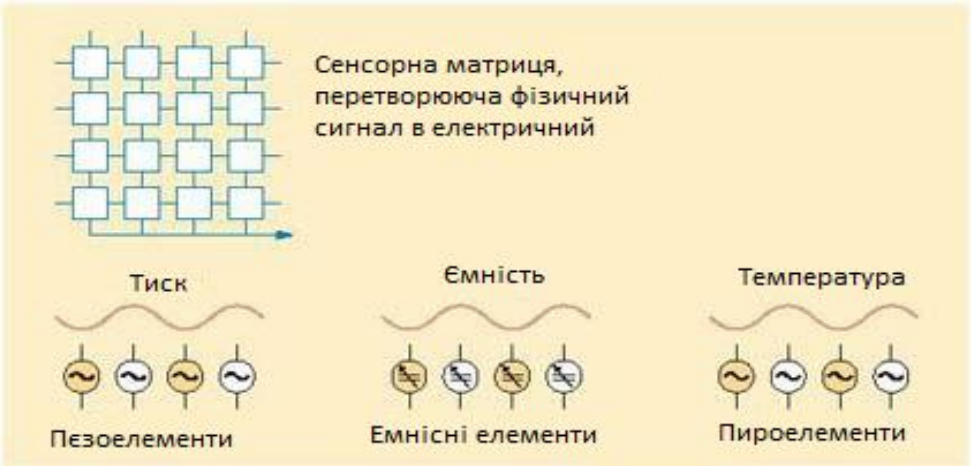


Рис.2.12. узагальнено схема роботи термо-сканерів.

4. Радіочастотні сканери - в таких сканерах використовується матриця елементів, кожен з яких працює як маленька антена. Сенсор генерує слабкий радіосигнал і направляє його на скановану поверхню пальця. Кожен з чутливих елементів приймає відбитий від папілярного візерунка сигнал. Величина наведеної в кожній мікроантенне електро-рушійна сила (ЕРС) залежить від наявності або відсутності в близи неї гребеня папілярного візерунка. Отримана таким чином матриця напруг перетвориться в цифрове зображення відбитка пальця.

5. Протяжні термо-сканери - різновид термо-сканерів, в яких для сканування, необхідно провести пальцем по поверхні сканера, а не просто прикласти його.

6. Ємнісні протяжні сканери - використовують аналогічний спосіб покадрової збірки зображення відбитка пальця, але кожен кадр зображення виходить за допомогою ємнісного напівпровідникового сенсора.

7. Радіочастотні протяжні сканери – аналогічно ємнісним, але використовують радіочастотну технологію.

- Ультразвукові сканери

Ультразвукове сканування - це сканування поверхні пальця ультразвуковими хвилями і вимірювання відстані між джерелом хвиль і западинами і виступами на поверхні пальця по відбитому від них луні. Якість одержуваного таким способом зображення в 10 разів краще, ніж отриманого будь-яким іншим, представленим на біометричний ринку методом. Крім цього, варто відзначити, що даний спосіб

практично повністю захищений від муляжів, оскільки дозволяє крім відбитка пальця отримувати і деякі додаткові характеристики про його стан (наприклад, пульс усередині пальця).

Імовірними вразливостями для підміни даних можуть бути: створення муляжу на базі латексу або желатину, перехоплення сигналу, варіант працює при умові прямого кабельного з'єднання сканера з основною системою, конденсація (відтворення останнього відбитку за допомогою струменя теплого повітря на сканер).

- Аутентифікація на базі райдужній оболонці ока.

Малюнок оболонки ока також є унікальною складовою людського тіла. Для сканування її зазвичай достатньо звичайної камери з інстальованим спеціальним програмним забезпеченням.

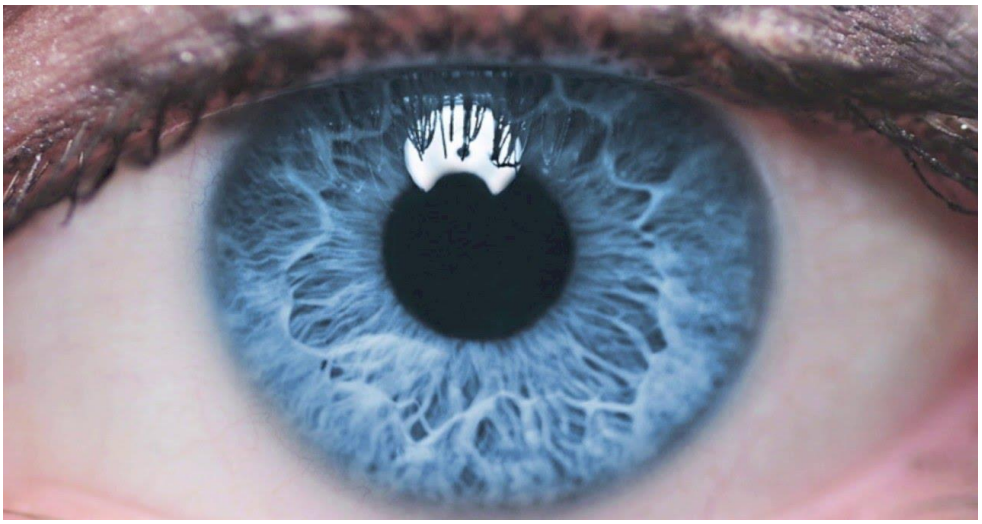


Рис.2.13. Райдужна оболонка ока

Час спрацювання зображення в сучасних система складає приблизно 300-500мс., а швидкість порівняння отриманого зображення з базою даних приблизно 50000-150000 порівнянь за секунду на звичайному комп'ютері. Тому така система з даною швидкістю не накладає обмежень на інтеграцію в системах контролю доступу.

Недоліком даного методу можна зазначити його вартість. Вартість системи набагато вища ніж в порівнянні з попереднім методом розпізнавання папілярних ліній. Також дуже низька доступність даних рішень, мало інтеграторів мають доступ до таких систем.

- Автентифікація по геометріїї обличчя.

Розроблено багато методів розпізнавання по геометрії обличчя.

Усі вони базуються на унікальності форми черепу з рисами обличчя. Ця сфера біометрії нам дуже близька через людський фактор, так як ми впізнаєм друг-друга за допомогою обличчя. Дана сфера поділяється на 2 напрямки: двомірне розпізнавання та трьохмірне розпізнавання обличчя.

1. Двомірне розпізнавання

Самий з статично-неєективних методів біометрії. З'явився цей метод давно і зазвичай він застосовувався в криміналістиці, завдяки цій сфері він і розвивався. На теперішній час, даний метод використовується в перекресній біометрії або в соціальних мережах. Використання в цих сферах обумовлено через низький показник статистичних показників.

Основною перевагою даного методу є його низька вартість при виборі обладнання.

Недоліком являється дуже низька статистична достовірність, оскільки є певні вимоги до освітлення. Також неприпустимість будь-яких зовнішніх завад, такі як борода, окуляри, зміна зачіски, далі необхідно фронтальне зображення обличчя для достовірної роботи метода, багато алгоритмів взагалі не розпізнають міміку обличчя.

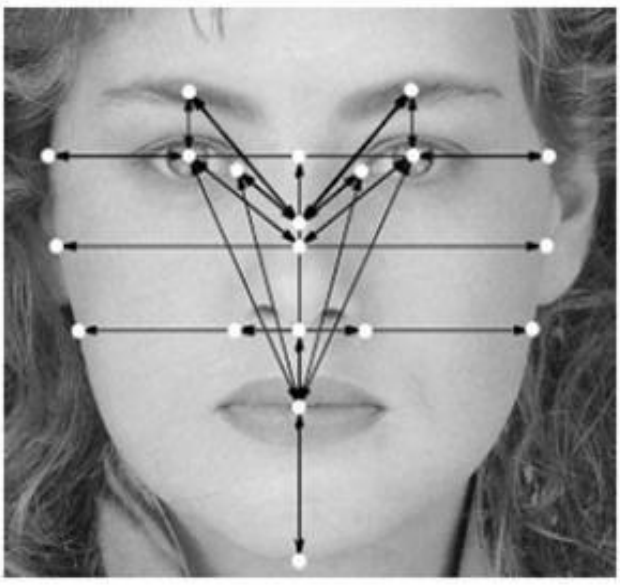


Рис.2.14. Двомірне розпізнавання обличчя

2. Трьохмірне розпізнання обличчя

На сьогодні існує величезна кількість методів розпізнавання за допомогою трьохмірного розпізнавання. І також ця задає є досить складна. Усі методи практично неможливо порівняти друг з другом, так як вони використовують різні модулі сканування та основні бази [21].

Перехідним моментом від двомірного то трьозмірного розпізнавання як полягає в накопиченні лицьової інформації.

Цей метод маж набагато кращі показники і використовує всього одну камеру. При внесені даних про особу, суб’єкт повертає голову і алгоритм складає отриману інформацію в один троьхмірний шаблон, для майбутнього використання. А під час розпізнавання використовується всього пару кадрів з відеопотоку.

Перевага полягає в низькій чутливості до зовнішніх факторів та й самої особи, висока надійність у порівнянні з ідентифікацією за скануванням папілярних ліній і відпадає необхідність прямого контакту зі скануючим пристроєм.

До недоліків можна віднести як черезвичайна вартість обладнання, зміна міміки обличчя знизують статистичну надійність.

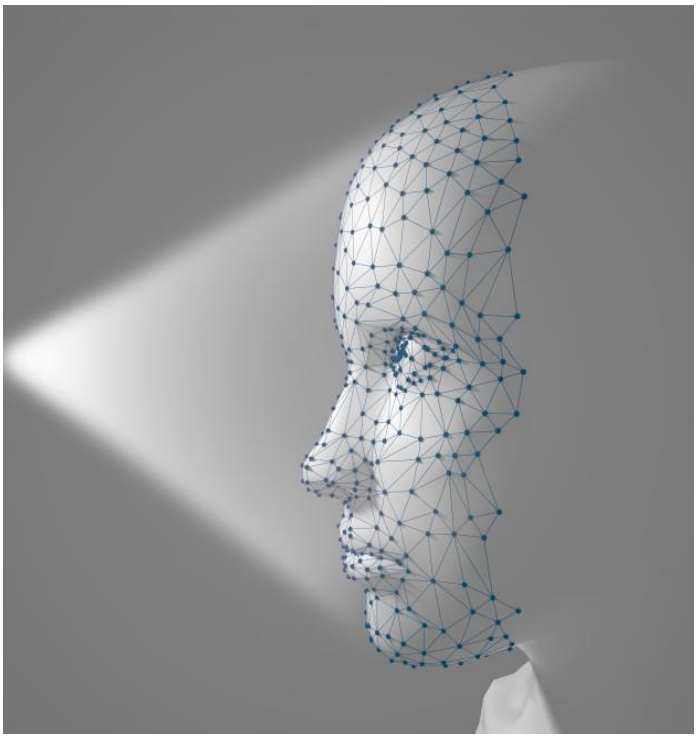


Рис.2.15. Трьохмірне розпізнання обличчя

Але треба зазначити, що дана методика активно вдосконалюється і ,я вірю, що цей метод стане доступним у повсякденні.

Варіантом роботи такого методу використовується під час аутентифікації на телефоні, комп’ютері, тощо.

- Автентифікація за геометрією кисті руки

Даний метод використовується біля 10 років і бере свої корні з сфери криміналістики.

Основою даного методу полягає в отримані геометричних показників рук: довжина фалангів, ширина долоней.

Основоною проблемою являється низька статистична характеристика, тому цей метод вже не актуальний, зі як раніше згаданий мною, метод райдужної оболонці ока

Щойно ми розглянули основні методи статичної автентифікації, далі переходимо до розглядання динамічних методів біометричної автентифікації , що базується на поведінковій характеристики людини, тобто побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якого-небудь дії.

- Автентифікація по почерку і динаміці підпису

На сьогодні дана технологія мало поширена, в порівнянні з попередніми методами. Підпис частно змінюється, що є суттєвою перевагою. Проблеми цього способу пов'язані виключно з людським фактором, так як почерк може значно змінитися в залежності від навколишнього оточення і емоційного стану людини. У зв'язку з цим розробники змушені допускати можливість досить великий похибки, ніж та можуть скористатися зловмисники. Використання динамічних характеристик, таких як сила натискання на перо або швидкість написання, ускладнює підробку, але веде до ускладнення пристрою автентифікації з істотним зростанням ціни методу.

- Автентифікація по голосу з особливостям мови

Одна з найстаріших методів. На теперішний день розвиток даного методу набирає оберти, оскільки побудова “Розумного Дому” за базу бере використання цього методу автентифікації та керування.

Існує багато методів побудови ідентифікації за голосом, за правило це поєднання частотних та статистичних характеристик голосу.

Даний вид біометричної автентифікації базується на аналізі характеристик голосу: гучності, швидкості, стилістики мови.

Але є суттєві недоліки цієї методики:

- Зміна голосу , стан здоров’я, ємоції можуть давати реацію на зміну голосу;
- Завади/перешкоди на приладі сприйняття голосу(мікрофон) та на лінії передачі;
- Порушник може отримати/перехватити конфедиціальну інформацію.

З кожним днем кількість методик та технологій автентифікації зростає в системах безпеки. Можливі наступні дуже перспективні методики, на яких зараз йде основний упор розвитку

- Термограма обличчя в інфрачервоному спектрі випромінювання;
- ДНК характеристики;
- Клавіатурна характеристика почерку;
- Аналіз структури шкіряного покриття з епітелієм на кінцівках пальців на основі ультразвукової інформації (спектроскопія шкіри);
- Аналіз відбитків долонь;
- Аналіз форми вушної раковини;
- Аналіз характеристик стилістики ходьби суб’єкта;
- Розпізнання по розташуванню вен.

2.4.4. Принцип роботи біометричної аутентифікації.

Для аутентифікації необхідно власнику або персоні, яка має права , пройти сканування фізіологічних або поведінкових характеристик. Алгоритм роботи полягає в наступному:

- Біометричний сканер/датчик зчитує біометричні дані користувача;
- Зчитані дані надсилаються до серверу, де відбувається порівняння даних отриманих з еталонними, які зберігаються в базі;
- Вдалою автентифікацією вважається коли збігаються отримані біометричні дані співпадають з еталонним варіантом. Якщо дані не співпали , то суб’єкт повертається до першого пункту.

Повну структуру можна побачити на наступному рисунку.

