Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента ***Ткачика Олексія Сергійовича***

академічної групи ***125м-17-2***

спеціальності ***125 Кібербезпека***

спеціалізації

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка рекомендацій щодо захисту інформації в корпоративній мережі на платформі Windows Server 2016 при взаємодії з мобільними пристроями***

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Флоров С.В			
розділів:				
спеціальний	к.т.н., доц. Флоров С.В			
економічний	д.е.н., проф. Вагонова О.Г.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

ЗАТВЕРДЖЕНО:

завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту ***Ткачик О.С.*** **академічної групи** ***125м-17-2***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка рекомендацій щодо захисту інформації в корпоративній мережі на платформі Windows Server 2016 при взаємодії з мобільними пристроями***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від _____ № _____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***інформаційно-комунікаційна система підприємства що взаємодіє з мобільними співробітниками***

Предмет досліджень ***рівень захисту інформації при доступі мобільних співробітників до інформаційних ресурсів підприємства***

Мета ***розробити рекомендації по підвищенню інформаційної безпеки при використанні хмарних технологій в учбових закладах***

Вихідні дані для проведення роботи ***результати та матеріали з виробничої, переддипломної практики та курсовому проекту з комплексних систем захисту інформації.***

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна ***Розроблено рекомендації щодо розгортання служб, засобів і сервісів в гібридному середовищі Windows Server 2016 які закладів що використовують хмарні технології забезпечують безпечний обмін інформацією з мобільними пристроями***

Практична цінність ***Отримані результати можуть бути використані для подальшого та поглибленого вивчення інформаційних систем які мають мобільних користувачів***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати повинні відповідати вимогам Закону України «Про інформацію», Закону України «Про захист персональних даних», Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», «Положення про технічний захист інформації в Україні», що затверджено указом Президента України від 27 вересня 1999 р. №1229/99, НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», «Про вищу освіту», Закону України «Про освіту», Положення про організацію навчального «процесу у вищих навчальних закладах», що затверджено наказом Міністерства освіти України від 2 червня 1993 р. №161, нормативних документів з технічного захисту інформації, державних стандартів України в галузі інформаційної безпеки та інших законів України, що стосуються забезпечення безпеки інформації.

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Огляд джерел за темою та напрям досліджень	03.09.18-06.10.18
Методи досліджень	07.10.18-31.10.18
Результати досліджень	01.11.18-24.11.18
Виконання економічного розділу	25.11.18-04.12.18
Оформлення пояснювальної записки	05.12.18-10.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***від реалізації результатів роботи очікується за рахунок підвищення рівня захищеності інформації в корпоративних мережах при взаємодії з мобільними користувачами***

Соціальний ефект ***від реалізації результатів роботи очікується позитивним завдяки створенню умов для реалізації можливостей співробітників підприємства підвищити продуктивність праці та її комфортність***

7 ДОДАТКОВІ ВИМОГИ

Відповідність оформлення «ДСТУ 3008-95. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення» та «Методичні вказівки. Загальні вимоги до оформлення магістерських дипломних робіт і дипломних проектів спеціалістів для студентів галузей знань 1701 «Інформаційна безпека» та 0509 «Радіотехніка, радіоелектронні апарати та зв'язок»

Завдання видано _____ Флоров С.В
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ Ткачик О.С.
(підпис студента)

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., __ табл., 4 додатка, _ джерела.

Об'єкт дослідження: Корпоративна комп'ютерна мережа третього класу на платформі Windows Server 2016**.**

Мета дипломної роботи: розробити рекомендації по процедурі розгортання служб та сервісів в середовищі Windows Server 2016 що забезпечують безпечний обмін інформацією із мобільними користувачами.

У спеціальній частині досліджено властивості сучасних систем управління мобільними пристроями в корпоративній мережі. Визначено загрози при підключенні до інтрамережі мобільних користувачів та визначити. Визначено служби, засоби методи та сервіси в середовищі Windows Server 2016, які забезпечують безпечний обмін інформацією між мобільними користувачами і корпоративною мережею. Розроблено рекомендації щодо плану впровадження хмарного сервісу Microsoft Intune в корпоративній мережі.

Наукова новизна полягає в розробці рекомендації щодо розгортання і налаштування служб та сервісів в гібридному середовищі Windows Server 2016, які забезпечують безпечний обмін інформацією з мобільними співробітниками.

В економічному розділі виконаний розрахунок економічної ефективності створення обґрунтованих рекомендацій захисту інформації.

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ЛОКАЛЬНА ОБЧИСЛЮВАЛЬНА МЕРЕЖА, MS WINDOWS SERVER 2016, ПОЛІТИКА БЕЗПЕКИ, МОБІЛЬНИЙ КОРИСТУВАЧ, МОБІЛЬНІ ПРИСТРОЇ, MDM, MAM, INTUNE

РЕФЕРАТ

Пояснительная записка: __ с., __ рис., __ табл., 4 приложения, источников.

Объект исследования: корпоративна компьютерная сеть третьего класса на платформе Windows Server 2016.

Цель дипломной работы: разработать рекомендации по процедуре развертывания служб и сервисов в среде Windows Server 2016 обеспечивающие безопасный обмен информацией с мобильными пользователями.

В специальной части исследованы свойства современных систем управления мобильными устройствами в корпоративной сети. Определены угрозы при подключении к интрасети мобильных пользователей. Определены службы, средства методы и сервисы в среде Windows Server 2016, которые обеспечивают безопасный обмен информацией между мобильными пользователями и корпоративной сетью. Разработаны рекомендации по плану внедрения хмарного сервиса Microsoft Intune в корпоративной сети.

В экономическом разделе выполнен расчет экономической эффективности создания обоснованных рекомендаций защиты информации.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ, MS WINDOWS SERVER 2016, ПОЛИТИКА БЕЗОПАСНОСТИ, МОБИЛЬНЫЕ УСТРОЙСТВА, MDM, MAM, INTUNE

THE ABSTRACT

Explanatory note: __ p., __ fig., table __., 4 applications, 45 of the sources.

The object of study: third-class corporate computer network on the platform of Windows Server 2016.

The aim of the thesis: to develop recommendations on the procedure for the deployment of services and services in the Windows Server 2016 environment to ensure the secure exchange of information with mobile users.

In a special section the properties of modern mobile device management systems in the corporate network are investigated. Threats identified when mobile users connect to the intranet.

Services, tools, and services in the Windows Server 2016 environment are defined that provide for the secure exchange of information between mobile users and the corporate network.

Developed recommendations for the plan to introduce Microsoft Intune hmarny service in the corporate network.

In the economic section, the calculation of the economic effectiveness of creating sound information security recommendations has been made

INFORMATION PROTECTION SYSTEM, LOCAL COMPUTING NETWORK, MS WINDOWS SERVER 2016, SECURITY POLICY, MOBILE DEVICES, MDM, MAM, INTUNE

СПИСОК УМОВНИХ СКОРОЧЕНЬ

КС – комп'ютерна система

ЛОМ – локальна обчислювальна мережа

МК – мобільні користувачі

МП – мобільні пристрої

НД ТЗІ – нормативний документ технічного захисту інформації

ОС – операційна система

ПБ – політика безпеки

ПК – персональний комп'ютер

ПЗ – програмне забезпечення

ПЕОМ – персональна електронно-обчислювальна машина

РС – робоча станція

AVAPI – Antivirus Application Programming Interface

CA – Certificate Authority

PKI – Public Key Infrastructure

SMS – System Management Server

SP – Service Pack

SUS –Software Update Services

TLS – Transport Layer Security

UPN – User Principal Name

MDM – Mobile Device Management

MAM – Mobile Application Management

AD – Active Directory

AzureAD – Azure Active Directory

ЗМІСТ

ВСТУП

З розвитком сучасних засобів мобільного зв'язку і збільшенням зони покриття операторами, мобільні пристрої і мобільні користувачі стають невід'ємною частиною корпоративних інтрамережі. Організації зіштовхуються із зростаючою загрозою порушення режиму безпеки, що виходить від цілого ряду джерел. Інформаційним системам і мережам можуть загрожувати такі небезпеки, як комп'ютерне шахрайство, шпигунство, саботаж, вандалізм, а також інші джерела відмовлень і аварій.

З'являються нові загрози, здатні завдати шкоди організації, такі як широко відомі комп'ютерні віруси чи хакери. Передбачається що такі загрози інформаційної безпеки згодом стануть більш розповсюдженими, небезпечними і витонченими. У той саме час через зростаючу залежність організацій від інформаційних систем і сервісів вони можуть стати більш уразливими стосовно загроз порушення захисту.

Поширення обчислювальних мереж надає нові можливості для несанкціонованого доступу до комп'ютерних систем, а тенденція до переходу на розподілені обчислювальні системи зменшує можливості централізованого контролю інформаційних систем фахівцями.

Захисні міри виявляються значно більш дешевими й ефективними, якщо вони вбудовані в інформаційні системи і сервіси на стадіях завдання вимог і проектування.

Чим швидше організація вжив заходів по захисту своїх інформаційних систем, тим більш дешевими й ефективними вони будуть для неї згодом.

Інтермережа сучасного підприємства виконує безліч функцій, пов’язаних із забезпеченням бізнес-процесів. Забезпечення безпечної, безперебійної і ефективної роботи мережі є однією з найважливіших задач що ставиться перед співробітниками. Одним з найважливіших засобів що

допомагають вирішити всі ці задачі є політика безпеки віддаленого доступу до ресурсів інтрамережі.

Мета дипломної роботи: на підставі аналізу можливостей Windows 2016 і протоколів, що використовуються в об'єкті дослідження, розробити рекомендації з вибору методу аутентифікації зовнішніх користувачів та процедуру розгортання служб та засобів Windows Server 2016 забезпечують безпечний обмін інформацією.

РОЗДІЛ 1. ІНФРАСТРУКТУРА КОРПОРАТИВНОЇ МЕРЕЖІ НА ПЛАТФОРМІ WINDOWS SERVER 2016

Забезпечення безпеки інформаційного простору в організації − є однією з умов успішної і прибуткової праці. Політика інформаційної безпеки необхідна основа для створення безпечного інформаційного простору в організації.

Політика інформаційної безпеки − набір законів, правил, практичних рекомендацій і розпорядницьких документів, що визначають управлінські і проектні рішення в області захисту інформації.

На основі політики безпеки будується керування, захист і розподіл критичної інформації в системі. Вона повинна охоплювати усі особливості процесу обробки інформації, визначаючи поводження інформаційної мережі в різних ситуаціях. Для кожної конкретної інформаційної системи політика безпеки повинна бути індивідуальною. Вона залежить від технології і способів обробки інформації, використовуваних програмних і технічних засобів, архітектури інформаційної мережі, структури організації і виду її діяльності, а також інших факторів визначаючих функціонуючу ІС організації.

Метою розробки політики організації в області інформаційної безпеки є визначення вірного (з погляду організації) способу використання інформаційних ресурсів, а також розробка процедур, що запобігають чи реагують на порушення режиму безпеки. Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих ресурсів.

При розробці і проведенні її в життя доцільно керуватися наступними засобами:

Неможливість минати захисні прилади: всі інформаційні потоки

в мережу що захищається і в систему, і із неї, повинні проходити через визначені захисні засоби. Не повинно бути "таємних входів і виходів" в обхід захисних прилади.

Посилення самої слабкої ланки: надійність будь-якого захисту визначається захистом самої слабкої ланки. Часто самою слабкою ланкою виявляється не комп'ютер чи програма, а людина, і тоді проблема забезпечення інформаційної безпеки здобуває нетехнічний характер.

Неприпустимість переходу у відкритий стан: Принцип неприпустимості переходу у відкритий стан означає, що при будь-яких обставинах (у тому числі позаштатних), ЗЗІ або цілком виконують свої функції, або повинні цілком блокувати доступ.

Мінімізація привілеїв: принцип мінімізації привілеїв наказує виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків.

Розподіл обов'язків: принцип поділу обов'язків припускає такий розподіл ролей і відповідальносте , при якому одна людина не може порушити критично важливий процес для організації. Це особливо важливо, коли треба запобігти зловмисним чи некваліфікованим діям системного адміністратора.

Багаторівневий захист: принцип багаторівневого захисту наказує не покладатися на один захисний рубіж яким би надійним він не здавався. Після засобів фізичного захисту повинні випливати програмно-технічні засоби, за ідентифікацією й аутентифікацією − керування доступом, і як останній рубіж − протоколювання і аудит. Наявність такого багаторівневого захисту здатне не тільки затримати зловмисника, але й істотно завадити непомітному виконанню злочинних дій.

Розмаїтість захисних засобів: принцип розмаїтості захисних засобів рекомендує організовувати різні за своїм характером оборонні

трубежі, щоб від потенційного зловмисника було потрібно оволодіння різноманітними і, по можливості, несумісними між собою навичками подолання ЗЗІ.

Простота і керованість інформаційної системи: принцип простоти і керованості інформаційної системи в цілому визначає можливість формального чи неформально доказу коректності реалізації механізмів захисту. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.

Забезпечення загальної підтримки мір безпеки: принцип загальної підтримки мір безпеки − носить нетехнічний характер. Рекомендується із самого початку передбачити комплекс мір, спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне і, головне, практичне.

1.1 Ролі та служби Windows Server 2016 для мобільних користувачів

Як Через те, що робочі ресурси в організації стають все більш і більш мобільними, в Windows Server 2016 були внесені значні поліпшення в засоби мобільності. Нові технології дозволяють користувачам ноутбуків більш гладко працювати при переміщенні між офісом, будинком і точками бездротового доступу в Інтернет, а також постійно підтримувати зв'язок з мережевими ресурсами. Для того щоб користуватися цими поліпшення і отримувати доступ до нових технологій, мобільні користувачі повинні обов'язково встановити на своїх ноутбуках клієнтську операційну систему не нижче Windows 7. Після цього доступ до мережевих ресурсів істотно спрощується, де б користувачі не знаходились

Технологія DirectAccess в Windows Server 2016.

Одним з найбільш значних поліпшень, що стосуються віддаленого доступу в Windows Server 2016, є додавання технології DirectAccess. Ця технологія надає віддаленому користувачеві можливість отримувати доступ до мережевих ресурсів, таким як загальні файлові ресурси, загальні ресурси SharePoint і тип., без підключення до віртуальної приватної мережі (VPN).

Це чудова технологія, яка для забезпечення віддаленого доступу до мережі об'єднує в собі складну технологію захисту і технологію отримання доступу на основі політик. Однак швидко розібратися з усіма компонентами, необхідними для приведення DirectAccess в дію, поки нелегко. Хоча багато організацій і будуть прагнути розгорнути DirectAccess, додавання всіх технологій, необхідних для впровадження DirectAccess в середовищі без особливих зусиль, може зайняти від декількох місяців до декількох років.

Нижче перераховані технології, які обов'язково потрібні для приведення Direct Access в дію.

Сертифікати PKI.

У DirectAccess сертифікати PKI застосовуються в якості методу ідентифікації віддаленого пристрою, а також як основа для установки шифрованих з'єднань між віддаленим пристроєм і мережею.

Отже, організації повинні розгортати у своїх середовищах відповідну інфраструктуру сертифікатів. Клієнти Windows 7. Технологія DirectAccess працює тільки з клієнтами, що функціонують під управлінням Windows 7. Саме Windows 7 змушує клієнтські компоненти для шифрування, інкапсуляції і управління політиками працювати разом з IPSec. Компонент, який застосовується в DirectAccess для керування політиками, передбачає використання протоколу IPSec для визначення цільових ресурсів, до яких у віддаленого користувача повинен бути доступ. Протокол IPSec може підтримуватися як від однієї кінцевої точки до іншої (тобто, починаючи від клієнтської системи і до

самого сервера додатків), так і (спрощений варіант) лише від клієнтської системи до проксі-сервера DirectAccess, у другому випадку підтримка IPSec на самих кінцевих серверах додатків стає необов'язковою. У будь-якому випадку IPSec є частиною структури забезпечення безпеки та застосування політик, яка гарантує можливість отримання клієнтської системою доступу лише до тих ресурсів сервера, до яких у неї згідно політиці повинен бути доступ в ході сеансу підключення DirectAccess.

Про IPv6. І, нарешті, в DirectAccess передбачено використання протоколу IPv6 в якості ідентифікатора IP-сеансів. Незважаючи на те що більшість організацій поки не перейшло на застосування IPv6, і в більшості методів доступу до Інтернету, як і раніше використовується IPv4, в Windows 7 і Windows Server 2016повністю підтримується тунелювання IPv6, тому воно може застосовуватися в якості проміжного варіанту доти , поки IPv6 не стане прийнятим стандартом повсюдно. На поточний момент IPv6 є обов'язковим у DirectAccess і використовується у вигляді частини рішення для забезпечення віддаленого доступу.

Технологія Mobile Broadband в Windows 10.

Ще однією технологією що належить Windows 10 для мобільних користувачів є Mobile Broadband. Підтримка пристроїв мобільного широкосмугового зв'язку. Ця технологія ніякого зв'язку з Windows Server 2016 не має. Вона являє собою пропоновану в ще в Windows 7 оновлену технологію для пристроїв і служб, які використовуються в роботі мобільних широкосмугових мереж (подібних AT & T, Sprint і Verizon).

У Windows 10 за умови встановлення новітніх драйверів Mobile Brand як для пристроїв, так і для Windows, вставка карт Mobile Broadband в мобільну систему автоматично призводить до підключенню користувача до Інтернету. Точно так само як при включенні користувачем в системі адаптер Wi-Fi відбувається автоматична установка з'єднання з Wi-Fi-точкою доступу, при підключенні адаптера

Mobile Broadband тепер автоматично проводиться підключення користувача до Інтернету. При відключенні адаптера Mobile Broadband від системи Windows 10 сеанс Mobile Broadband переривається і при наявності доступного бездротового підключення Wi-Fi або проводового підключення Ethernet автоматично встановлюється з'єднання з альтернативною точкою доступу. У поєднанні з VPN Reconnect або DirectAccess технологія Mobile Broadband дозволяє мобільному користувачеві легко отримувати доступ до мережі організації.

Підтримка філій.

До складу Windows Server 2016 входять значно поліпшені технології для більш якісного IT- обслуговування віддалених офісів або філій організацій. Зазвичай віддалені офіси або філії мають обмежену IT-підтримку або, принаймні, потребують тих же функціональних можливостей і ступені надійності, якими володіє головний офіс, але не передбачають виділення бюджету на резервне обладнання та пристрої для забезпечення повної операційної підтримки. З новими ресурсами Windows Server 2016 для дочірніх офісів віддалені філії тепер можуть мати високу ступінь безпеки, високу продуктивність, доступ до даних без значних затримок і робочі можливості навіть у разі їх відключення від мережі через проблеми зв'язку з Інтернетом або регіональної мережею (WAN).

До числа нових і поліпшених засобів і технологій для цієї мети в Windows Server 2016відносяться системи RODC (Read-Only Domain Controller - контролер домену тільки для читання), технологія BitLocker, Drive Encryption (Шифрування дисків з допомогою Bitlocker), служба Distributed File System Replication (Реплікація розподіленої файлової системи) і технологія розподіленого адміністрування.

Використання технології BitLocker для захисту сервера. Технологія BitLocker, що вперше з'явилася в Windows Vista, надає організує цілям можливість виконувати шифрування цілих розділів

дисків з усіма що зберігаються на них файлами, документами і даними. Коли вона була вперше запропонована в Windows * Server 2008 у вигляді інструменту для сервера, було важко зрозуміти, навіщо може вимагатися шифрування дискового тому на сервері. Шифрувати вміст ноутбука подібним методом мало сенс на випадок його крадіжки (щоб ніхто зміг отримати доступ до зберігаються на його жорсткому диску даними).