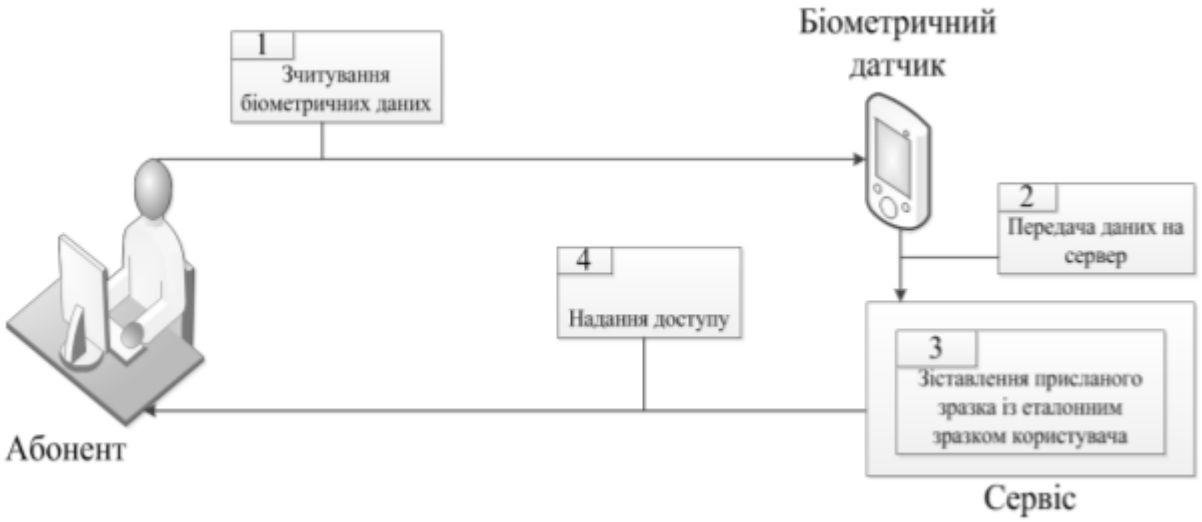


Рисунок 2.16. Алгоритм роботи біометричної автентифікації

2.4.5. Багатофакторна аутентифікація

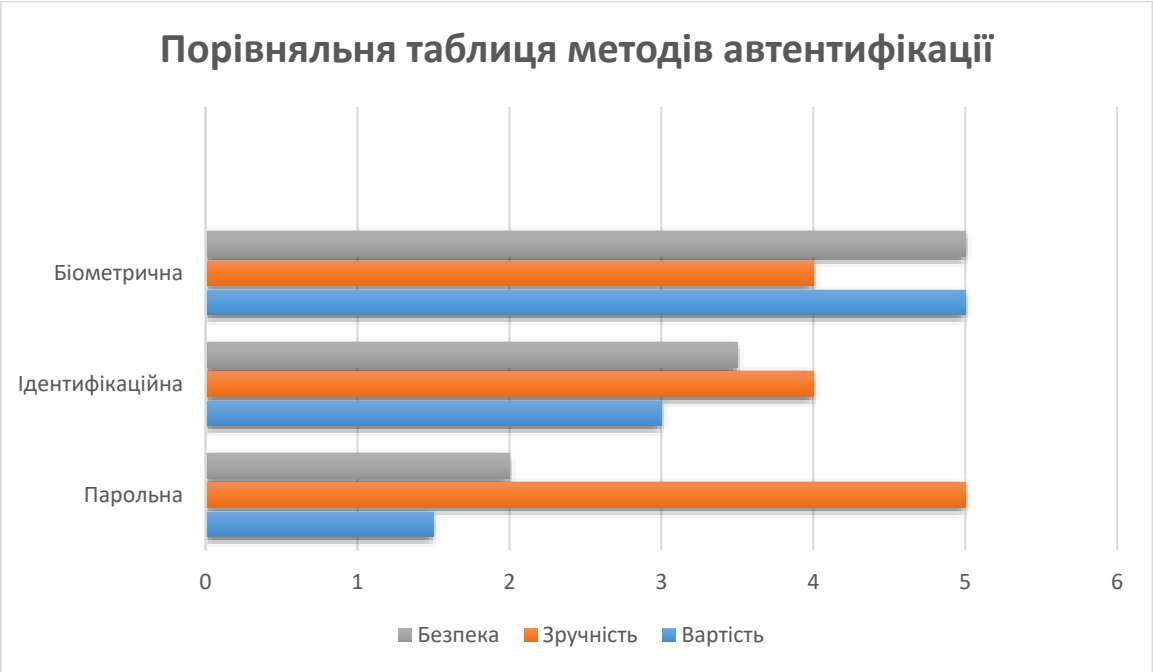
Багатофакторні засоби автентифікації реалізовуються за допомогою комбінування двох різних однофакторних методів, частіше всього ідентифікаційного та парольного. Наприклад: «пароль + додаток», «магнітна карта + PIN». Кожен з типів методів має свої сильні сторони і звичайно недоліки. Нажаль дані методи і засоби мають одну й туж негативну особливість, яка складається в тому, що вони автентифікують не конкретного суб'єкта, а всього фіксують факт, що ідентифікатор

співпадає з автентифікатором суб'єкта . Усі описані методики автентифікації не захищені від втрати,використання втрачених даних автентифікатора [22].

Зараз треба порівняти ці методи за характеристиками:

- Вартість;
- Зручність;
- Безпека.

Це основні критерії для вибору більш зручного методу для власного користування чи для корпорації.



Згідно того, що кожна людина на підприємстві має свою заліковий запис, тому першим етапом автентифікації в побудові нашій двофакторній системі автентифікації. Наступним етапом автентифікації в нашій роботі буде вибраний метод за допомоги ідентифікації додаткового пристрою або системи.

2.5. Висновки

Будь якій структурі необхідно розуміти свої слабкі місця захисту, без цього ніяк не можливо виконати та реалізувати надійний захист особливо не скидувати на “Ні” людський фактор. Тому необхыдно, хоча б , доступ до мережі обмежувати , поскладнювати.

Існує велика кількість пристроїв для проведення аутентифікації суб’єкта, але проблема полягає в тому, що всі високонадійні сервіси дуже дорогі зі складною системою інтеграції.

Але з часом вартість виготовлення буде дешевшати і сам функціонал ще збільшуватись.

Але нажаль на території України до цього тільки доходять, а за кордоном вже відомі компанії приймають троьхфаторні методи аутентифіції особливо до критичних систем та даних.

РОЗДІЛ 3. НАЛАШТУВАННЯ БАГАТОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ

На обладнанні Next Generation Firewall (NGFW) або в побуті брандмауер на базі CISCO ASA була зроблена віртуальна машина, яка виконує такий самий функціонал, але з одним обмеженням це потужність. Ця система після створення являє собою чисте обладнання “з коробки” тобто без будь-якого налаштування та конфігурації. Повна кінцева конфігурація описана в додатку 1. [23]

Далі хочу показати загальну схему.

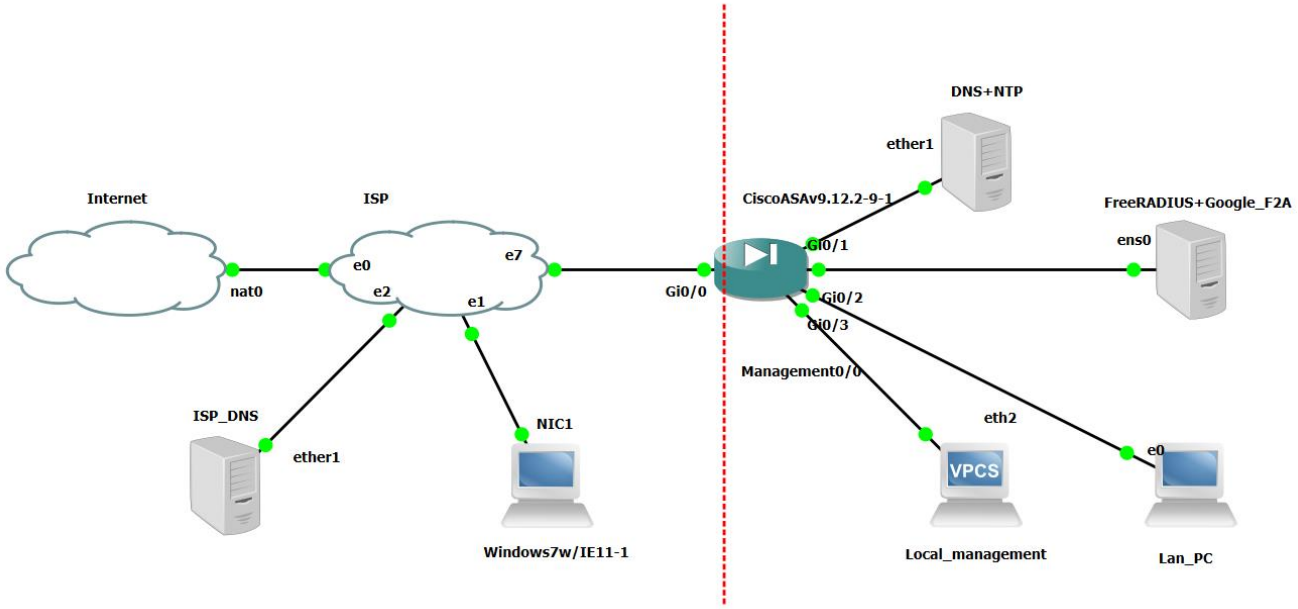


Рис.3.1. Загальна схема

Схема логічно поділена на дві частини, ліва частина зовнішня складова, а права це внутрішня DMZ зона.

Усі інтерфейси на цій частині були умовними і з одним інтернет провайдером. При використанні іншого провайдера картина не поміняється.

На схемі зображені наступні елементи:

- Internet – глобальна мережа;
- ISP – Internet Service Provider, Інтернет провайдер, який забезпечує доступ до глобальної мережі інтернет.
- ISP_ DNS – Домена система яка пов’язує назви доменів з унікальними IP-адресами комп’ютерів, звичайно які відповідають їм. Принцип схожий на телефону

книгу в телефоні або будь-якому девайсі. При введені IP-адреси відбувається співпадіння до певного ресурсу так і навпаки.

- NIC1 – це робоча станція кінцевого споживання. В данному випадку звідки ми будемо роботи VPN з'єдання до корпоративної мережі та робочого місця.
- CiscoASAv9 – віртуальний тенант освного брандмауера.
- DNS+NTP – Внутрішній DNS сервер поєднаний з NTP (Network Time Protocol).
- FreeRADIUS+Google_F2A – Сукупність систем для роботи двофакторної автентифікації.
- LAN_PC – робоча станція;
- Local_management – робоча станція адміністратора мережі.

По корпоративним стандартом для підключення віддаленого робочого місця використовується програма Cisco AnyConnect. Для доступу було достатньо ввести шлях для корпоративного віддаленого підключення і ввести свої унікальні дані логін та пароль. Ця система досить застаріла і не гарантує надійного захисту від підбору або зчитування цієї інформації. І рішенням для покращення надійності це використання двофакторної автентифікації. У нашому випадку будемо використовувати безкоштовний варіант рішення двофактоної автентифікації Google Authenticator.

3.1 Налаштування Cisco Anyconnect на ASA.

За допомогою Cisco ASDM заходимо на наш брандмауер та через вкладку "Wizads" вибираємо нашу систему віддаленого підключення AnyConnect VPN Wizard. [24]

Cisco ASDM являє собою системою для забезпечення керування та моніторингу через зручний та звичний для нас Web-інтерфейс. Ця система спрощує користувачам процес розгортання обладнання цього типу та захист , використовуючи інтелектуальні налаштування, ефективних інструментальних засобів адміністрування та гнучких функцій моніторингу.

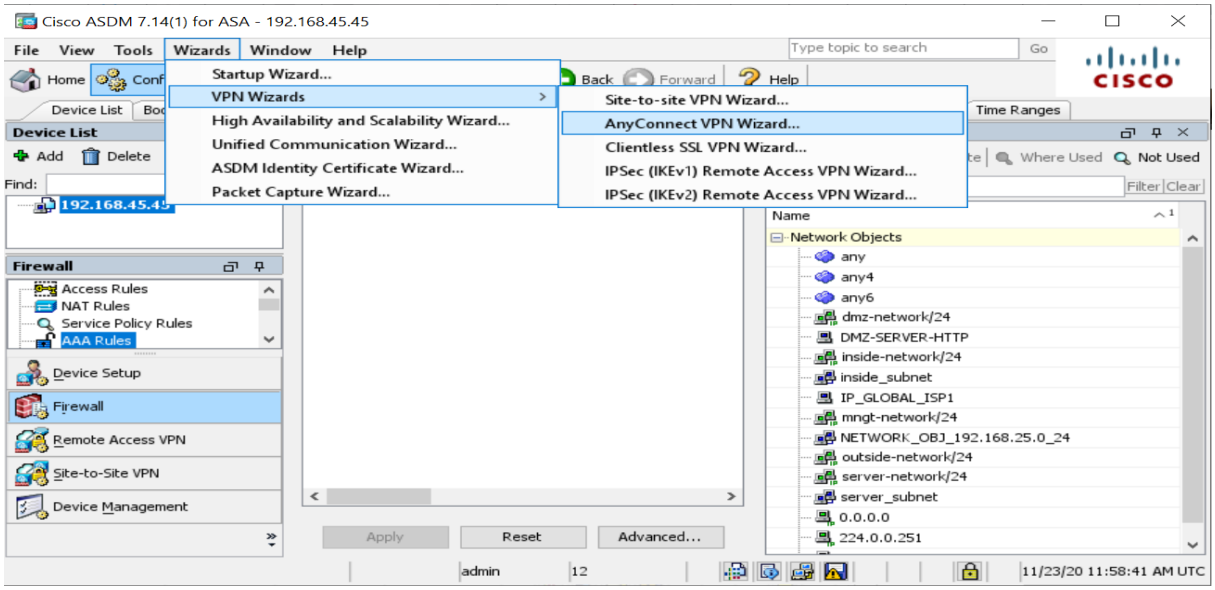


Рис.3.2. За допомогою ASDM, вибираємо наш тип віддаленого робочу столу.

Надалі вибираємо профіль , згідно якого буде працювати наша система з типом інтерфеса, через який буде виконуватись вхід в нашу систему.

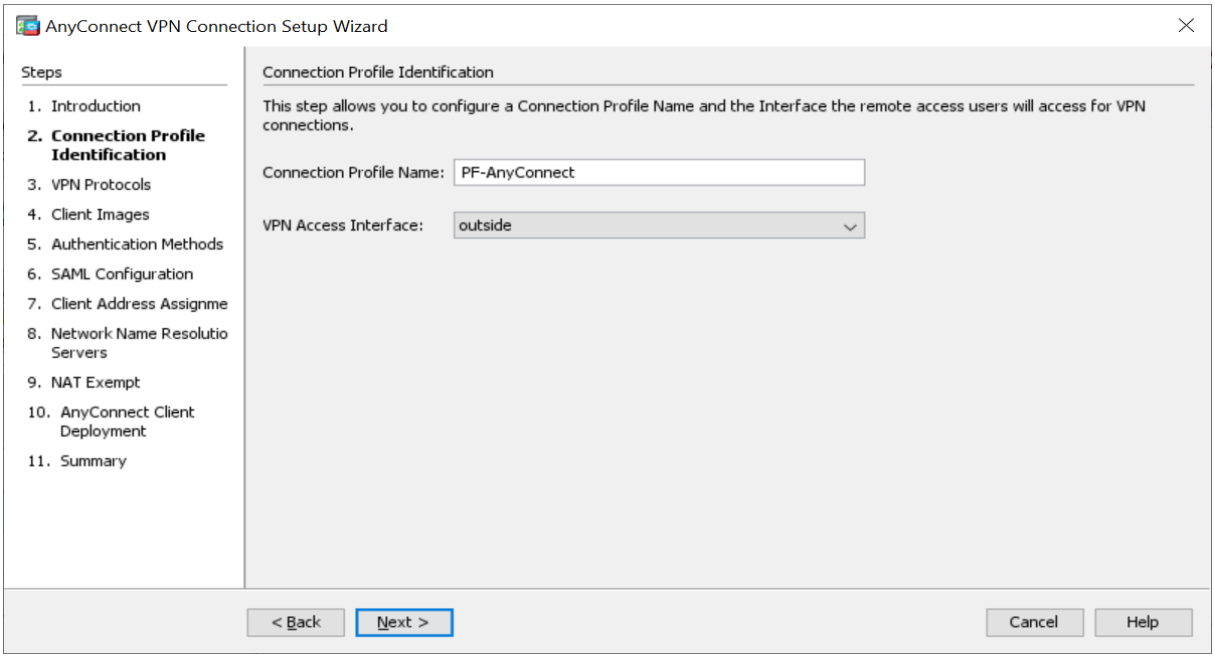


Рис.3.3.Вкладка з типом профайла та внтерфейсом зовнішнього з’єднання

В наступній вкладці перед нами стоїть варінт вибору протоколу побудови VPN каналу з можливістю перевірки сертифікатів між кінцевою точкою та основним сервером.