Однак якщо подумати про тих серверах, які розміщуються у віддалених місцях і часто не в заблокованій серверної стойці в закритій ком комп'ютерні кімнаті, а скоріше в якомусь кабінеті чи навіть під касовим апаратом у разі магазинів, де сервери виступають в ролі системи розрахункових терміналів то стає зрозуміло, що серверів з чутливими даними в виробничих середах більшість. Технологія BitLocker дозволяє шифрувати все тому сервера Windows Server 2016і є просто чудовим компонентом для організацій, що турбуються про можливу фізичну крадіжку даних з сервера

Розподілене адміністрування.

У віддалених або дочірніх офісах, в яких присутні IT-персонал, раніше завжди було важко призначати відповідні права на виконання пов'язаних з адмініструванням та управлінням завдань. IT-співробітникам у віддалених офісах або надавалися права адміністраторів всього домену, в той час як їм потрібні були права, що стосуються тільки їх конкретного сайту, або не видавалися взагалі ніякі адміністративні права через те, що призначити їм більш вузьку роль було надто важко.

Тепер в Windows Server 2016 Active Directory поставляється набір прав, який спеціально призначений для адміністраторів віддалених сайтів і дочірніх офісів. Багато в чому подібно адміністраторам сайтів у старій версії Exchange Server 5.5, де адміністраторам дозволялося додавати користувачів і контакти і вирішувати адміністративні завдання

на локальних серверах Exchange, мережевим адміністраторам в Active Directory тепер можна видавати права в залежності від ролі обслуговується ними дочірнього або віддаленого сайту. Це дає можливість вносити зміни, що стосуються тільки конкретного дочірнього офісу. Дана можливість, разом з усіма іншими засобами в Windows Server 2016, призначеними для дочірніх і віддалених офісів, забезпечує більш якісне IT-обслуговування в організаціях з безліччю офісів.

Роль Remote Desktop Services для тонких клієнтів. У Windows Server 2016в компонент Terminal Services (Термінальні служби), тепер званий Remote Desktop Services (Служби віддалених робочих столів) або, скорочено, RDS, були внесені значні поліпшення в механізм доступу тонких клієнтів, застосовуваних віддаленими і керованими користувачами підприємства. Якщо раніше в Windows Server 2000/2003 для приведення базової конфігурації Terminal Services в робочий стан потрібно встановлювати додаткові сторонні додатки, то в складу Windows Server 2008 входять всі необхідні технології, які були поліпшена в Windows Server 2016. До цих технологій належить, наприклад, можливість доступу до Remote Desktop Services через стандартний порт 443 з SSL, а не спеціальний порт 3389, або можливість публікації лише конкретних програм, а не всього робочого стола. Крім того, до їх складу входять також поліпшення, такі як дозвіл клієнту використовувати при віддаленому доступі великий екран або кілька екранів, або спрощена процедура друку на віддалених принтерах.

Всі ці поліпшення в компоненті Remote Desktop Services роблять його одним із найлегших у плані додавання в існуючу середу Windows 2003 Active Directory для тестування нових можливостей Windows Server 2016, особливо тому, що установка системи Windows 2016 Remote Desktop Services зводиться просто до додавання в домен ще одного рядового сервера, який потім може бути вилучений.

Роль Remote Desktop Services Web Access.

Ще одним поліпшенням, яке вперше з'явилося в Windows Server 2008 і було розширено в Windows Server 2016 Remote Desktop Services, стало додавання нової ролі, яка спочатку називалася Terminal Services Web Access (Веб-доступ до служб терміналів), а тепер називається так: Remote Desktop Services Web Access (Веб-доступ до віддалених робочих столів). Ця роль дозволяє віддаленому клієнту отримувати доступ до сеансу Remote Desktop Services не за рахунок запуску клієнта RDP 6.x, а за рахунок підключення до веб сторінці, на якій користувачеві потім надається можливість увійти в систему і почати сеанс роботи. Це спрощує спосіб отримання доступу користувачами, оскільки дозволяє їм просто додати URL-адресу відповідної веб-сторінки в обрані посилання браузера.

Для підключення до сеансу Remote Desktop Services з використанням ролі Remote Desktop Services Web Access як і раніше потрібно, щоб клієнтська система функціонувала під управлінням, Windows 7, Windows 8, Windows 10, Windows Server 2012R2. Починаючи з Windows Server 2016 отримати доступ до Remote Desktop Services Web Access з браузера в системах Apple Macintosh і Linux стало можливо. Для веб-клієнтів, що функціонують під керуванням ОС, відмінних від Windows, повинні використовуватися спеціальні з'єднувачі від сторонніх виробників, таких як Citrix Systems.

Роль Desktop Services Gateway. Роль Remote Desktop Services Gateway (Шлюз віддалених робочих столів) була оновлена в Windows Server 2012R2 Remote Desktop Services, і тепер вона дозволяє підключатися до сеансу Remote Desktop Services через стандартний порт 443 з SSL-шифруванням (Port 443 SSL). Раніше користувачі могли підключатися до Windows Remote Desktop Services тільки через спеціальний порт 3389. На жаль, у багатьох організаціях з міркувань безпеки з'єднання, що встановлюються через нестандартні порти, часто

блокуються, тому в разі використання Інтернет-з'єднання в готелі, аеропорту, Інтернет-кафе і інших місцях, де нестандартні порти блокувалися, користувачі отримувати доступ до Terminal Services не могли. Тепер, завдяки Remote Desktop Services Gateway, віддалені користувачі можуть підключатися до Remote Desktop Services Terminal Services через порт 443 точно таким же чином, як і при прогляданні безпечних веб-сторінок. Через застосування при доступі до веб-сторінок SSL-шифрування (за допомогою https: / /), Підключення до Windows Server 2016 Remote Desktopl Services тепер може проводитися з будь-якого місця.

Роль Remote Desktop Services RemoteApps. Ще однієї серверної роллю, яка вперше з'явилася в Windows Server 2008 і була оновлена в Windows Server 2016, є Remote Desktop Services RemoteApps (Дистанційні програми служб віддалених робочих столів). Ця роль дозволяє адміністраторам "публікувати" для користувача доступу тільки якісь конкретні програми. Цими додатками можуть бути Microsoft Outlook, Microsoft Word, програма ведення обліку відпрацьованого співробітниками компанії часу або програма управління відносинами з клієнтами (Customer relationship management - CRM). То замість щоб надавати користувачам повний доступ до всього робочого столу разом з кнопкою Start (Пуск) і всіма додатками, в організаціях тепер може публікуватися лише кілька додатків, до яких дозволений доступ.

Застосовуючи разом з Remote Desktop Services RemoteApp групові політики та роль Network Policy Server (Сервер мережевих політик), мережеві адміністратори можуть публіко вать для різних користувачів різні набори програм, тобто, наприклад, предоставлятг одним користувачам доступ тільки до додатків Outlook і Word, а іншим - до додатку Outlook, Word і CRM. Завдяки додаванню в компонент політик можливості визначати місцезнаходження в мережі (новий засіб Windows Server 2016), додатки можуть робитися доступними в залежності від

того, звідки користувач підключається з локальної мережі або з віддаленого місця.

Крім обмеження користувачів тільки програмами, до яких у них повинен бути доступ згідно встановленої політиці, Remote Desktop Services RemoteApp також дозволяє зводити до мінімуму пов'язані з підключенням користувачів накладні витрати, оскільки передбачає запуск для кожного користувача не всього робочого стола, а тільки набору конкретних додатків.

Роль Remote Desktop Services Connection Broker. Новою роллю, яка була додана вже в Windows Server 2016, є Virtual Desktop Infrastructure (Інфраструктура віртуальних робочих столів) або, скорочено, VDI. На відміну від ролі Remote Desktop Services, яка забезпечує відносини типу "один до багатьох", маючи на увазі поділ єдиного примірника сервера між безліччю користувачів, VDI забезпечує між сервером і віддаленим клієнтом відношення типу "один до одного" за рахунок застосування віртуального гостьового сеансу. Коли користувач клієнта VDI запускає гостьовий сеанс, що виділяється гостьовий сеанс робиться доступним для нього із завантаженням окремої клієнтської оболонки, виділенням окремого пулу пам'яті і повною ізоляцією від всіх інших гостьових сеансів на хост-сервері. Windows Server 2016 VDI підтримує два різних режими: режим особистого робочого столу (Personalized Desktop) і режим пулу робочих столів (Pooled Desktop). Перший являє собою виділяється гостьовій сеанс, до якого користувачі отримують доступ при кожному підключенні до сервера VDI і в якому, використовуваний гостем образ виглядає щоразу однаково. Другий режим - це гостьовий сеанс, при якому параметри користувача (вибрані посилання, фон і конфігураційні установки додатків) зберігаються і при вході завантажуються знову в стандартний шаблон. Виділені для таких гостьових сеансів ресурси є не постійними, а виділяються і призначаються під час входу. Роль Remote

Desktop Services Connection Broker (Посередник підключень до віддаленого робочого столу) раніше називалася Terminal Services Session Broker (Посередник сеансів служб терміналів). Ця роль дозволяє створювати систему керування сеансами Remote Desktop, що гарантує наявність у користувачів в разі їх відключення від сервера Remote Desktop можливості відновлювати підключення зі своїми сеансами без втрати даних про той стан, в якому все знаходилося на момент відключення. Без такої системи спроби знову підключитися до Remote Desktop Services після переривання сеансу можуть закінчитися з'єднанням з іншим сервером Remote Desktop і необхідністю повернення до місця останнього збереження даних з повторенням всіх дій, виконаних до переривання сеансу.

Крім зміни назви ролі з Session Broker на Connection Broker, нової в Windows Server 2016 Connection Broker є ще й можливість кластеризації цієї ролі. Раніше дана роль представляла собою одиничний екземпляр сервера. У разі переривання сеансу зв'язку з цими примірником сервера, дані про стан підключень не зберігалися, і компонент Session Broker не міг виконувати свою роботу. За рахунок кластеризації ролі Connection Broker організація може забезпечити надмірність і, отже, розгорнути кілька серверів Remote Desktop і надати користувачам можливість підключатися до сеансів після їх тимчасового переривання.

Роль Virtual Desktop infrastructure (VDI). Зовсім новою роллю, яка була додана в Windows Server 2016, і получида розвіток у Windows Server 2016 є Virtual Desktop Infrastructure (Інфраструктура віртуальних робочих столів) або, скорочено, VDI. На відміну від ролі Remote Desktop Services, яка забезпечує відносини типу "один до багатьох", маючи на увазі поділ єдиного екземпляра сервера між безліччю користувачів, VDI забезпечує між сервером і віддаленим клієнтом відношення типу "один до одного" за рахунок застосування віртуального гостьового сеансу.

Коли користувач клієнта VDI запускає гостьовий сеанс, що виділяється гостьовий сеанс робиться доступним для нього із завантаженням окремої клієнтської оболонки, виділенням окремого пулу пам'яті і повної ізоляцією від всіх інших гостьових сеансів на хост-сервері.

Windows Server 2016 VDI підтримує два різних режими: режим особистого робочого столу (Personalized Desktop) і режим пулу робочих столів (Pooled Desktop). Перший являє собою виділяється гостьовій сеанс, до якого користувачі отримують доступ при кожному підключенні до сервера VDI і в якому, по суті, використовуваний гостем образ виглядає щоразу однаково. Другий режим - це гостьовий сеанс, при якому параметри користувача (вибрані посилання, фон і конфігураційні установки додатків) зберігаються і при вході завантажуються знову в стандартний шаблон. Виділені для таких гостьових сеансів ресурси є не постійними, а виділяються і призначаються під час входу.

1.2 Проблеми аутенфікації для мобільних користувачів

В системі аутентифікації зазвичай можна виділити кілька елементів:

- суб'єкт, який буде проходити процедуру аутентифікації;
- характеристика суб'єкта - відмінна риса;
- господар системи аутентифікації, що несе відповідальність
- і контролює її роботу;
- сам механізм аутентифікації, тобто принцип роботи системи;
- механізм, який надає або позбавляє суб'єкта певних прав доступу;

1.2.1 Фактори аутентифікації

Ще до появи комп'ютерів використовувалися різні відмінні риси суб'єкта, його характеристики. Зараз використання тієї чи іншої характеристики в системі залежить від необхідної надійності, захищеності та вартості впровадження. Виділяють 3 фактора аутентифікації:

1. щось, що ми знаємо - пароль. Це секретна інформація, якою повинен володіти тільки авторизований суб'єкт. Паролем може бути мовне слово, текстове слово, комбінація для замка або персональний ідентифікаційний номер (PIN). Парольний механізм може бути досить легко реалізований і має низьку вартість. Але має суттєві мінуси: зберегти пароль в секреті часто буває проблематично, зловмисники постійно придумують нові методи крадіжки, злому і підбору пароля (див. бандитський крипто аналіз). це робить парольний механізм слабозахищенним. Те, що ми знаємо - пароль. Це секретна інформація, якою повинен володіти тільки авторизований суб'єкт. Паролем може бути мовне слово, текстове слово, комбінація для замка або персональний ідентифікаційний номер.
2. щось, що ми маємо - пристрій аутентифікації. Тут важливий факт володіння суб'єктом якимось унікальним предметом. Це може бути особиста печатка, ключ від замка, для комп'ютера це файл даних, що містять характеристику. Характеристика часто вбудовується в спеціальний пристрій аутентифікації, наприклад, пластикова картка, смарт-карта. Для зловмисника дістати такий пристрій стає більш проблематично, ніж зламати пароль, а суб'єкт може відразу ж повідомити в разі крадіжки пристрою. Це

робить даний метод більш захищеним, ніж парольний механізм, однак, вартість такої системи вища.

3. щось, що є частиною нас - біометрика. Характеристикою є фізична особливість суб'єкта. Це може бути портрет, відбиток пальця або долоні, голос чи особливість очі. З точки зору суб'єкта, даний метод є найбільш простим: не треба ні запам'ятовувати пароль, ні переносити з собою пристрій аутентифікації. Однак, біометрична система повинна володіти високою чутливістю, щоб підтверджувати авторизованого користувача, але відкидати зловмисника зі схожими біометричними параметрами. Також вартість такої системи досить велика. Але незважаючи на свої мінуси, біометрика залишається досить перспективним фактором.

1.2.2 Засоби аутентифікації

Аутентифікація по багаторазовим паролів. Один із способів аутентифікації в комп'ютерній системі полягає у введенні вашого користувацького ідентифікатора, в просторіччі званого «логіном» (англ. login — реєстраційне ім'я користувача) і пароля - якоїсь конфіденційної інформації. Достовірна (еталонна) пара логін-пароль зберігається в спеціальній базі даних. Проста аутентифікація має такий загальний алгоритм:

- суб'єкт запитує доступ до системи і вводить особистий ідентифікатор та пароль;
- ведені унікальні дані надходять на сервер аутентифікації, де порівнюються з еталонними;
- при збігу даних з еталонними, аутентифікація визнається успішною, при відмінності - суб'єкт переміщується до 1-го кроку;

Введений суб'єктом пароль може передаватися в мережі двома способами:

- незашифрованому, у відкритому вигляді, на основі протоколу парольного аутентифікації (Password Authentication Protocol, PAP);
- з використанням шифрування або односпрямованих хеш-функцій;

В цьому випадку унікальні дані, введені суб'єктом передаються по мережі захищено. З точки зору максимальної захищеності, при зберіганні і передачі паролів слід використовувати односпрямовані функції. Зазвичай для цих цілей використовуються криптографічна стійкі хеш-функції. У цьому випадку на сервері зберігається тільки образ пароля. Отримавши пароль та виконавши його хеш-перетворення, система порівнює отриманий результат з еталонним чином, що зберігаються в ній. При їх ідентичності, паролі збігаються. Для зловмисника, який отримав доступ до образу, обчислити сам пароль практично неможливо. Використання багаторазових паролів має ряд істотних мінусів. По-перше, сам еталонний пароль або його хешированних образ зберігаються на сервері аутентифікації. Найчастіше зберігання пароля проводиться без криптографічних перетворень, в системних файлах. Отримавши доступ до них, зловмисник легко добереться до конфіденційної інформації. По-друге, суб'єкт змушений запам'ятовувати (або записувати) свій багаторазовий пароль. Зловмисник може отримати його, просто застосувавши навички соціальної інженерії, без всяких технічних засобів. Крім того, сильно знижується захищеність системи у випадку, коли суб'єкт сам вибирає собі пароль. Найчастіше це виявляється якесь слово чи комбінація слів, присутні в словнику. При достатній кількості часу зловмисник може зламати пароль простим перебором. Вирішенням цієї проблеми є

використання випадкових паролів або обмеженість за часом дії пароля суб'єкта, після закінчення якого пароль необхідно поміняти.

На комп'ютерах з ОС сімейства UNIX, базою є файл / etc / master.passwd (в дистрибутивах Linux зазвичай файл / etc / shadow, доступний для читання лише root), в якому паролі користувачів зберігаються у вигляді хеш-функцій від відкритих паролів, крім цього в цьому ж файлі зберігається інформація про права користувача. Спочатку в Unix-системах пароль (в зашифрованому вигляді) зберігався у файлі / etc / passwod, доступному для читання всім користувачам, що було небезпечно. На комп'ютерах з операційною системою Windows NT/2000/XP/2003/2008 (не входять в домен Windows) така база даних називається SAM (Security Account Manager - Диспетчер захисту облікових записів). База SAM зберігає облікові записи користувачів, що включають в себе всі дані, необхідні системі захисту для функціонування. Знаходиться в директорії % windir% \ system32\config\.

В доменах Windows Server 2000/2003/2008 такою базою є Active Directory.Прі необхідності забезпечення роботи співробітників на різних комп'ютерах (з підтримкою системи безпеки) використовують апаратно-програмні системи, що дозволяють зберігати аутентифікаційні дані і криптографічні ключі на сервері організації. Користувачі вільно можуть працювати на будь-якому комп'ютері (робочої станції), маючи доступ до своїх аутентифікаційні даними і криптографічним ключам.

1.2.3 Аутентифікація за одноразовими паролями

Отримавши одного разу багаторазовий пароль суб'єкта, зловмисник має постійний доступ до зламаної конфіденційної інформації. Ця проблема вирішується застосуванням одноразових паролів (OTP - One Time Password). Суть цього методу - пароль дійсний тільки для одного входу в систему, при кожному наступному запиті

доступу - потрібен новий пароль. Реалізовано механізм аутентифікації по одноразовим паролів може бути як апаратно, так і програмно.

Технології використання одноразових паролів можна розділити на:

- використання генератора псевдовипадкових чисел, єдиного для суб'єкта і системи.
- використання тимчасових міток разом з системою єдиного часу;
- використання бази випадкових паролів, єдиного для суб'єкта і для системи;

У першому методі використовується генератор псевдовипадкових чисел з однаковим значенням для суб'єкта і для системи. Згенерований суб'єктом пароль може передаватися системі при послідовному використанні односторонньої функції або при кожному новому запиті, грунтуючись на унікальної інформації з попереднього запиту.

У другому методі використовуються тимчасові мітки. Як приклад такої технології можна привести SecurID. Вона заснована на використанні апаратні ключів і синхронізації за часом. Аутентифікація заснована на генерації випадкових чисел через певні тимчасові інтервали. Унікальний секретний ключ зберігається тільки в базі системи і в апаратній пристрої суб'єкта. Коли суб'єкт запитує доступ до системи, йому пропонується ввести PIN-код, а також випадково генерується число, відображуваного в цей момент на апаратній пристрої. Система порівнює введений PIN-код і секретний ключ суб'єкта зі своєї бази і генерує випадкове число, грунтуючись на параметрах секретного ключа з бази і поточного часу. Далі перевіряється ідентичність згенерованого числа і числа, введеного суб'єктом.