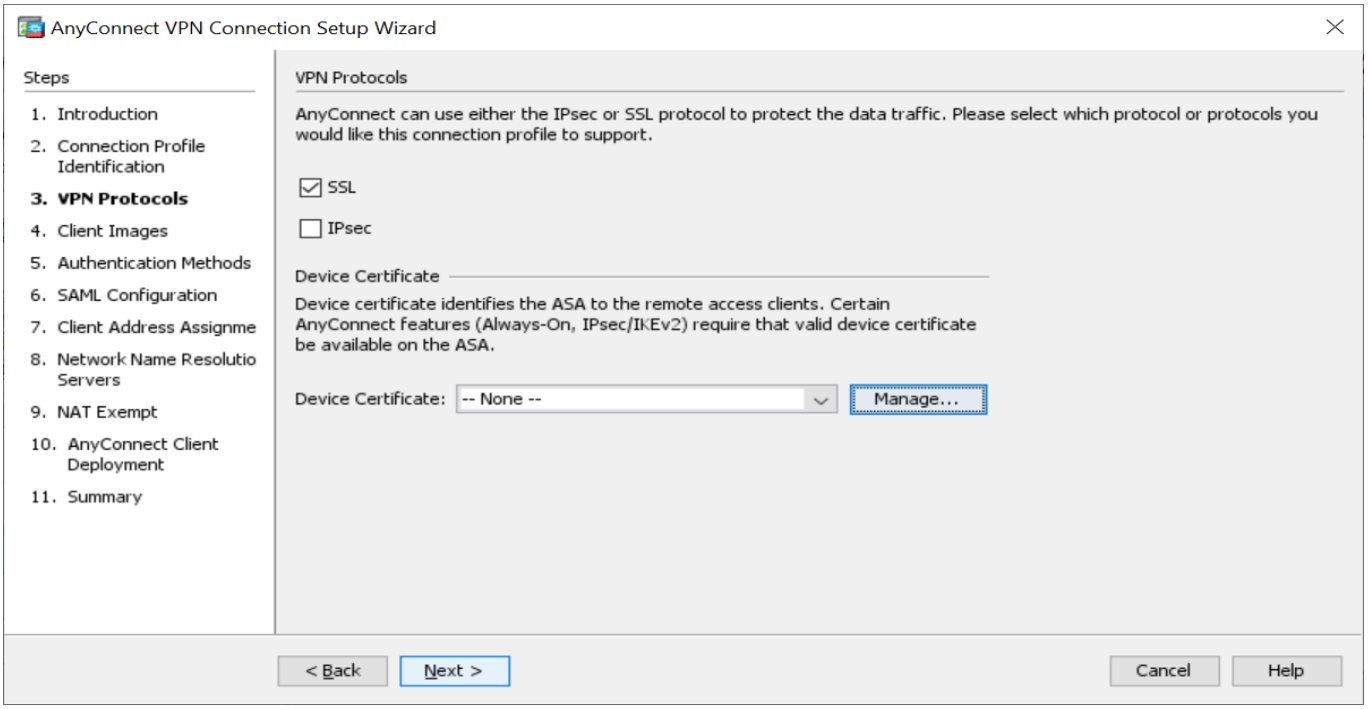


Рис. 3.4. Вибір протоколу VPN

Наступним кроком нам необхідно загрузити в систему останню версію програми Cisco AnyConnect або версію, яку підтримує замовник.

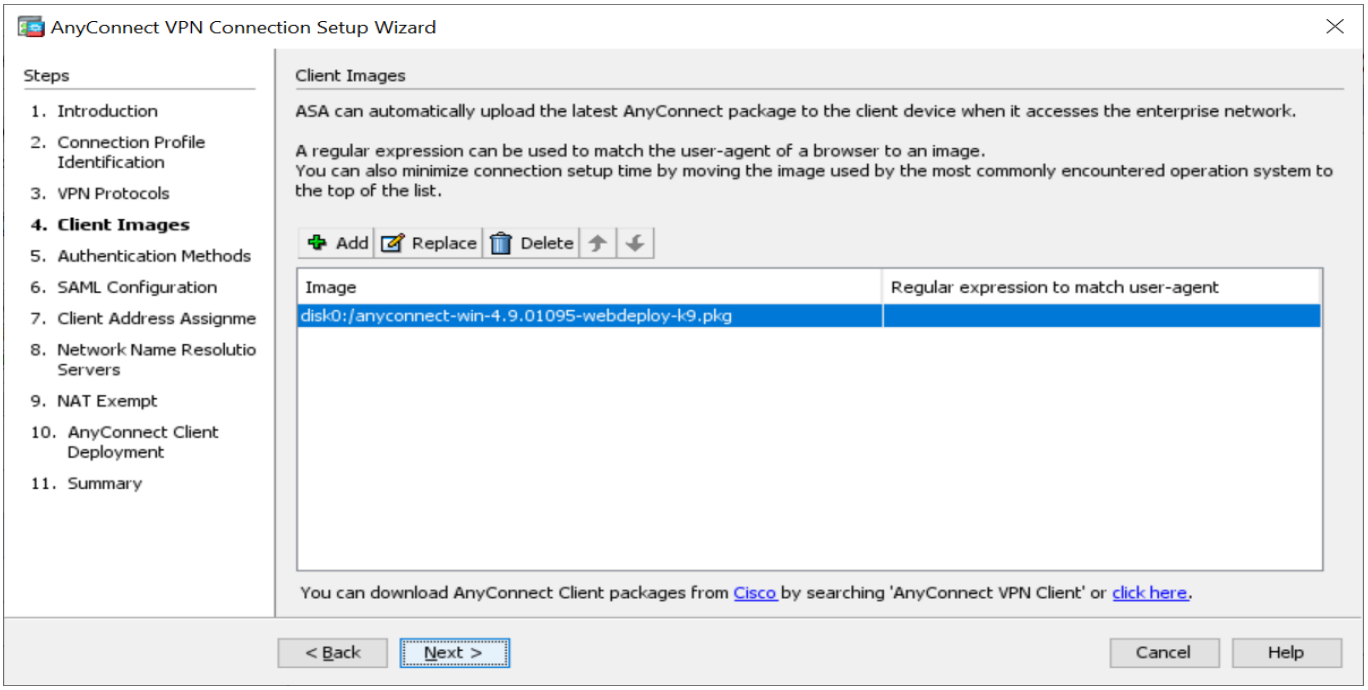


Рис.3.5. Варінти роботи з робочим образом клієнта Cisco AnyConnect

Далі нам необхідно вибрати тип авторизації. Для початку необхідно зробити тестування на

локальному AAA сервері реєстрації з додаванням користувачів до бази даних. Після тестуванню на локальному AAA сервері, переводимо на RADIUS сервер.

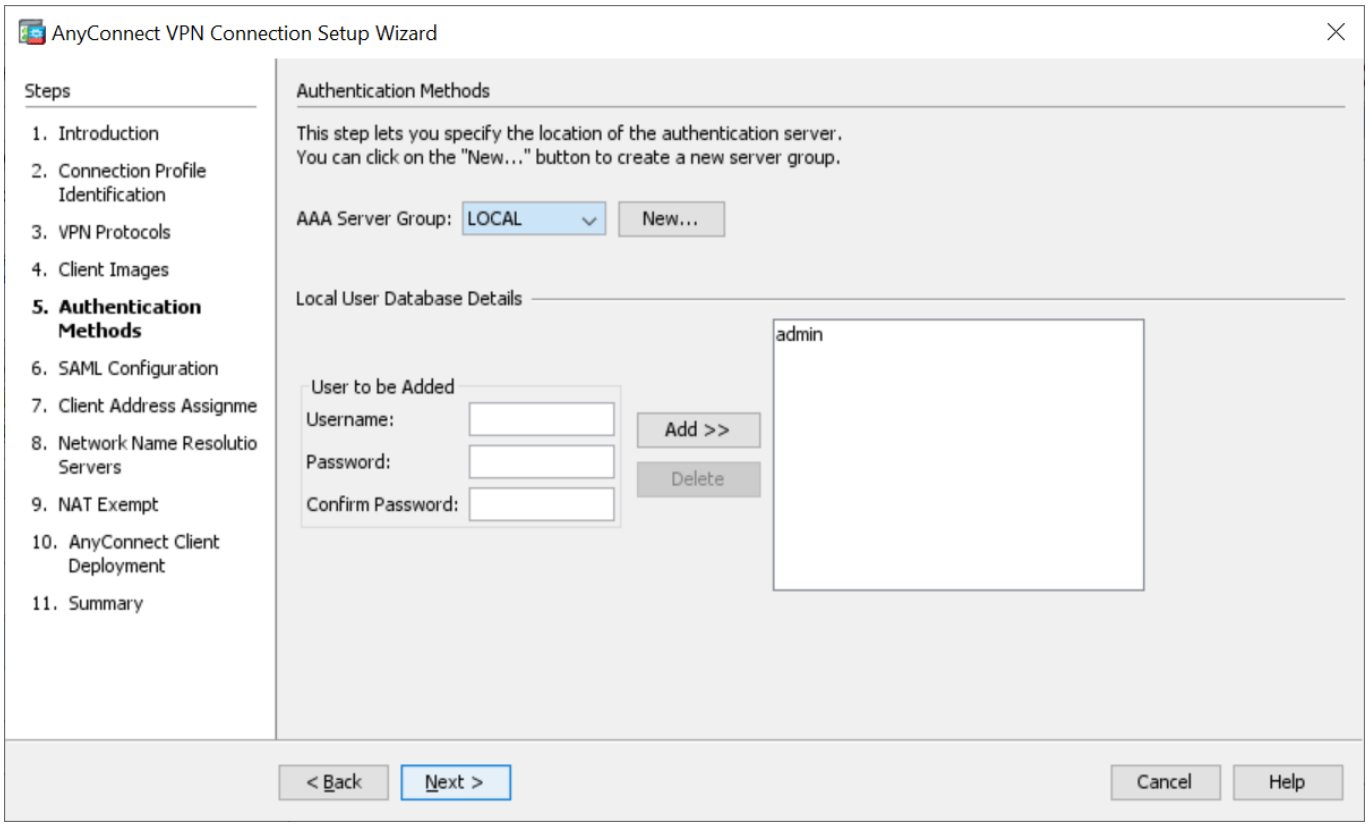


Рис.3.6.Тип Авторизації

Потім нашим кроком становиться вибір автентифікації за допомогою SAML.

Спочатку необхіодно зазначити метод, у нашому випадку це буде AAA з локальною групою серверу. SAML це відкритий стандарт на основі XML, який призначений для обміну інформації автентифікації та авторизації між сторонами. Цей стандарт передбачає за собою можливість обміну інформації облікових записів між довіреними поставщиками сертифікатів та додатків (хмарних або Web-додатків)

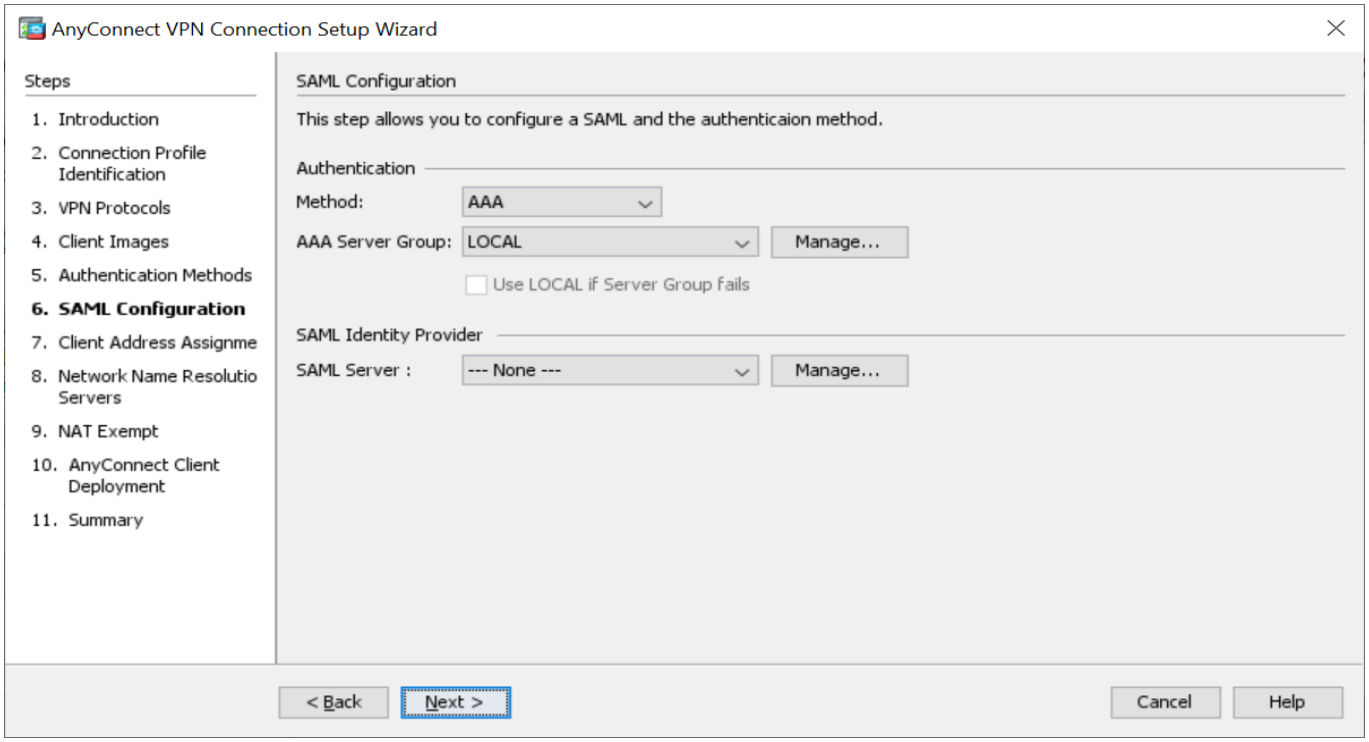


Рис.3.6. SAML автентифікація

Наступним пунктом нам треба визначити діапазон IP адрес який буде видаватись для VPN підключень. Необхідно зазначити , що треба прораховувати таким чином, щоб на кожне 1 нове підключення було виділено дві адреси. Перша адреса для кінцевого користувача, який під'єднується, друга для внутрінього використання на сервері, щоб прив'язати тунель.