Третій метод заснований на єдиній базі паролів для суб'єкта і системи та високоточної синхронізації між ними. При цьому кожен

пароль з набору може бути використаний тільки один раз. Завдяки цьому, навіть якщо зловмисник перехопить використовуваний суб'єктом пароль, то він вже буде недійсний. По порівнянні з використанням багаторазових паролів, одноразові паролі надають більш високу ступінь захисту.

1.2.4 Багатофакторна аутентифікація

Windows Server 2016 застосовується так звану розширену або багатофакторна аутентифікація. Вона побудована на спільному використанні декількох факторів аутентифікації. Це значно підвищує захищеність системи. Як приклад можна привести використання SIM-карт в мобільних телефонах. Суб'єкт вставляє апаратно свою карту (пристрій аутентифікації) в телефон і при включенні вводить свій PIN-код(пароль). Також, наприклад в деяких сучасних ноутбуках присутній сканер відбитка пальця. Таким чином, при вході в систему суб'єкт повинен пройти цю процедуру (біометрика), а потім ввести пароль.

Вибираючи для системи той чи інший фактор або спосіб аутентифікації необхідно перш за все відштовхуватися від необхідного ступеня захищеності, вартості побудови системи, забезпечення мобільності суб'єкта.

1.3 Огляд протоколів аутентифікації для мобільних користувачів

З точки зору інформаційної безпеки будь-якої, віддалений користувач повинен бути аутентифікований, перш ніж зможе отримати доступ до ресурсів.

Аутентифікація відбувається безпосередньо при спробі клієнта встановити з'єднання з сервером віддаленого доступу. Кожен користувач, який підключається віддалено до корпоративної мережі, повинен мати на сервері або в каталозі Active Directory відповідну

обліковий запис. Пароль, співставлений цього облікового запису, і використовується для аутентифікації користувача. Для аутентифікації віддалених користувачів не можна використовувати ті ж механізми, що застосовуються в локальній мережі. Фахівцями розроблено цілий ряд спеціальних механізмів, які отримали назву протоколів аутентифікації віддалених користувачів.

У Windows Server 2016 реалізована підтримка наступних протоколів:

- протокол RADIUS (Remote Authentication Dial-In User Service);
- протокол EAP (Extensible Authentication Protocol);
- протокол MS-CHAP (Microsoft Challenge Handshake Authentication Protocol);
- протокол MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocolversion 2);
- протокол CHAP (Challenge Handshake Authentication Protocol);
- протокол SPAP (Shiva Password Authentication Protocol);
- протокол PAP (Password Authentication Protocol)
- протокол SSL 3.0
- протокол S/MIME
- протокол Kerberos 5.0

1.3.1 Протокол RADIUS

Протокол аутентифікації Remote Authentication Dial-in User Service (RADIUS) розглядається як механізм аутентифікації і авторизації віддалених користувачів в умовах розподіленої мережевої інфраструктури, що надає централізовані послуги з перевірки достовірності та обліку для служб віддаленого доступу. Протокол

RADIUS реалізований у складі Служби перевірки автентичності в Інтернеті (Internet Authentication Service, IAS), забеспечующий централізоване управління аутентифікацією, авторизацією і аудитом доступу на підставі інформації про користувачів, одержуваної від контролер домена Windows Server 2016.

В рамках стандарту виділяються три компоненти протоколу:

- клієнт RADIUS. Клієнт RADIUS приймає від користувачів запити на аутентифікацію. Всі прийняті запити переадресовуються серверу RADIUS для подальшої аутентифікації і авторизації. Як правило, в якості клієнта протоколу RADIUS виступає сервер віддаленого доступу;
- сервер RADIUS. Основне завдання сервера RADIUS полягає в централізованій обробці інформації, наданої клієнтами RADIUS.Один сервер здатний обслуговувати декілька клієнтів RADIUS. Сервер здійснює перевірку автентичності користувача та його повноважень. Прицьому в залежності від реалізації сервера RADIUS для перевірки автентичності використовуються різні бази даних облікових записів. Реалізований в рамках служби Internet Authentication Service (IAS) сервер RADIUS здатний в процесі перевірки автентичності користувача здійснювати взаємодію зі службою каталогу Active Directory;
- посередник RADIUS. Взаємодія клієнтів і серверів RADIUS здійснюється за допомогою спеціальних повідомлень. У розподілених мережах клієнт і сервер RADIUS можуть бути розділені різними мережевими пристроями (такими, наприклад, як маршрутизатор). Під посередником RADIUS розуміється мережеве пристрій, здатний здійснювати пере направлення повідомлень протоколу RADIUS;

- протокол RADIUS є відкритим стандартом Інтернету. В силу цього он может використовуватися для організації процесу аутентифікації в гетерогенних мережах. Так, наприклад, для аутентифікації на UNIX-системах може використовуватися інформація про облікові записи користувачів з каталогу ActiveDirectory;
- підтримка функцій сервера RADIUS, а також посередника RADIUS реалізована в Windows Server 2016в рамках Служби перевірки автентичності в Інтернеті (Internet Authentication Service, IAS). Ця служба позиціонується як механізм централізованої аутентифікації та авторизації користувачів, використовують різні способи підключень до мережі. Служба IAS інтегрована з іншими;
- базовими службами Windows Server 2016, такими як служба маршрутизації та віддаленого доступу та служба каталогу Active Directory. Служба маршрутизації та віддаленого доступу використовує службу IAS для аутентифікації і авторизації користувачів, що підключаються до мережі віддалено. Фактично у разі розгортання в корпоративній мережі служби IAS сервери віддаленого доступу не виконують процес аутентифікації користувачів. Всі обов'язки з перевірки достовірності користувачів бере на себе служба IAS. При цьому служба каталогу розглядається службою IAS як сховище інформації про облікові записи користувачів;
- перевага використання IAS для аутентифікації і авторизації користувачів особливо очевидно в гетерогенних мережах, що реалізують різні механізми підключень до мережі (без проводовий доступ, комутовані підключення, а також VPN-

підключення). Підтримка цього протоколу реалізована на багатьох сучасних платформах, що дозволяє використовувати його в між платформних рішеннях;

1.3.2 Протокол EAP

Протокол EAP (Extensible Authentication Protocol) являє собою розширюваний механізм аутентифікації, що дозволяє уніфікувати процес перевірки справжності користувачів, надаючи при цьому учасникам з'єднання можливість використання найрізноманітніших схем аутентификации. Специфікація протоколу EAP описує способи підключення найрізноманітніших схем аутентифікації (в числі яких - смарт-карти, протокол RADIUS і т. п.). Можна розглядати протокол EAP як універсальну платформу для реалізації будь-яких необхідних схем аутентифікації. Точна схема аутентифікації, використовувана учасниками з'єднання, встановлюється в результаті переговорів між клієнтом віддаленого доступу і сервером віддаленого доступу.

Протокол EAP дозволяє виробляти відкриті переговори між клієнтом віддаленого доступу і сервером віддаленого доступу, що складаються із запитів сервера на отримання ідентифікуючої інформації та відповідних відповідей клієнта. Наприклад, якщо EAP використовується спільно зі смарт-картами, сервер віддаленого доступу може окремо запросити у клієнта віддаленого доступу назву, PIN-код і ємність смарт-карти. Якщо на всі питання отримані задовільні відповіді, клієнт віддаленого доступу вважається аутентіфіцированним і отримує дозвіл на віддалений доступ до мережі.

Спеціальна схема перевірки автентичності EAP називається типом EAP(EAP type). Для успішної перевірки автентичності і клієнт віддаленого доступу, і сервер видаленого доступу повинні підтримувати один і той же тип EAP.

У Windows Server 2016 реалізована підтримка двох типів EAP (EAP-MD5 CHAPi EAP-TLS), Однак при необхідності адміністратор може розширити функціональність протоколу EAP, додавши підтримку інших типів EAP. Для цього достатньо підключити відповідні модулі аутентифікації. Необхідно, однак, пам'ятати про те, що для успішної аутентифікації соответствующій модуль повинен бути підключений як на сервері віддаленого доступу, так і на клієнті віддаленого доступу.

Крім того, в рамках Windows Server 2016 передбачена можливість передачі повідомлень протоколу EAP в середині повідомлень протоколу RADIUS (компонент EAP-RADIUS), Ця можливість може бути використана в ситуації, коли в мережах експлуатується інфраструктура протоколу RADIUS як основний механізм аутентифікації. При цьому інфраструктура RADIUS може бути використаний для передачі повідомлень протоколу EAP.

Щоб забезпечити перевірку справжності на базі EAP, необхідно:

- дозволити EAP як протокол аутентифікації на сервері віддаленого доступу;
- дозволити EAP, і, якщо потрібно, налаштувати тип EAP для відповідної політики, віддаленого доступу;
- дозволити і налаштувати EAP на стороні клієнта віддаленого доступу.

1.3.3 Протокол CHAP

Протокол CHAP (Challenge Handshake Authentication Protocol) являє собою механізм перевірки достовірності типу "запит-відповідь", що використовує схему хешування MD-5 для необоротного перетворення пароля користувача в унікальну послідовність символів.

Обидва учасники з'єднання виконують подібне перетворення. Завдяки цьому по мережі передається не сам пароль, а тільки хешированa послідовність. Сервер порівнює отриману послідовність з власною копією і тільки в разі ідентичності послідовностей користувач вважається аутентіфіцированим. В якості одного з притаманних протоколу недоліків можна відзначити відсутність механізмів взаємної аутентифікації всіх учасників з'єднання.

Протокол аутентифікації CHAP є стандартом Інтернету (RFC 1994) і підтримується безліччю виробників програмного забезпечення. У середовищі Windows Server 2003 протокол CHAP може бути використаний для аутентифікації клієнтів віддаленого доступу сторонніх виробників.

1.3.4 Протокол MS-CHAP v2

Протокол MS-CHAP (Microsoft Challenge Handshake Protocol) являє собою реалізацію протоколу CHAP, запропоновану компанією Microsoft. На відміну від CHAP, для хешування паролів застосовується алгоритм MD4. Існує дві версії протоколу MS-CHAP. Друга версія протоколу MS-CHAP (MSCHAPv2) пропонує більш ефективний механізм аутентифікації. Зокрема, реалізований механізм взаємної аутентифікації. Сервер віддаленого доступу по закінченні процедури аутентифікації клієнта віддаленого доступу надає йому інформацію про власні повноваження. З'єднання несчітаемих встановленим до тих пір, поки клієнт не упевниться в автентичності сервера віддаленого доступу.

1.3.5 Протоколи PAP і SPAP

Протокол PAP (Password Authentication Protocol) використовує паролі, що передаються відкритим текстом, і є найпростішим

протоколом перевірки автентичності користувачів. Зазвичай з'єднання на його основі встановлюється, якщо клієнт віддаленого доступу і сервер віддаленого доступу не можуть домовитися про більш безпечної формі перевірки автентичності. Протокол PAP передбачає передачу паролів користувачів відкритим текстом. Кожен, хто перехопить пакети процесу аутентифікації, може легко прочитати пароль і використовувати його для несанкціонованого доступу до корпоративної мережі. Фактично протокол PAP застосовується тільки в тому випадку, коли клієнт і сервер віддаленого доступу не підтримують ніяких інших протоколів аутентифікації. У цій ситуації передача пароля відкритим текстом є єдиною можливістю підтвердити повноваження користувача. С іншого боку, заборонивши використання протоколу PAP, можна бути впевненим у тому, що паролі користувачів ніколи не будуть передаватися по мережі відкритим текстом. Відключення протоколу PAP дозволить зробити процес аутентифікації більш захищеним. Однак клієнти видаленого доступу, що підтримують тільки протокол PAP, не зможуть встановити з'єднання з вашим сервером віддаленого доступу. Протокол аутентифікації SPAP (Shiva Password Authentication Protocol) використовує для шифрування паролів реверсивний механізм шифрування Shiva. У середовищі Windows Server 2003 протокол SPAP може застосовуватися для організації з'єднань з Shiva LAN Rover. Ця схема перевірки достовірності більш безпечна, ніж передача даних відкритим текстом, але менш безпечна, ніж CHAP або MS-CHAP. Пов'язано це з тим, що протокол SPAP не передбачає захист від перехоплення зашифрованих паролів, які згодом можуть бути використані для несанкціонованого доступу в систему (один і той же пароль при виконанні операції шифрування буде давати одну і ту ж послідовність).

1.3.6 Протокол SSL 3.0

Протокол SSL (secure socket layer) був розроблений фірмою Netscape як протокол, який надає захист даних між сервісними протоколами (такими як HTTP, NNTP, FTP і т.д.) і транспортними протоколами (TCP/IP). Часто для нього використовується абревіатура HTTPS. Саме ця латинська буква "s" перетворює звичайний не захищений канал передачі даних в Інтернету по протоколі HTTP у засекречений чи захищений.

Протокол SSL надає "безпечний канал", що має три основні властивості:

- канал є часткою. Шифрування використовується для всіх повідомлень після простого діалогу, що служить для визначення секретного ключа;
- канал аутентифікован. Серверна сторона діалогу аутентифіковується завжди, у той час як клієнтська − опціонально;
- канал надійний. Транспортування повідомлень містить у собі перевірку цілісності (із залученням MAC).

Слід зазначити, що SSL не тільки забезпечує захист даних в Інтернеті, але й так само робить упізнання сервера і клієнта (server/client authentication). У цей час протокол SSL прийнятий W3 консорціумом (W3 Consortium) на розгляд як основний захисний протокол для клієнтів і серверів (WWW browsers and servers) у мережі Інтернет.

1.3.7 Протокол обміну повідомленнями S/MIME

Цифрові підписи і шифрування інформації − це фундаментальні компоненти S/MIME. З іншого боку, S/MIME − це невелика підмножина інфраструктури PKI, що забезпечує багатий вибір засобів захисту, PKI підтримує смарт-карти, SSL-користувальницькі сертифікати і багато

чого іншого. X.509 − це стандарт цифрових сертифікатів, що визначає формат сертифікату, фактично використовуваного S/MIME. Сертифікат ідентифікує інформацію про власника і включає інформацію про його відкритий ключ. X.509 − найбільш широко використовуваний цифровий сертифікат і тому він вважається промисловим стандартом. Продукти, які використовують PKI, такі як Windows Server 2016Certificate Services, генерують сертифікати X.509 для використання клієнтами, що розпізнають формати S/MIME.

1.3.8 Протокол Kerberos

Протокол Kerberos являє собою набір методів ідентифікації і перевірки істинності партнерів по обміну інформацією (робітників станцій чи користувачів серверів) у відкритій (незахищеній) мережі. Процес ідентифікації не залежить від аутентифікації, виконуваною мережною операційною системою, не ґрунтується в прийнятті рішень на адресах хостів і не припускає обов'язкову організацію фізичної безпеки всіх хостів мережі. Крім того допускається, що пакети інформації, передані по мережі, можуть бути змінені, прочитані і передані в будь-який момент часу.

Слід зазначити, що більшість додатків використовує функції протоколу Kerberos тільки при створенні сеансів передачі потоків інформації. При цьому передбачається, що наступне несанкціоноване руйнування потоку даних неможливо. Тому застосовується пряма довіра, заснована на адресі хоста. Kerberos виконує аутентифікацію як довірена служба третьої сторони, використовуючи шифрування за допомогою загального секретного ключа (shared secret key).

Аутентифікація виконується в такий спосіб:

- клієнт надсилає запит серверу аутентифікації (Authentication Server,AS) на інформацію, що однозначно ідентифікує деякий потрібний клієнту сервер;
- сервер AS передає необхідну інформацію, зашифровану за допомогою відомого користувачу ключа. Передана інформація складається з квитка сервера і тимчасового ключа, призначеного для шифрування (часто називаного ключем сеансу);
- клієнт пересилає серверу квиток що містить ідентифікатор клієнта ключ сеансу, зашифровані за допомогою ключа, відомого серверу;
- тепер ключ сеансу відомий і клієнту і серверу. Він може бути використаний для аутентифікації клієнта, а також для аутентифікації сервера. Ключ сеансу можна застосовувати для шифрування переданої в сеансі інформації для взаємного обміну ключами під-сеансу, призначеними для шифрування наступної переданої інформації.

Протокол Kerberos функціонує на одному чи декількох серверах аутентифікації, що працюють на фізично захищеному хості. Сервери аутентифікації ведуть бази даних партнерів по обміну інформацією в мережі (користувачів, серверів та ін.) і їхніх секретних ключів. Програмний код що забезпечує функціонування самого протоколу і шифрування даних, знаходиться в спеціальних бібліотеках. Для того щоб виконувати аутентифікацію Kerberos для своїх транзакцій, додатки повинні зробити кілька звертань до бібліотек Kerberos.

Процес аутентифікації складається з обміну необхідними повідомленнями із сервером аутентифікації Kerberos.

Протокол Kerberos складається з декількох субпротоколів (чи протоколів обміну повідомленнями). Існує два методи, якими клієнт

може запросити в сервера Kerberos інформацію, що ідентифікує визначений сервер.

Перший спосіб припускає, що клієнт посилає AS простий текстовий запит квитка для конкретного сервера, а у відповідь одержує дані, зашифровані за допомогою свого секретного ключа. Як правило, у даному випадку клієнт надсилає запит на квиток, що дозволяє одержати квиток (Ticket Granting Ticket, TGT), що надалі використовується для роботи із сервером, що видає квитки, (Ticket Granting Server, TGS). Другий спосіб припускає, що клієнт посилає TGT-квитки на TGS-сервер так само, начебто він обмінюється інформацією з іншим сервером додатків, що вимагають аутентифікації Kerberos.

Інформація, що ідентифікує сервер, може бути використана для ідентифікації партнерів по транзакції, що дозволить гарантувати цілісність переданих між ними повідомлень чи зберегти в секреті передану інформацію. Для ідентифікації партнерів по транзакції клієнт посилає квиток на сервер.

Оскільки квиток, що посилається, "відкритий" (деякі його частини зашифровані, але вони не перешкодять виконанню посиланню копії) і може бути перехоплений і використаний зловмисником, для підтвердження істинності партнера, що послав квиток, передається додаткова інформація, названа аутентифікатором. Вона зашифрована за допомогою ключа сеансу і містить відлік часу, який підтверджує, що повідомлення було згенеровано недавно і не є копією оригінальної посилки. Шифрування аутентифікатора за допомогою ключа сеансу доводить, що інформація була передана щирим партнером по обміну даними. Оскільки крім запитуючого партнера і сервера ніхто не знає ключ сеансу (він ніколи не посилається по мережі для перевірки ідентифікації користувачів і шифрування обміну даними по мережі), для настроювання SSL для Web серверов необхідно виконати наступні дії:

1. одержання й установка сертифіката сервера;

2. підтвердження установки;
3. створення резервної копії сертифіката сервера;
4. включення SSL для віртуальних каталогів IIS 7.0.

Безпечні/багатоцільові розширення електронної пошти (Secure/Multipurpose Internet Mail Extensions − S/MIME) застосовуються для цифрового підпису і шифрування повідомлень. Цифровий підпис забезпечує аутентифікацію, неможливість відмовлення і цілісність даних, а шифрування захищає конфіденційний зміст повідомлень.

Для підтримки S/MIME використовуються цифрові сертифікати X.509. Сертифікат ідентифікує інформацію про власника сертифіката і включає інформацію про відкритий ключ власника.

X.509 − це промисловий стандарт цифрових сертифікатів. S/MIME підтримують наступні шаблони сертифікатів Windows Server 2016: Exchange User (Користувач Exchange), Exchange Signature Only (Тільки для цифрових підписів Exchange), Smartcard User (користувач смарт-карти) і User (Користувач).Щоб описаний процес працював, відправник повинен мати в себе копію цифрового сертифікату одержувача. Сертифікат може бути отриманий як із глобального списку адрес (Global Address List - GAL), так і зі списку контактів відправника. Цифровий сертифікат містить відкритий ключ шифрування одержувача, що використовується для створення сейфа для основного ключа шифрування.