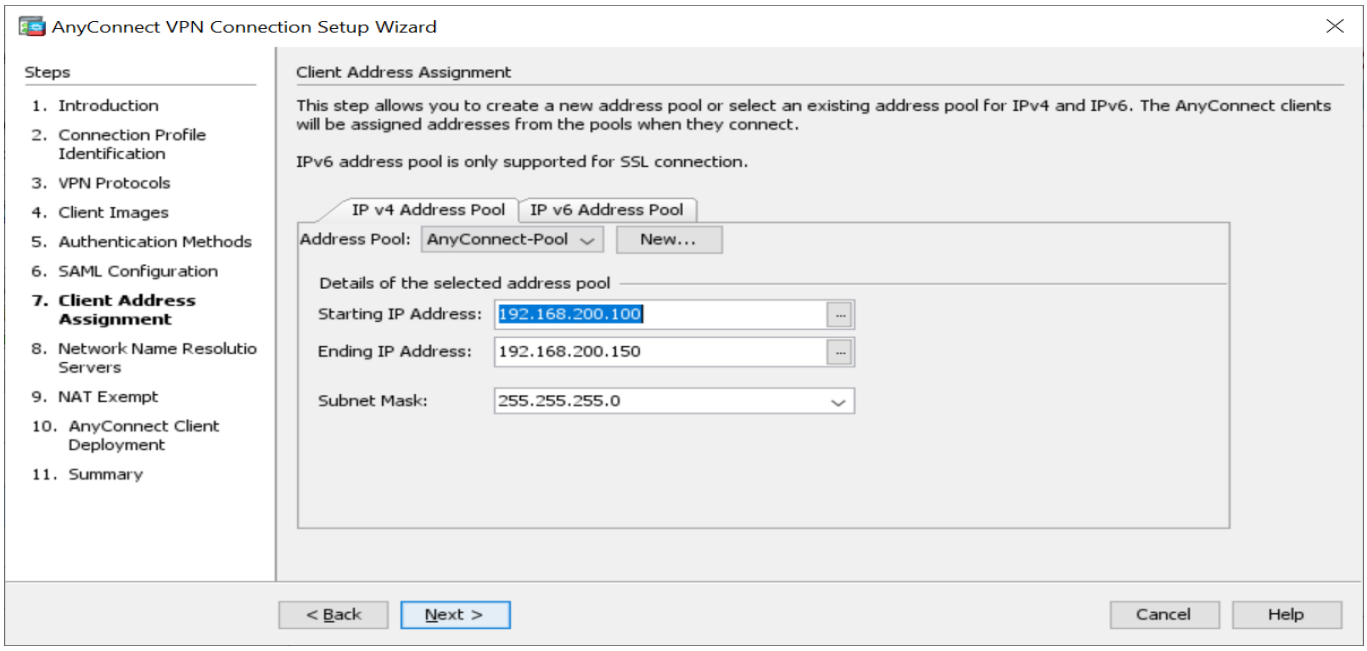


Рис.3.7. Налаштування IP адрес.

Надалі необхідно вказати адресу внутрішнього DNS серверу компанії, звичайно якщо він використовується.

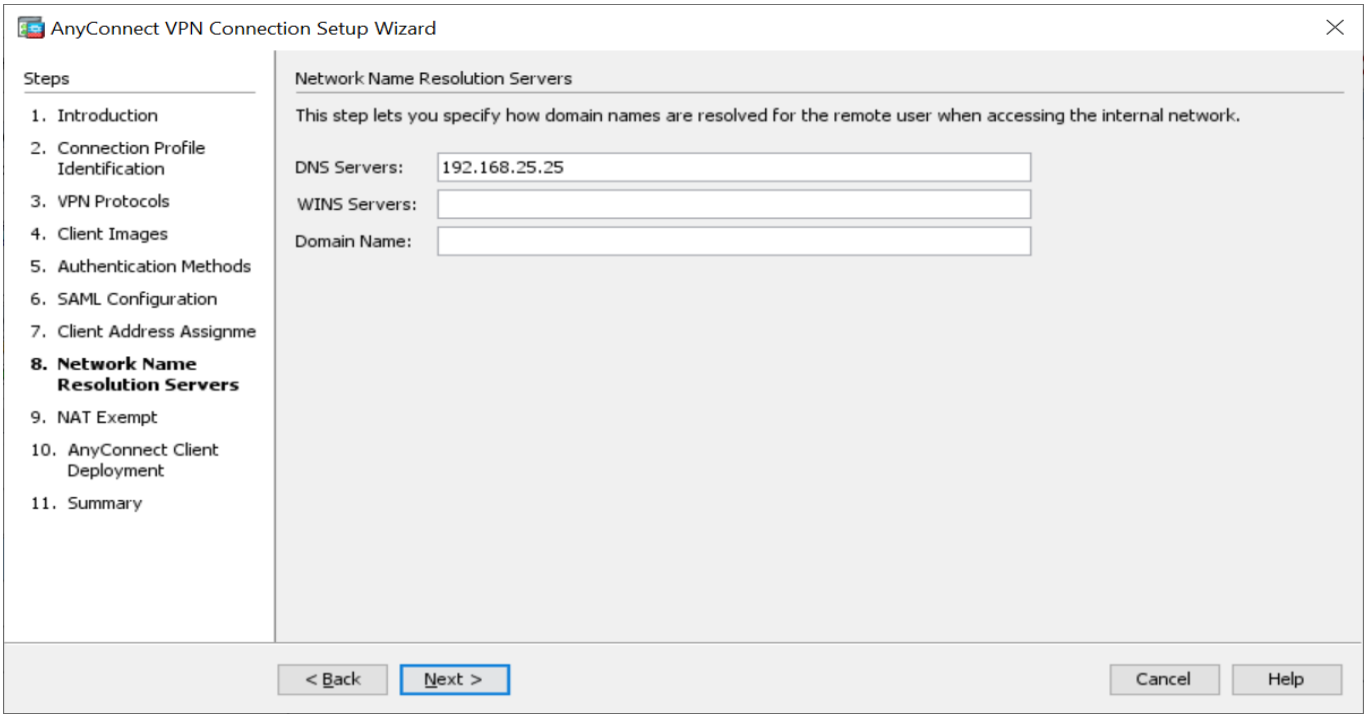


Рис.3.8. Додавання адреси DNS Сервера.

Надалі потрібно застосувати налаштування NAT (Network Address Translation) разом з погодженням доступу до локального внутрішнього сервера.

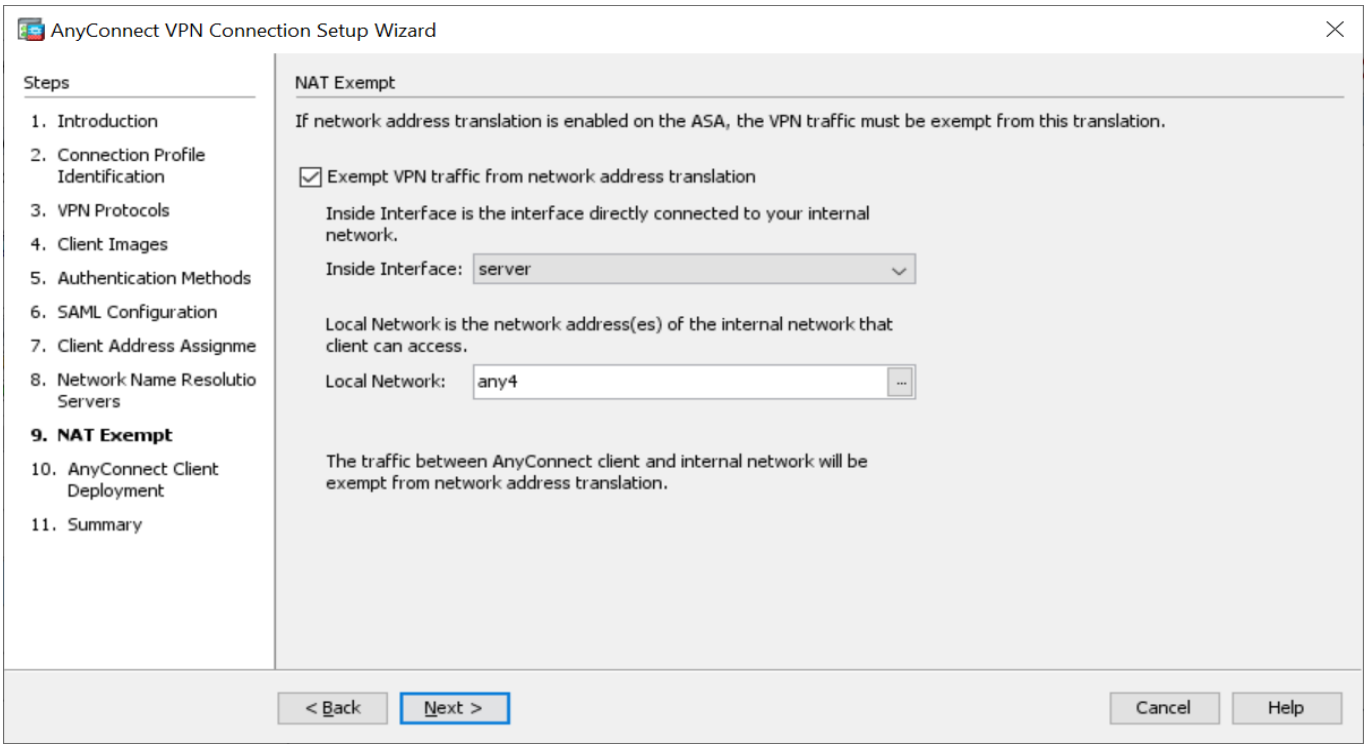


Рис.3.9.Підключення NAT з підключенням внутрішнього серверу.

Десятий пункт налаштування ми пропустимо, так як він містить інформацію текстову щодо завантаження додатку Cisco AnyConnect без будь-якої конфігурації. Тому далі переходимо до останньої вкладки, яка зображена на рис.3.10.

На ньому зображена таблиця з нашими налаштуваннями для фінальної перевірки перед його прийняттям на обладнанні.

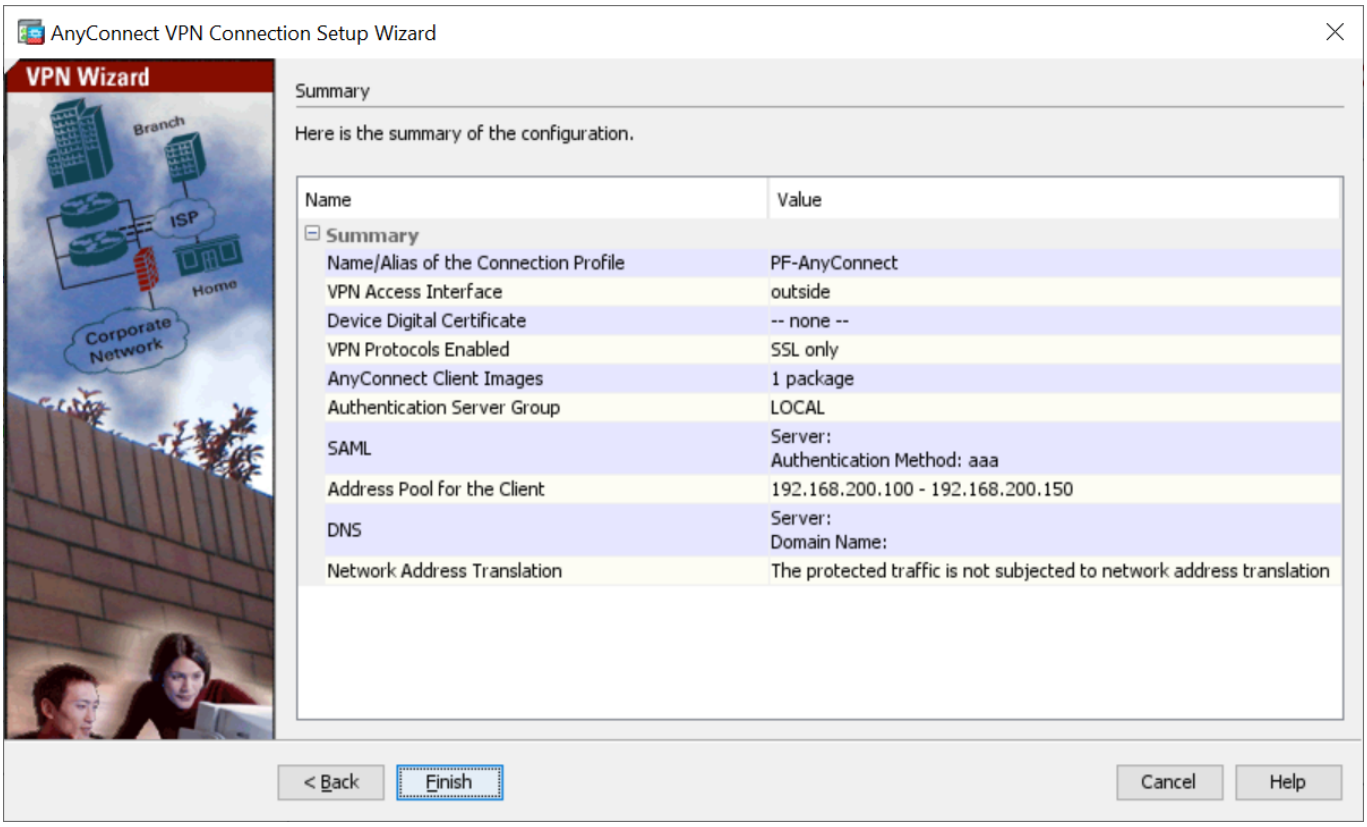


Рис.3.10 Таблиця нашого налаштування.

Перша частина автентифікації парольним методом у нас описана. Далі розглянемо основні моменти налаштування Google Authenticator.

3.2. Налаштування Google Authenticator.

Спочатку ми беремся за скачування Ubuntu серверу, версія 16.0.4.1 була вибрана нами , та розгортаємо на ESX хості. [25]

Конфігурація починається з запуску FreeRADIUS, але його особливість полягає в запуску тільки під root правами (Рисунок 3.11).

```
sudo passwd root
ENTER AND CONFIRM PASSWORD
sudo passwd -u root
```

Рис.3.11. Конфігурація root прав.

Після цього важливо оновити всю систему та налаштувати NTP. Це необхідно для генерації ключів від Google. Ці процеси зображені на рис3.12 та 3.13

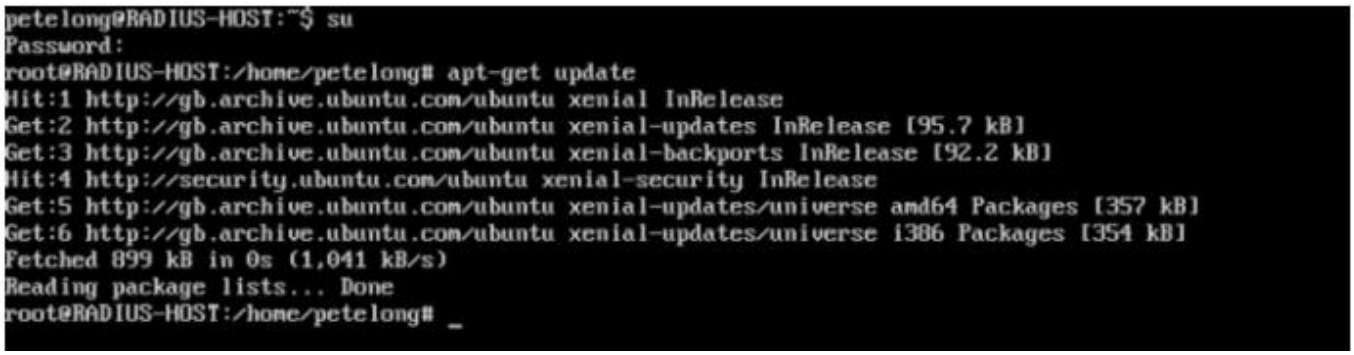


Рис.3.12. Конфігурація оновлення системи

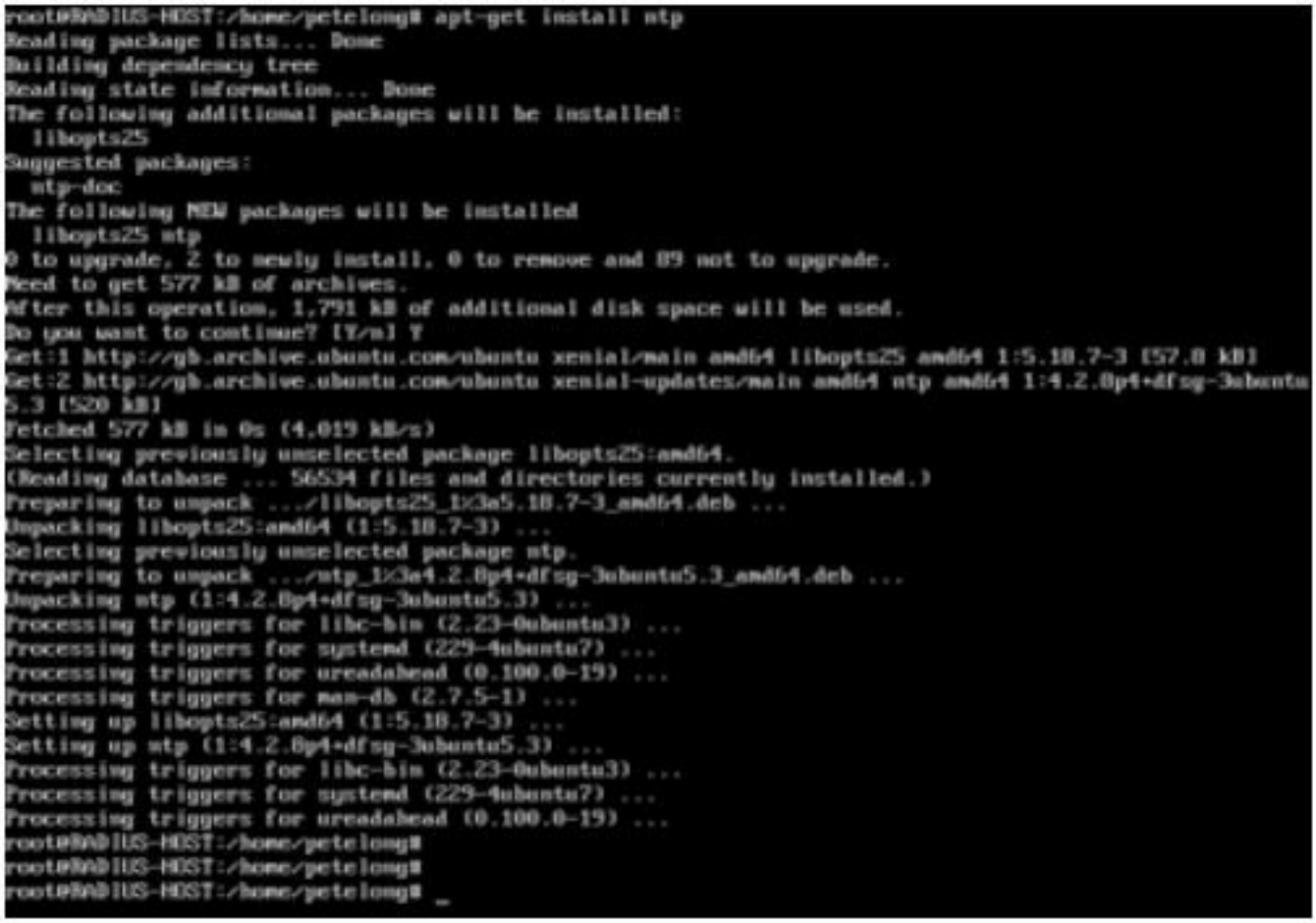


Рис.3.13. Налаштування NTP

3.2. Налаштування Google Authenticator.

Наступним етапом є підключення Google Authenticator. Для цього треба додати папку з інстялятором до web-серверу, далі в каталозі вибрати цей матеріал і інсталювати його. Команда зображена на рисунку.3.14. [26]

```
cd ~
git clone https://github.com/google/google-authenticator.git
cd google-authenticator/libpam/
./bootstrap.sh
./configure
make
make install
```

Рис.3.14. Інсталювання опрограмного забезпечення Google Authenticator.

Наступним етапом у нас буде налаштування FreeRadius з Google Authenticator.

Спачатку треба поміняти FreeRadius, оскільки він працює з правами “root”, згідно рис.3.15.

```
nano /etc/freeradius/radiusd.conf
```

Рис.3.15. Зміна доступу.

В самому файлі конфігурування треба замінити користувача и групу з freerad на root. Та не забути зберегти файл. Ця процедура зображена на рис.3.16. Зміни помічені червоним кольором.

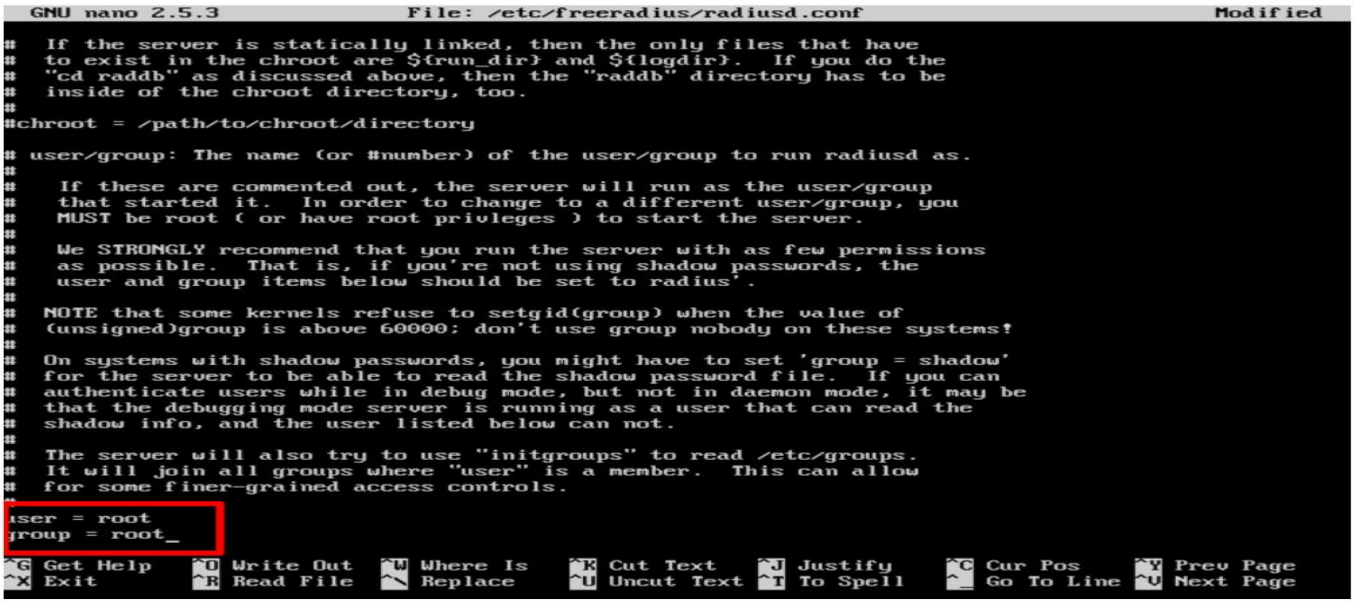


Рис.3.16. Заміна користувача та групи.

Надалі можливо створити окрему групу , в яку можна занести не бажаних користувачів. Цю групу я назвав “radius-disabled”. Цю процедуру зображено на рис.3.17.

```
addgroup radius-disabled
```

Рис.3.17. Створення групи “radius-disabled”.

Надалі конфігуруємо FreeRADIUS на відхилення членів цієї групи, згідно рис.3.18.

```
nano /etc/freeradius/users
```

Рис.3.18. Налаштування Radius для відхилення цих користувачів.

Далі треба замінити деяку конфігурацію на сервері, вказуючи наступні параметри, згідно рис.3.19.

```
DEFAULT Group == "radius-disabled", Auth-Type := Reject
        Reply-Message = "Your account has been disabled."
DEFAULT Auth-Type := PAM
```

Рис.3.19. Прописання нових політик в загальній конфігурації.

Загальний вигляд конфігурації,після попередньої зміни, повинен виглядати як на рис.3.20.

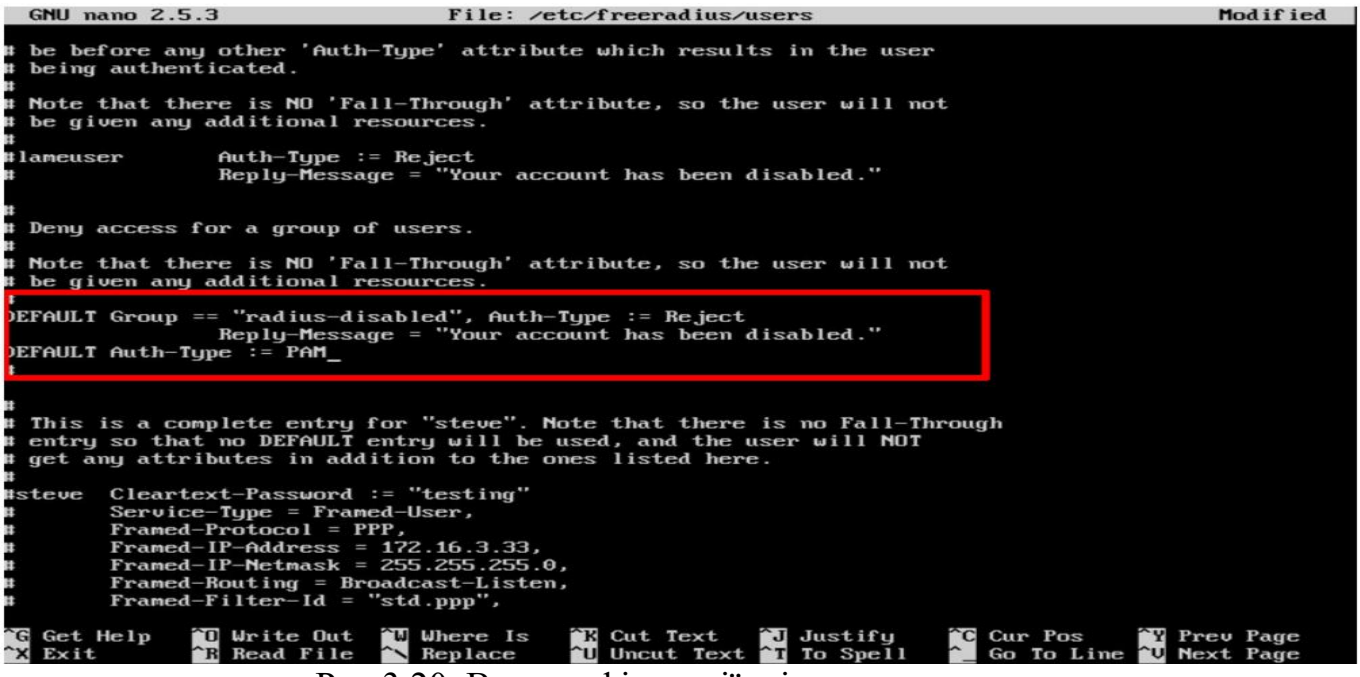


Рис.3.20. Вид конфігурації згідно нових введень.

Далі редагуємо файл, активуючи PAM (Pluggable Authentication Mode) за допомогою команди на рис.3.21.

```
nano /etc/freeradius/sites-enabled/default
```

Рис.3.21. Активація PAM

Надалі наша конфігурація повинна виглядати, як зображено на рис.3.22

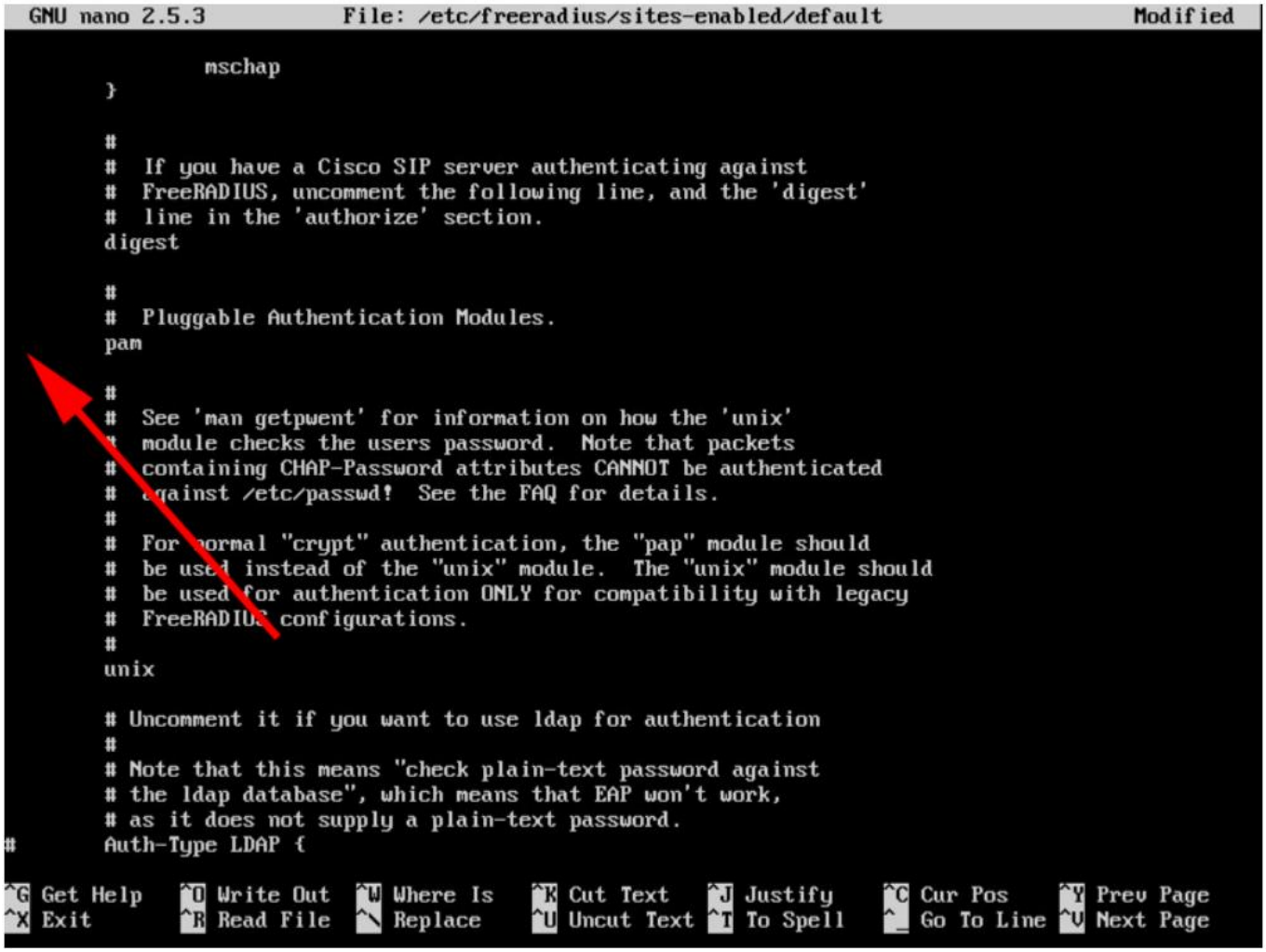


Рис.3.22 Вигляд оновленої конфігурації.

Червоним кольором помічено місце на якому не повинно бути символу решітка «#», іначе зміни не відбулись.

Далі налаштовуєм FreeRADIUS для використання Google Authenticator. Спочатку треба редагувати наступний файл, згідно рис.3.23.

```
nano /etc/pam.d/radiusd
```

Рис.3.23. Редагування файлу pam.d.

В цьому документі треба знайти всі строки, які починаються з “@” і замінити на “#”, так сказати зарекомендувати їх і в кінці документу вставити наступну конфігурацію, яка зображена на рисунку.3.24.

```
auth requisite /usr/local/lib/security/pam_google_authenticator.so forward_pass
auth required pam_unix.so use_first_pass
```

Рис.3.24. Додавання нової конфігурації.

Для перевірки ,чи все вірно, можна побачити на рис.3.25. Усі зміни помічені червоним.

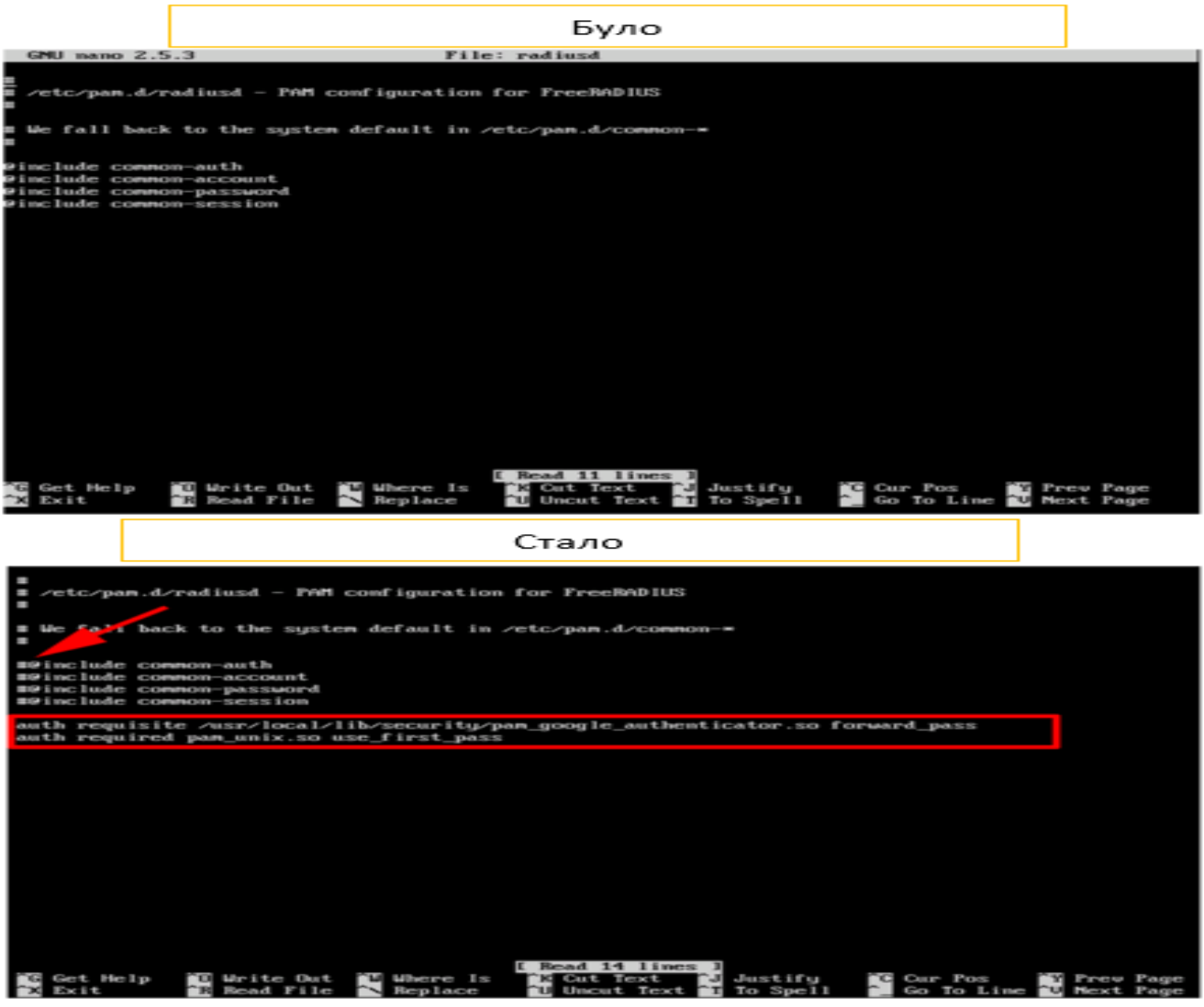


Рис.3.25. Порівняння конфігурації після застосування попередньої команди.

Далі приступаємо для перевірки працездатності нашої конфігурації FreeRadius з Google Authenticator. Найпростішим варіантом являється налаштування тестового користувача зі створенням паролю для нього, потім присвоїти Google Authenticator код на Linux сервері.

```
adduser tommytester
ENTER AND CONFIRM PASSWORD
su tommytester
ENTER THE PASSWORD
google-authenticator
```

Рис.3.26. Зразок додавання тестового користувача.

Далі, можете за допомогою двох методів пройти автентифікацію, за допомогою сканування QR коду в додатку Google Authenticator або введенням секретного паролю також в додаток. Приклад коду можна побачити на рис.3.27.

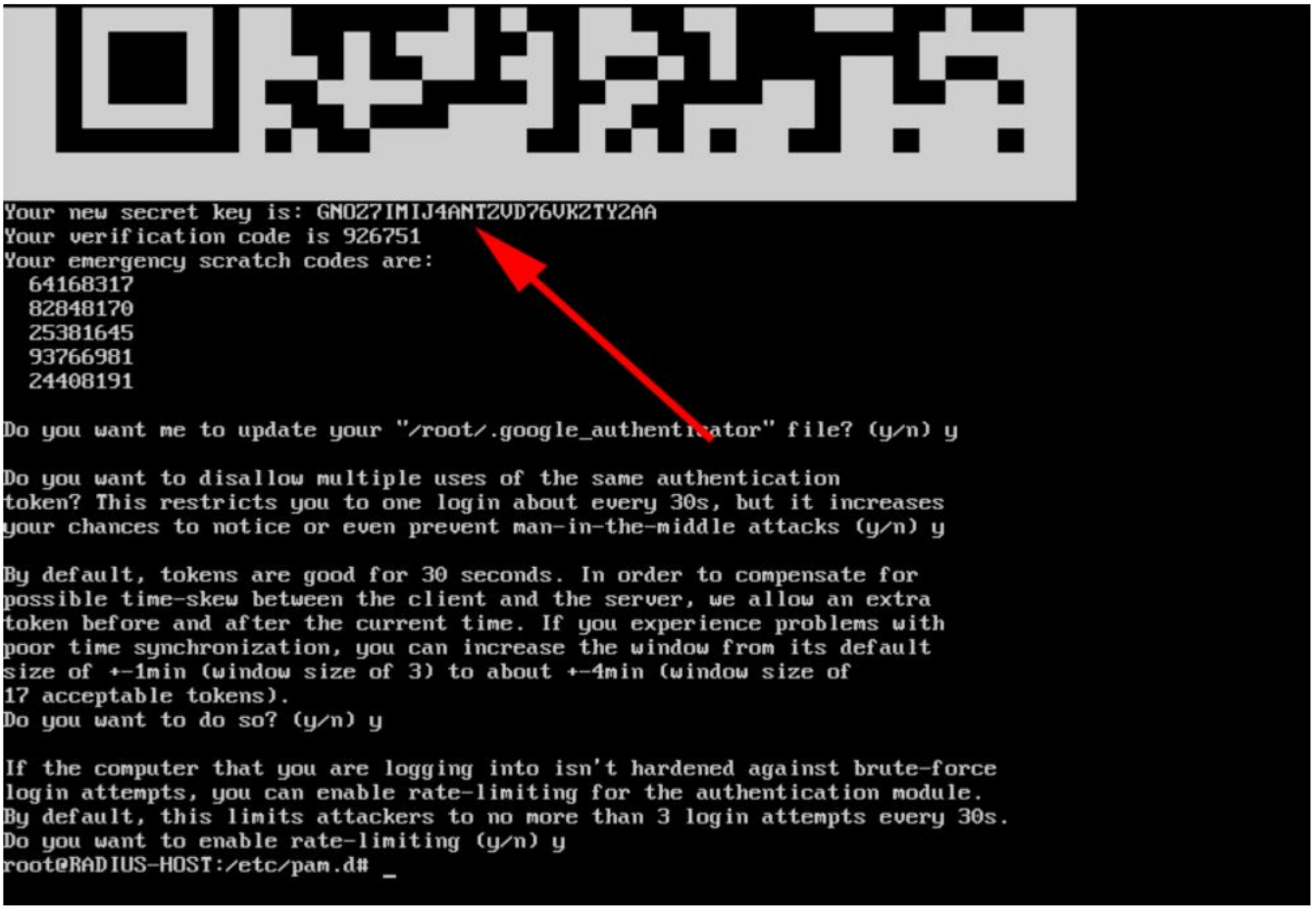


Рис.3.27. Приклад коду для введення в Google Authenticator

Після виконання одного з вище наведених рішень ви побачите шестизначний код, який генерується кожні 30 секунд. Приклад коду зображено на рис.3.28.

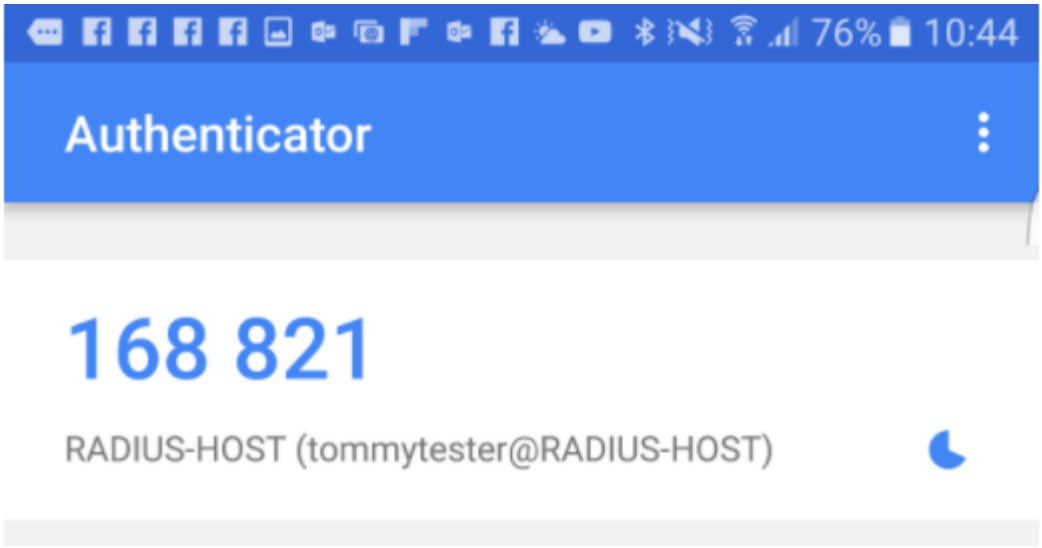


Рис.3.28. Зразок шестизначного коду автентифікації.

Звичайно ще треба протестувати наш FreeRADIUS сервер за допомогою команди, яка описана на рис.3.29.

```
radtest tommytester password456743 localhost 18120 testing123
```

Рис.3.29. Команда тестування нашого RADUIS сервера.

Але треба зазначити, що пароль для tommytester – “пароль”, а в кінець додається 6-значний код, значення testing123 встановлюється в FreeRadius у файлі /etc/freeradius/clients.conf. Після виконання цієї процедури система видасть два варінта вдалу спробу або невдалу. Зразки варіантів можна побачити на рис.3.30.

Варіант з успішною авторизацією

```
tommytester@RADIUS-HOST:/home/petelong$ radtest tommytester password302971 localhost 18120 tes
ting123
Sending Access-Request of id 165 to 127.0.0.1 port 1812
 User-Name = "tommytester"
 User-Password = "password302971"
 NAS-IP-Address = 192.168.110.85
 NAS-Port = 18120
 Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=165, length=20
tommytester@RADIUS-HOST:/home/petelong$
```

Варіант з невдалою авторизацією

```
tommytester@RADIUS-HOST:/home/petelong$ radtest tommytester password302973 localhost 18120 tes
ting123
Sending Access-Request of id 36 to 127.0.0.1 port 1812
 User-Name = "tommytester"
 User-Password = "password302973"
 NAS-IP-Address = 192.168.110.85
 NAS-Port = 18120
 Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=36, length=20
tommytester@RADIUS-HOST:/home/petelong$
```

Рис.3.30. Зразки варіантів авторизації

Для поєднання цього методу автентифікації нам необхідно наш робочий брандмауер додати до переліку користувачів RADIUS. Для цього треба модифікувати наступний файл, це вказано на рис 3.31 з додаванням Cisco ASA в користувачі, рис 3.32.

```
nano /etc/freeradius/clients.conf
```

Рис.3.31. Посилання на необхідний файл модифікування.

```
client 192.168.110.1 {
 secret = cisco123
 shortname = CiscoASA
 nastype = cisco
}
```

Рис.3.32. Команда додавання нового користувача зі зміною назви, якщо необхідно.

3.4. Налаштування CISCO ASA під FreeRADIUS.

Для налаштування ASA нам треба було зробити AAA группу, присвоївши їй групу автентифікації на RADIUS, потім додаємо сервер FreeRADIUS в якості хосту, вказуючи секретний ключ, який ми використовували раніше на рис.3.27. [27]

Треба зазначити, що необхідно вказати порти, або відбудеться збій автентифікації (ми отримаємо повідомлення про відсутність відповіді від RADIUS сервера). Додатково нагадую, що наш брандмауер повинен мати коректний час для роботи, бо не відбудеться синхронізація сервісів.

```
aaa-server PNL-RADIUS protocol radius
aaa-server PNL-RADIUS (inside) host 192.168.110.85
 authentication-port 1812
 accounting-port 1813
 key cisco123
 radius-common-pw cisco123
 exit
```

Рис.3.33. Налаштування FreeRADIUS в якості автентифікації.

Далі нам необхідно змінити метод AAA автентифікації в нашій програмі Cisco AnyConnect. Якщо попередньо нічого не було встановленно, то система використовує локальну базу даних користувачів з паролями. Зараз нам треба її замінити, що б використовувати тільки наш налаштований RADIUS хост. Це можливо зробити у вкладці “tunnel-group general-attribures”. Виконавши команду show run tun , ми побачимо перелік тунельних груп.

```
Petes-ASA# show run tun
tunnel-group ANYCONNECT-PROFILE type remote-access
tunnel-group ANYCONNECT-PROFILE general-attributes
 address-pool ANYCONNECT-POOL
 default-group-policy GroupPolicy_ANYCONNECT-PROFILE
tunnel-group ANYCONNECT-PROFILE webvpn-attributes
 group-alias ANYCONNECT-PROFILE enable
```

Рис.3.34. Перелік груп на нашій Cisco ASA.

Далі необхідно додати нашу радіус групу в якості автентифікаційного сервера.

```
Petes-ASA# tunnel-group ANYCONNECT-PROFILE general-attributes
Petes-ASA(config-tunnel-general)# authentication-server-group PNL-RADIUS
```

Рис.3.35. Додавання нашого RADIUS сервера.

Наша конфігурація повністю готова. Залишилось лише інсталювати додаток Cisco AnyConnect на наше віддалене робоче місце.

Встановлення Cisco AnyConnect на робоче місце

Для початку нам треба зайти на ресурс для завантаження додатка Cisco AnyConnect, Після чого запустити програму встановлення завантаженого додатку.[28]

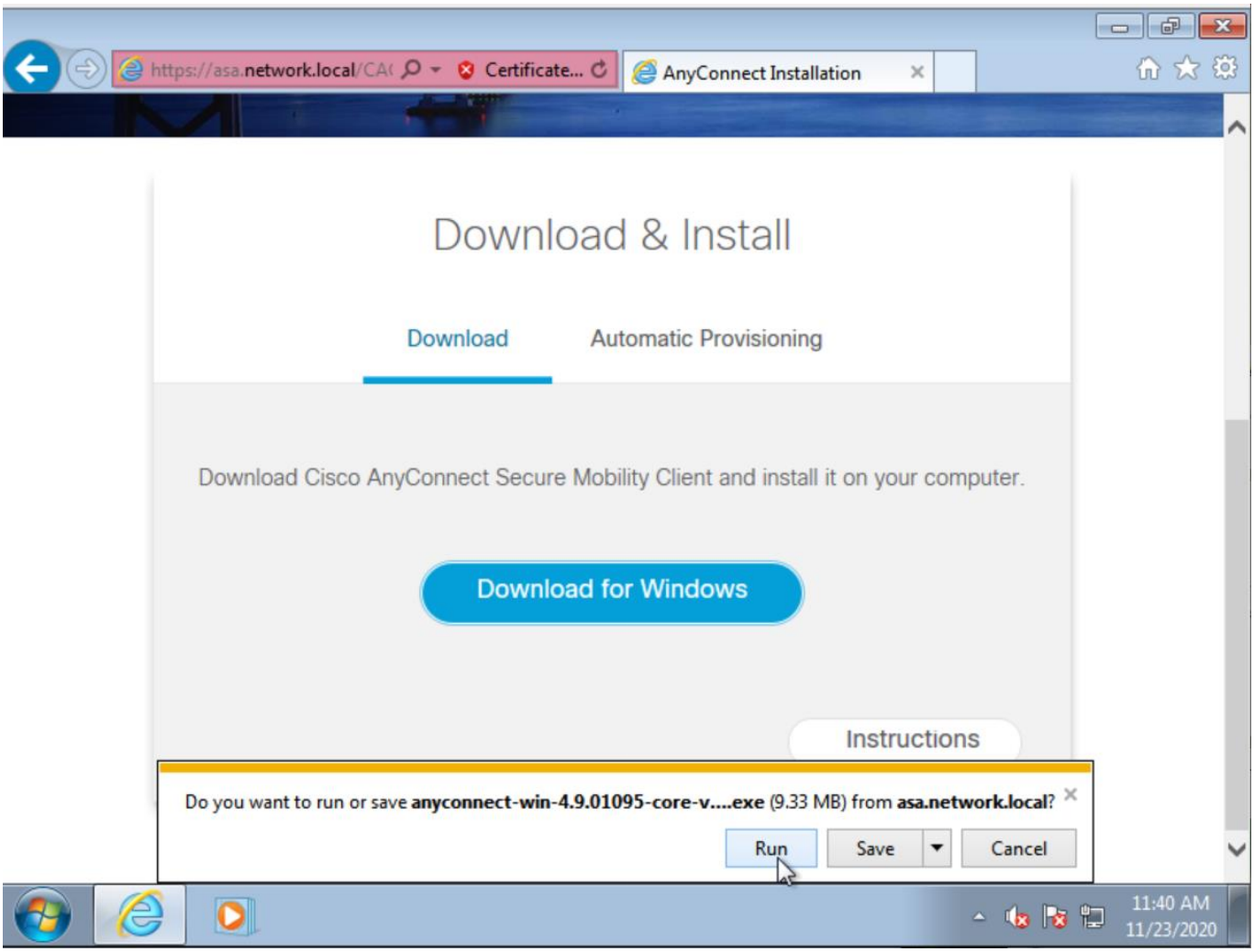


Рис.3.36. Запуск завантаженого додатку

Після чого запускається стартова сторінка інсталювання Cisco AnyConnect,де ми повинні перейти на наступний етап, натиснувши “Next”.

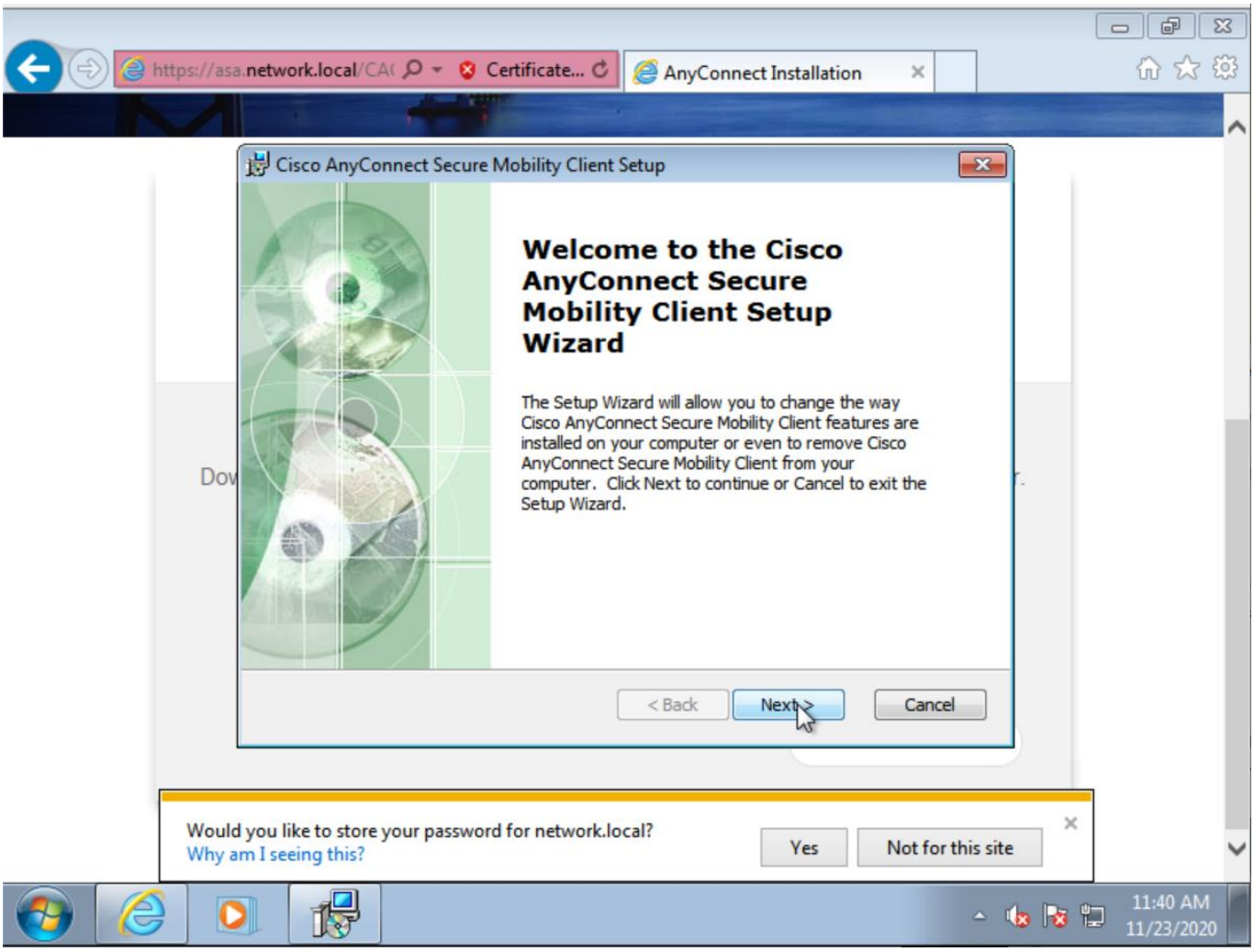


Рис.3.37 Стартова сторінка інсталятора Cisco AnyConnect.

Далі система нам пропонує варіанти інсталяції додатку. MainFeature- основна частина додатку. Win32Only – варіант для тридцяти двох розрядній операційних систем Windows.ReleaseOnly – варіант інсталювання тестового програмного забезпечення. Для нас обхідна частина з повністю працюючою частиною, тому вибираємо MainFeature.

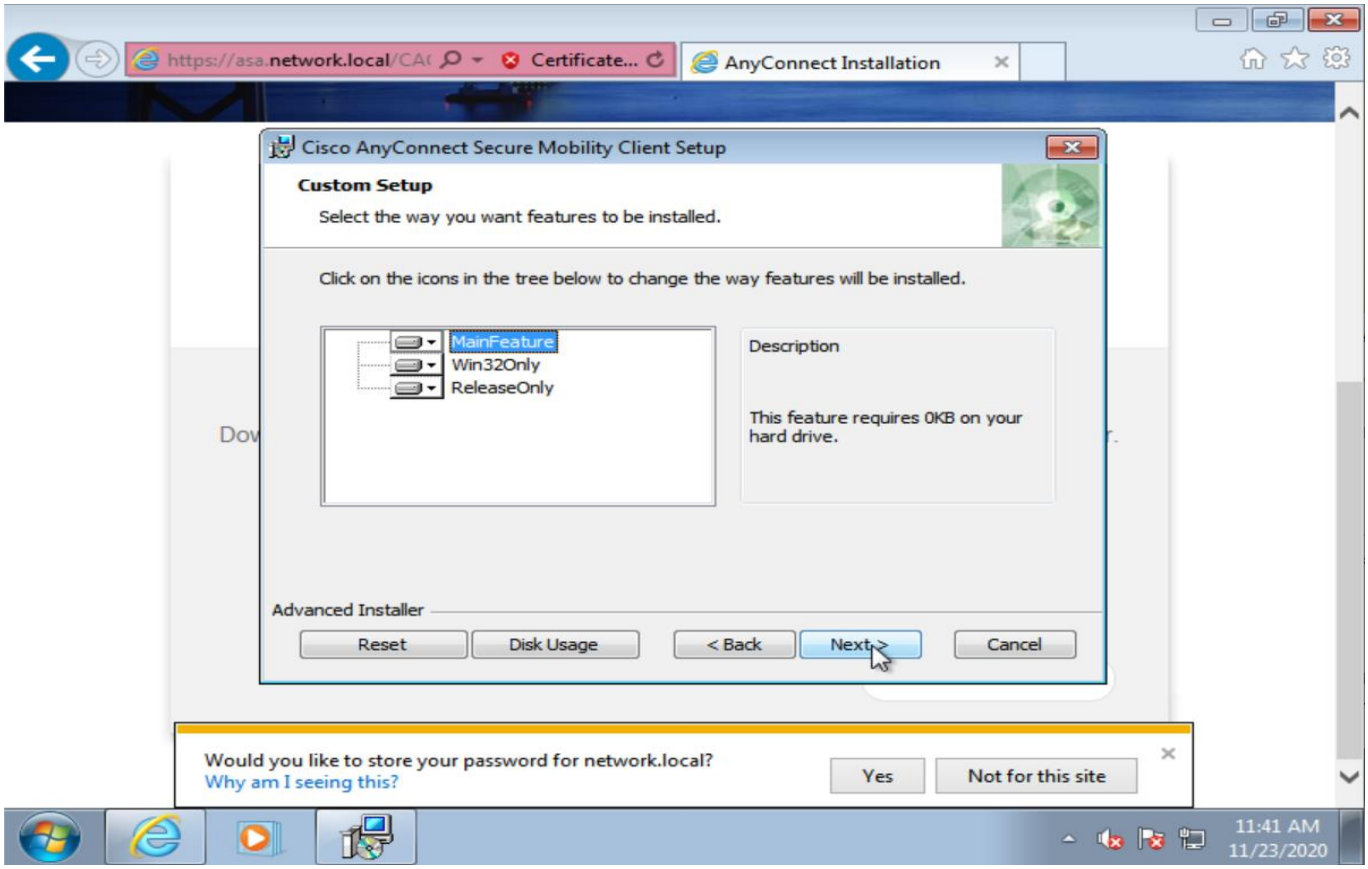


Рис.3.38. Вибір унікального інсталювання.

Далі погоджуємось з останнім слайдом і переходимо до частини інсталювання, очікуємо деякий час і наша система інстальована успішно, що можемо побачити на рисунку.3.39.

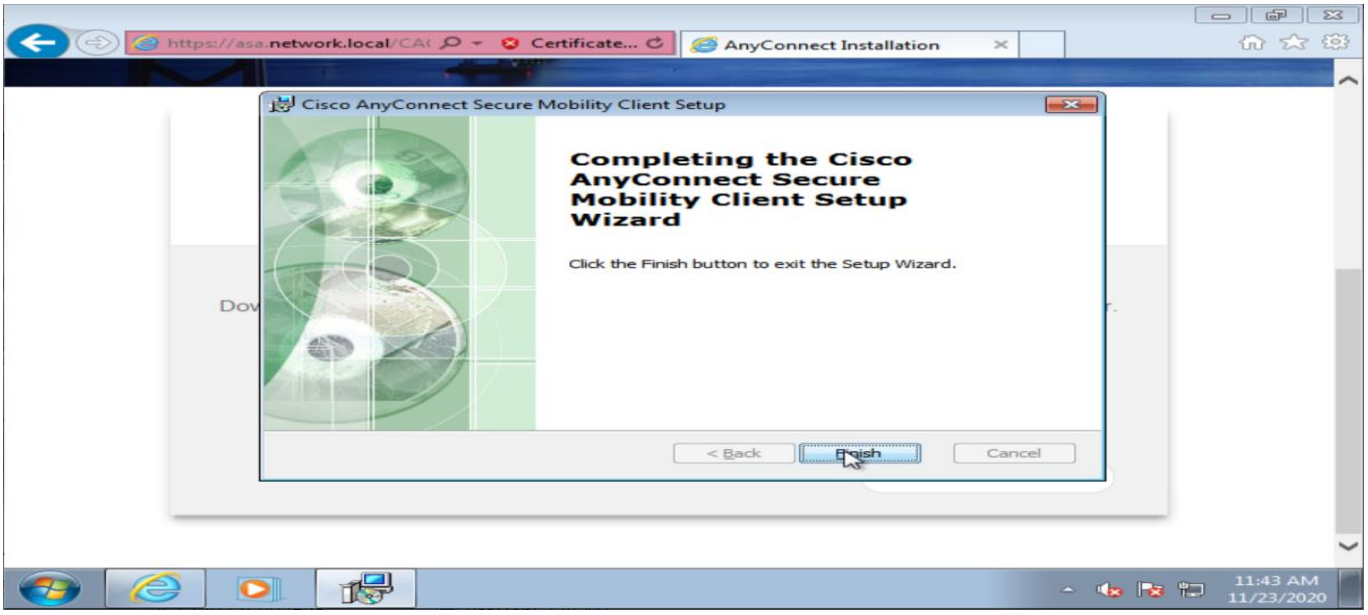


Рис.3.39. Вікно успішного інсталювання Cisco AnyConnect.

Надалі перевіряємо наскільки вдала робота. Відкриваємо кліент програми , вводимо посилання на наш робочий Cisco ASA з коректним профілем тунельної групи а саме його адресу, що зображене на рис.3.40.

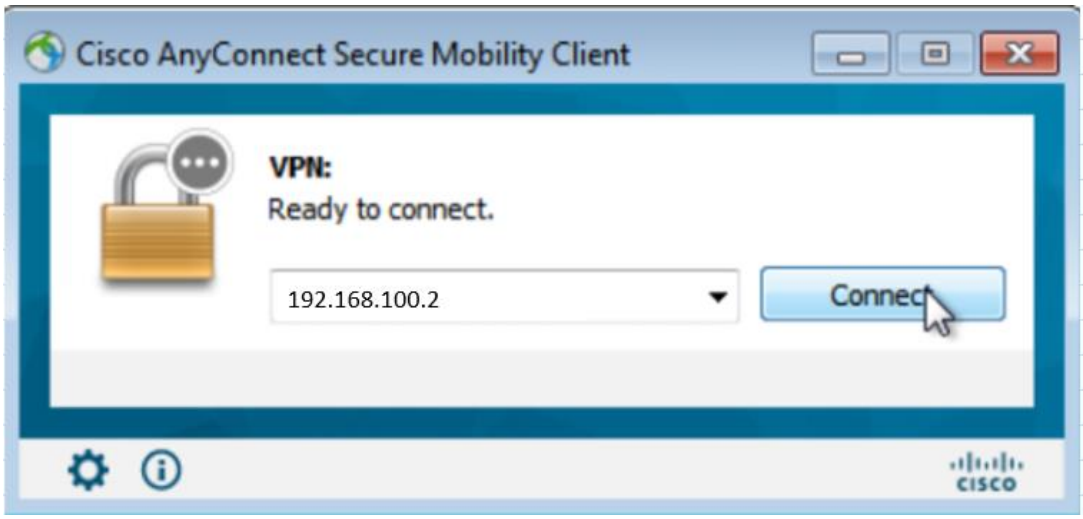


Рис.3.40. Прописання адреси підключення

Надалі висвічується вікно для введення нашого облікового запису. Спочатку вводимо наш логін в строчці “Username”, далі необхідно в полі “Password” внести наш персональний пароль та згенерований пароль нашим додатком, який інстальований на мобільному телефонію. Треба спочатку вказати наш пароль від облікового запису та одразу згенерований пароль системою(обов’язково без введеня пробілів або інших символів). Далі натискаємо “ОК” і бачимо що система нам дозволяє зайти за нашими даними, тобто двофакторна автентифікація пройдена.

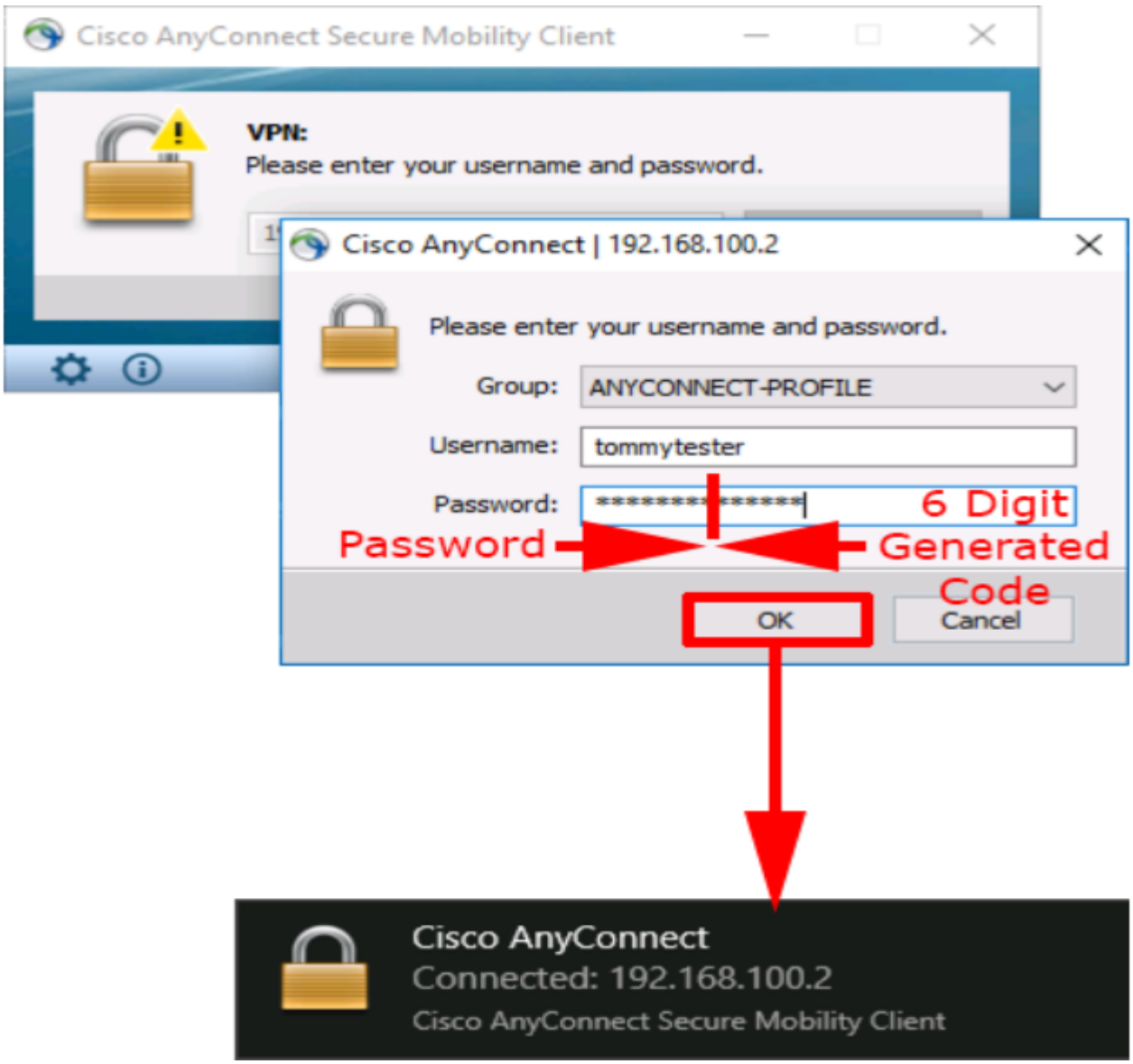


Рис.3.41.Процедуравведення двофакторної автентифікації.

3.5. Розрахунок коефіцієнту захисту від несанкціонованого доступу методу багатофактороної автентифікації.

Далі хочу прорахувати загальний коефіцієнт захисту моєї системи від несанкціонованого доступу розробленим вище вище методу. Для розрахунку нам треба використати наступну формулу розрахунку, яка вкаже нам імовірність несанкціонаваного доступу в струткурі багатофакторної автентифікації за теоремою множення ймовірностей. [29]

$$P_{\text{йнд}} = P_{\text{п}}^{\text{йпп}} \times P_{\text{к}}^{\text{йпк}} = (1 - P_{\text{п}}) \times (1 - P_{\text{і}})$$

Опис даних:

$P_{\text{йнд}}$–ймовірність несанкціонованого доступу;

$P_{\text{п}}^{\text{йпп}}$ –ймовірність підбору паролю;

$P_{\text{к}}^{\text{йпк}}$– ймовірність підроблення коду;

$P_{\text{п}}$–ймовірність правильного використання паролю;

$P_{\text{і}}$– ймовірність правильного використання ідентифікатора.

Вхідні дані для двох методів ідентифікації виглядають наступним чином:

$P_{\text{в}} = 0{,}7$

$P_{\text{п}} = 0{,}91$

Далі робимо розрахунок та визначимо ймовірність несанкціонованого доступу з нашою двофакторную аутентифікацією.

$$P_{\text{нсд}} = (1 - 0{,}7) \times (1 - 0{,}99) = 0{,}027$$

З розрахунків отримали, що вірогідність отримання несанкціонованого доступу при використанні запропонованого методу $P_{\text{нсд}} = 0{,}27\%$

3.6. Висновок

Метод двофакторної аутентифікаї набирає великих обертів щодо популяції серед сучасних компаній.

Оскільки кожний працівник, якого робота полягає з використанням персонального компьютера має особисти пароль для аутентицікаї, то введення додаткових ресурсів захисту необхідно, що б якось мінімізувати ризики витоку інформації чи проникнення в систему.

Інтеграція системи двофакторної аутентифікії може використовуватись, особливо другим методом не тільки на безкоштовних ресурсах, де мінімальна кількість кастомізації та всіляких додаткових функції розширення функціоналу.

Наша система може лише генерацію кодів, а платні аналоги можуть інтенгровуватись з SMS серверами, можливими функціями відновлення паролю та всесвітня підтримка та встановлення не тільки на телефонах, а вже популярних аксесуарах , як смарт годинники і тд.

Треба зазначити, що парольний метод є первинним, але самим поширеним.

Використання поролю необхідна складова сучасних систем. Але завжди треба вносити обовзякові правила , щодо мінімальної безпеки. Наприклад мінімальна кількість символів, підтримка системи розпізнавання великих літер та маленьких (оскільки деякі системи не розпізнають) та використання додатових символів.

Других фактор аутентифікації у нас використовується Google Authenticator.

Аутентифікатор реалізує алгоритм одноразового пароля на основі часу (TOTP). Він має такі інгредієнти:

- Спільний секрет (послідовність байтів)
- Вхідні дані, отримані з поточного часу

- Функція підписання

Спільний секрет: Спільний секрет - це те, що вам потрібно отримати для налаштування облікового запису на телефоні. Або ви сфотографуєте QR-код за допомогою телефону, або можете ввести секрет вручну.

Вхідні дані (поточний час): значення введеного часу, яке ви просто отримаєте з телефону, не вимагає подальшої взаємодії з сервером після отримання секрету. Однак важливо, щоб час вашого телефону був точним, оскільки сервер по суті повторюватиме те, що відбувається з вашим телефоном, використовуючи поточний час, відомий серверу. Функція підписання: Використана функція підпису - HMAC-SHA1. HMAC розшифровується як код автентифікації повідомлень на основі хешу, і це алгоритм, який використовує безпечну односторонню хеш-функцію (у цьому випадку SHA1) для підписання значення. Використання HMAC дозволяє нам перевірити справжність - лише люди, які знають секрет, можуть генерувати однакові результати для одного входу (поточний час).

```
original_secret = xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

secret = BASE32_DECODE(TO_UPPERCASE(REMOVE_SPACES(original_secret)))

input = CURRENT_UNIX_TIME() / 30  // sets a constant value for 30 seconds

hmac = SHA1(secret + SHA1(secret + input)) //apply hashing

offset = hmac[len(hmac)-1] & 0x0F //Last nibble

four_bytes = hmac[offset : offset+4] //takes a subset of 4 bytes from 20 bytes

large_integer = INT(four_bytes) //Covert four bytes to integer

small_integer = large_integer % 1,000,00 //gives 6 digit code
```

Рис.3.42. Код псевдо коду.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України про інформацію. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (15.10.2020).
2. Закон України про державну таємницю. URL:https://zakon.rada.gov.ua/laws/show/3855-12#Text (01.10.2020).
3. Указ президента України Про Положення про порядок здійснення криптографічного захисту інформації в Україні. URL: https://zakon.rada.gov.ua/laws/show/505/98#Text(05.10.2020).
4. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf (10.10.2020).
5. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. URL:https://tzi.com.ua/downloads/1.1-003-99.pdf (07.10.2020).
6. Информационная технология – Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности. URL: https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf (01.11.2020).
7. Боровиков А.М., Тимошенко А.А. Системы защиты информационного обмена «Клиент – Банк». Безопасность информации. 1995. №1. С. 53–60.
8. Додонов О.Г., Ланде Д.В., Путятин В.Г. Інформаційні потоки в глобальних комп’ютерних мережах. К. : Наукова думка, 2009. 295 с.
9. Малигін В.Р., Козьмовский Д.В. Методи забезпечення безпеки розподілених інформаційних систем, заснованих на аналізі трафіку і контроль мережевої діяльності користувачів. Проблеми управління ризиками в техносфері. 2013. № 2 (26). С. 78-82.
10. Гайкович В., Першин А. Безопасность электронных банковских систем. М. : Единая Евро- па, 1994. 364 с.
11. Компьютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: Навч. посібник / В.К. Задірака, А.М. Кудін, В.О. Людвиченко, О.С. Олексюк./ К.-Тернопіль: Підручники і посібники, 2007. 272 с.
12. Вербіцький О.В. Вступ до криптології. Львів: Вид-во науково-технічної літератури, 1998. 247.
13. Методы аутентификации Панасенко Сергей, 2005. URL: http://www.panasenko.ru/Articles/69/69.html (07.11.2020).

14. Автентифікація. URL: https://uk/wikipedia.org/wiki/Автентифікація (08.11.2020)

15. Даклин Пол. Простые советы по более разумному выбору и использованию паролей. Сетевая газета InfoSecurity.ru. [URL] : http://www.infosecurity.ru/_gazeta/content/060525/article01.shtml (12.11.2020).

16. Office of the Government Chief Information Officer. "Passwords and PINs based Authentication". The Government of the Hong Kong Special Administrative Region of the People's Republic of China. Archived from the original on May 31, 2015. Retrieved 2 November 2015.

17. Office of the Government Chief Information Officer. "Public-Key Authentication". The Government of the Hong Kong Special Administrative Region of the People's Republic of China. Archived from the original on May 31, 2015. Retrieved 3 November 2015

18. Office of the Government Chief Information Officer. "Symmetric-key Authentication". The Government of the Hong Kong Special Administrative Region of the People's Republic of China. Archived from the original on July 9, 2015. Retrieved 3 November 2015.

19. Office of the Government Chief Information Officer. "SMS based Authentication". The Government of the Hong Kong Special Administrative Region of the People's Republic of China. Archived from the original on August 27, 2015. Retrieved 3 November 2015

20. Матвеев И.А., Ганькин К.А. Распознавание человека по радужке. Системы безопасности. 2004. № 5. С. 72-76.

21. Jeffery, L.; Rhodes, G "Insights into the development of face recognition mechanisms revealed by face after effects". British Journal of Psychology. 102 (4) , (2011). : 799–815.

22. Digital Identity Guidelines. [URL] : https://pages.nist.gov/800-63-3/sp800-63b.html (13.11.2020)

23. Cisco Adaptive Security Appliance (ASA) [URL] : https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html (20.11.2020)

24. Cisco Adaptive Security Device Manager (ASDM) [URL] : https://www.cisco.com/c/en/us/products/security/adaptive-security-device-manager/index.html (21.11.2020)

25. Ubuntu 16.04.1 LTS [URL] : http://old-releases.ubuntu.com/releases/16.04.1/ (25.11.2020)

26. Google Authenticator [URL] : https://wiki.archlinux.org/index.php/Google_Authenticator (26.11.2020)
27. Cisco Security Appliance Command Line Configuration Guide, Version 7.2 URL : https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/aaa.html (27.11.2020)
28. Cisco AnyConnect Secure Mobility Client [URL] : https://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/index.html (28.11.2020)
29. Теорема множення ймовірностей незалежних подій [URL] : https://disted.edu.vn.ua/courses/learn/8032 (29.11.2020)

ВИСНОВКИ

На основі аналізу нормативно-правової бази України в галузі інформаційної безпеки, було обрано нормативні документи , що дало можливість проведення аналізу та вибору подальшого удосконалення захисту інформації.

На основі аналізу загроз інформаційної безпеки ,каналів витоку інформації та методів аутентифікації було визначено найбільш актуальні методи логічної багатофакторної аутентифікації.

Було розроблено та налаштовано конфігурація віртуальної системи з використанням обладнанням : , що дало можливість тестування розробленого програмного продукту.

Розроблений програмний продукт для підвищення рівню захищеності інформації від несанкціонованого доступу був проведений на розробленій віртуальній системі. Та був підтверджений на основі розрахунку коефіцієнту можливості проникнення в дану систему.