Коли адресат одержує повідомлення, він використовує свій секретний ключ шифрування для одержання доступу до основного ключа, який застосовується далі для розшифровки самого повідомлення (можливості по відкритому виду), з його допомогою можна цілком гарантувати істинність партнера. Цілісність повідомлень, якими обмінюються партнери, гарантується за допомогою ключа сеансу (передається у квитку і міститься в інформації ідентифікації партнера). Цей підхід дозволяє знайти атаки типу посилки зловмисником

перехопленої копії запиту і модифікації потоку даних. Це досягається генеруванням і пересиланням контрольної суми (хеш-функції) повідомлення клієнта, зашифрованої за допомогою ключа сеансу. Безпека і цілісність повідомлень якими обмінюються партнери може бути забезпечена шифруванням переданих даних за допомогою ключа сеансу, що пересилається в квитку і партнера, що міститься в інформації ідентифікації.

Описана вище аутентифікація вимагає доступу на читання до бази даних Kerberos. Однак іноді записи бази даних можуть бути модифіковані. Це відбувається, наприклад, при додаванні нових партнерів по обміну інформацією чи при зміні секретного ключа партнера. Зміни бази даних виконуються за допомогою спеціального протоколу обміну між клієнтом і сервером Kerberos, що застосовується із підтримкою декількох копій баз даних Kerberos.

Для нормальної роботи протоколу Kerberos необхідно, щоб кожен хост мережі мав годинник, які б були приблизно синхронізовані з годинником інших хостів. Синхронізація потрібна, щоб було легше знайти факт передачі копії заздалегідь перехопленого повідомлення. Ступінь приблизності синхронізації може бути встановлена індивідуально для кожного сервера. Сам протокол синхронізації серверів мережі повинен бути захищений від атак зловмисників

1.4 Висновок

Використання захищеного доступу для мобільних користувачів доступу забезпечує:

- можливість одержання email повідомлень у ручному й автоматичному режимі для базових мобільних користувачів;
- можливість мобільного доступу по захищеному каналу до базових елементів workflow типу Пошта, Контакти, Календар,

Задачі для просунутих користувачів із шифруванням трафіку на всіх етапах передачі інформації;

- організацію захищеного каналу, що блокує можливість перехоплення і дешифрування даних;
- швидке, якісне і надійне забезпечення бізнес-процесів і створення загального робочого простору для мобільних користувачів інтрамережі підприємства.

Для реалізації цих можливостей потрібно:

- Проаналізувати нормативну базу та загрози при підключенні до інтрамережі мобільних пристроїв користувачів.
- Налаштувати архітектуру інтрамережі підприємства для безпечного віддаленого доступу до ресурсів.
- Розгорнути центр сертифікації підприємства з можливістю web-доступу для отримання клієнтських сертифікатів для мобільних співробітників
- Налаштувати сервери інтрамережі підприємства і процедуру видачі сертифікатів для віддалених користувачів.
- Розробити рекомендації по налаштуванню міжмережевого екрану на взаємодію з мобільними користувачами
- Розробити рекомендації політики видачі, відновлення та відкликання сертифікатів для мобільних користувачів

РОЗДІЛ 2. ДОСЛІДЖЕННЯХ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ ПРИ ВЗАЇМОДІЇ З МОБІЛЬНИМИ КОРИСТУВАЧАМИ

Об’єкт досліджень –інформаційно-комунікаційна система підприємства що взаємодіє з мобільними користувачами.

Предмет досліджень – рівень захисту інформації при доступі мобільних співробітників до інформаційних ресурсів підприємства.

Мета – Розробити рекомендації по процедурі розгортання служб та сервісів в середовищі Windows Server 2016 що забезпечують безпечний обмін інформацією із мобільними користувачами.

Вихідні дані для проведення роботи:

- державні стандарти України в галузі інформаційної безпеки, нормативні документи з технічного захисту інформації та закони України;
- міжнародні стандарти в галузі інформаційної безпеки.

Наукова новизна роботи полягає у розробці рекомендацій щодо розгортання служб, засобів і методів аутентифікації в середовищі Windows Server 2016, що забезпечують безпечний обмін інформацією з віддаленими користувачами.

Практична цінність результатів полягає у розробці практичних рекомендацій щодо створення політики безпеки віддаленого доступу в комп'ютерної мережі 3 класу на платформі Windows Server 2016.

Результати повинні відповідати вимогам Закону України «Про інформацію», Закону України «Про захист персональних даних», Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», «Положення про технічний захист інформації в Україні», що затверджено указом Президента України від 27 вересня 1999 р. №1229/99, НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу», НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в

комп’ютерних системах від несанкціонованого доступу», НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу», «Про вищу освіту», Закону України «Про освіту», «Положення про організацію навчального процесу у вищих навчальних закладах», що затверджено наказом Міністерства освіти України від 2 червня 1993 р. №161, нормативних документів з технічного захисту інформації, державних стандартів України в галузі інформаційної безпеки та інших законів України, що стосуються забезпечення безпеки інформації.

Результати досліджень мають бути подано у вигляді, що дозволяє безпосереднє використання для створення засобів захисту інформації в гібридних або повністю системах хмарних обчислень.

Економічний ефект від реалізації результатів роботи очікується позитивним завдяки зниженню вірогідності порушення цілісності та конфіденційності корпоративної інформації.

Соціальний ефект від реалізації результатів роботи очікується позитивним завдяки створенню умов для реалізації можливостей працівникам підприємства підвищити продуктивність праці та її комфортність.

2.1 Хмарні сервіси Windows Server 2016 для мобільних користувачів

В разі гібридного розгортання, рішення Microsoft Intune є на порталі Azure. Вибравши Intune на порталі Azure, ви можете управляти мобільними пристроями, комп'ютерами та додатками вашої організації.

Intune — хмарна служба в середовищі управління мобільністю пристроями та додатками , що підвищує продуктивність праці співробітників при захисті корпоративних даних. Можна використовувати Intune для виконання наступних завдань:

- керування мобільними пристроями, які використовують

працівники для доступу до даних організації.

- Керування мобільними застосунками, які використовуються співробітниками.
- Захист даних організації за допомогою керування та спільного доступу до неї.
- Забезпечення відповідності пристроїв і прикладних вимог безпеки організації
- За допомогою Intune виконуються такі бізнес-задачі:
- Захист локальної електронної пошти та даних для доступу з мобільних пристроїв.
- Захист електронної пошти та даних Office 365 для безпечного доступу з мобільних пристроїв.
- Видача телефонів що належать організації співробітникам
- Програма " Принеси свій пристрій" (BYOD) з використанням персональних пристроїв для всіх співробітників.
- Забезпечення безпечного доступу співробітників до Office 365 з непрямих загальнодоступних кіосків.
- Видача співробітникам загальних планшетів для обмеженого користування.

Intune - це компонент рішення Enterprise Mobility + Security (EMS), який управляє мобільними пристроями і додатками. Intune тісно інтегрується з іншими компонентами EMS, такими як Azure Active Directory (Azure AD), для керування посвідченнями та контролю доступу, а також з Azure Information Protection для захисту даних. При використанні разом з Office 365 ваші співробітники можуть ефективно працювати на всіх пристроях з одночасним захистом даних організації.

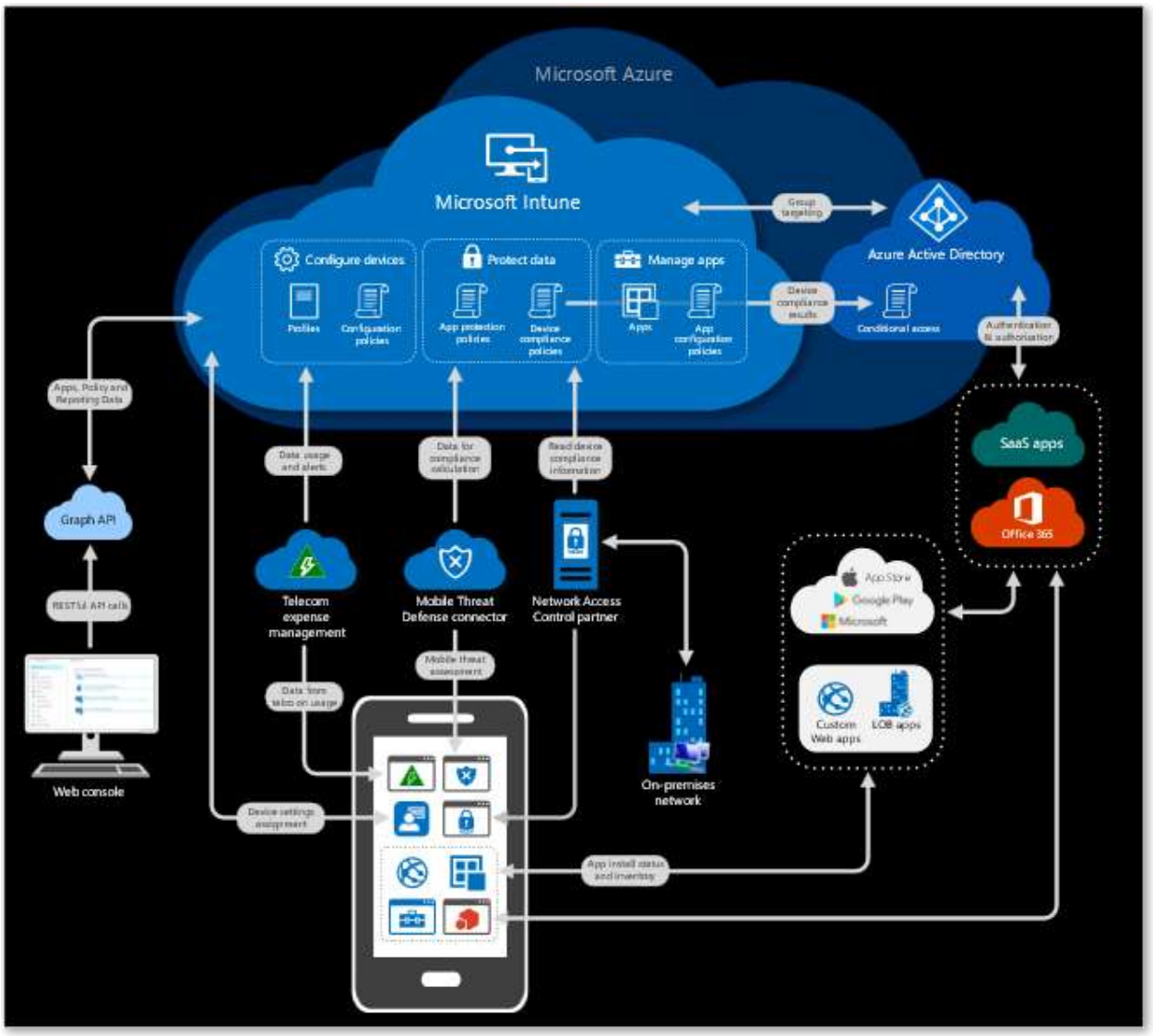

Рисунок 2.1 Схема архітектури Intune

2.2 Принципи управління пристроями Intune

Управління пристроями Intune використовує протоколи або API, доступні в операційних системах мобільних пристроїв. Вона включає такі завдання, як:

- Реєстрація пристроїв в системі управління, щоб IT-відділ мав відомостями про пристрої, здійснюють доступ до корпоративних службам.

- Налаштування пристроїв, щоб забезпечити їх відповідність стандартам по працездатності і безпеки організації.
- Надання сертифікатів і профілів Wi-Fi і VPN для доступу до корпоративних службам.
- Оцінка відповідності пристроїв корпоративним стандартам і ведення відповідних звітів.
- Видалення корпоративних даних з керованих пристроїв.

Вважають, що контроль доступу до корпоративних даних є функцією управління пристроями. Але ці можливості не надаються мобільною операційною системою. За це відповідає постачальник посвідчень. У нашому випадку постачальником посвідчень є Azure Active Directory (Azure AD) - система управління ідентифікацією та доступом корпорації Майкрософт. Intune інтегрується з Azure AD, щоб підтримувати широкий набір сценаріїв контролю доступу.

Наприклад, можна зажадати, щоб мобільний пристрій відповідало корпоративним стандартам, визначеним у Intune, перш ніж воно зможе отримати доступ до корпоративної службі, такий як Exchange. Аналогічним чином можна прив'язати корпоративну службу до певного набору мобільних додатків. Наприклад, можна дозволити доступ до Exchange Online тільки з Outlook або Outlook Mobile.

2.3 Принципи управління додатками Intune

Коли говориться про управління додатками, то мають на увазі такі завдання:

- призначення мобільних додатків співробітникам;
- настройку додатків за допомогою стандартних налаштувань, які використовуються при запуску додатки;
- управління використанням корпоративних даних і загальним доступом до них в мобільних додатках;

- видалення корпоративних даних з мобільних додатків;
- оновлення додатків.
- звіти по інвентаризації мобільних додатків;

- відстеження використання мобільних додатків.

Коли говориться про конфігурацію програми та Intune, ми маємо на увазі конкретні технології, наприклад конфігурація керованого застосування в iOS або в Android. Поняття управління мобільними додатками (MAM), позначається як кожна з цих можливостей окремо, так і певне їх поєднання. Наприклад, користувачі часто не відрізняють концепцію конфігурації програми від концепції захисту корпоративних даних в мобільних додатках. Це викликано тим, що деякі мобільні додатки містять параметри для настройки функцій забезпечення безпеки даних.

При використанні Intune з іншими службами в EMS для мобільних додатків організації можна забезпечити значно вищий рівень безпеки, ніж той, який дозволяє реалізувати мобільна операційна система і конфігурація мобільних додатків. Додаток, кероване з допомогою EMS, має доступ до великого набору засобів захисту мобільних додатків і даних, включаючи наступне:

- Єдиний вхід.
- Багатофакторна перевірка справжності
- Умовний доступ для додатка - дозвольте доступ, якщо мобільний додаток містить корпоративні дані
- Ізоляція корпоративних даних від особистих даних всередині однієї програми.
- Політика захисту програми (ПІН-код, шифрування, елемент "зберегти як", буфер обміну і т.д.).
- Очищення корпоративних даних з мобільного додатка.

2.4 Безпека додатків Intune

Забезпечення безпеки додатків є частиною управління додатками і в Intune, коли говориться про безпеку мобільного додатка, мається на увазі наступне:

1. Зберігання особистих відомостей окремо від корпоративних.
2. Обмеження дій, які користувачі можуть виконувати з корпоративною інформацією, наприклад: копіювання, вирізання та вставка, збереження і перегляд.
3. Видалення корпоративних даних з мобільних додатків, яке також називають вибіркової або корпоративним очищенням.

Одним із способів забезпечення безпеки мобільних додатків в Intune є функція політики захисту додатків. Політика захисту додатків використовує посвідчення Azure AD, щоб ізолювати корпоративні дані від особистих даних. Для відомостей, доступ до яких здійснюється даних за допомогою корпоративних облікових даних, застосовуються додаткові заходи захисту.

Наприклад, при вході на пристрій за допомогою корпоративних облікових даних користувач отримує доступ до даних, які недоступні при використанні особистого посвідчення. При використанні корпоративних даних політики захисту додатків контролюють їх збереження і спільне використання. Аналогічні засоби захисту не застосовуються, коли доступ до даних здійснюється з допомогою особистого посвідчення користувача. Таким чином, IT-відділ може керувати корпоративними даними, і кінцевий користувач зберігає контроль над своїми особистими даними, які залишаються конфіденційними.

Більшість рішень для управління корпоративною мобільністю підтримує основні технології мобільних пристроїв і мобільних додатків.

Зазвичай вони нерозривно пов'язані з пристроєм, який реєструється в рішенні управління мобільними пристроями (MDM) організації. Intune підтримує такі сценарії, а також підтримує безліч сценаріїв "без реєстрації".

Рівень впровадження сценаріїв "без реєстрації" в різних організаціях різний. У деяких організаціях вони є основним стандартом або дозволені для додаткових пристроїв, таких як особисті планшети. В інших вони взагалі не підтримуються. Навіть в останньому випадку, коли організації потрібно реєструвати всі пристрої співробітників в системі MDM, сценарії "без реєстрації" зазвичай підтримуються для підрядників, постачальників та інших пристроїв, що представляють певні виключення.

Технологію "без реєстрації" Intune можна використовувати навіть на зареєстрованих пристроях. Наприклад, пристрої, зареєстровані в MDM, можуть мати засоби захисту, що надаються мобільною операційною системою. Захист від відкриття - це функція iOS, яка забороняє відкривати документи в додатках, наприклад Outlook, в інших додатках, наприклад Word, якщо обидва додатки не перебувають під управлінням провайдера управління мобільними пристроями. Крім того, IT-відділ може застосувати до керованим за допомогою EMS мобільних додатків політику захисту додатків, щоб управляти функціями "зберегти як" або надати багатофакторну перевірку справжності.

Яку б позицію організація не займала по відношенню до зареєстрованих і незареєстрованим мобільних пристроїв і додатків, Intune в складі EMS володіє засобами, які допоможуть підвищити ефективність роботи співробітників і захистити корпоративні дані.

2.5 Сценарії захисту інформації на мобільних пристроях

Потреби в мобільності підприємства стрімко змінюються, і підхід Microsoft до задоволення їх іноді може відрізнятися від інших рішень на ринку. Найкращий спосіб узгодити ваші бізнес-цілі полягає в тому, щоб представити те, що ви хочете досягти, у вигляді сценаріїв, які необхідно реалізувати для ваших співробітників, партнерів і IT-відділів.

В дипломній роботі розглядалося шість найбільш поширених сценаріїв для використання Intune.

2.5.1 Захист локальної електронної пошти та даних для безпечного доступу з мобільних пристроїв

Більшість стратегій мобільності підприємства починаються з плану надання співробітникам безпечного доступу до електронної пошти з мобільних пристроїв, підключених до Інтернету. Багато організацій досі мають локальні дані та сервери застосунків, наприклад, Microsoft Exchange, розміщені в корпоративній мережі.

Intune надає інтегрований умовний доступ рішення для Exchange Server, який гарантує, що доступ до електронної пошти доступний тільки через мобільні пристрої, зареєстровані в Intune. Не потрібно розгортати інші шлюзові комп'ютери в корпоративній мережі.

Крім того, Intune дозволяє надавати мобільні додатки з безпечним доступом до локальних даних, таких як сервер додатків. Зазвичай, для керування доступом у поєднанні зі стандартним шлюзом VPN або проксі-сервером у мережі периметра використовувати керовані сертифікати Intune.

У цих випадках єдиним способом доступу до корпоративних даних є реєстрація пристрою в системі управління. Після реєстрації пристроїв система керування гарантує, що пристрої відповідають політиці перед наданням їм доступу до корпоративних даних. Крім того, ви можете використовувати інструмент упаковки додатків в Intune для

забезпечення того, щоб корпоративні дані будуть залишаються в бізнес-додатках і не будуть передані споживачу додатків або послуг.

2.5.2 Захист хмарної електронної пошти та даних для безпечного доступу з мобільних пристроїв

Захист корпоративних даних (e-mail, документи, миттєві повідомлення, контакти) в хмарному сервісі Office 365 не дає жодних труднощів для вас або ваших користувачів.

Intune є інтегроване рішення умовного доступу, яке гарантує, що користувачі, додатки та пристрої можуть отримати доступ до даних Office 365, лише якщо вони відповідати вимогам щодо відповідності організації :

- пройшли багатофакторну автентифікацію,
- зареєстровані з Intune,
- використовують керовану програму,
- мають підтримувану версію ОС,
- мають пристрій PIN-код пристрою,
- мають низький ризик профілю користувача .

Офісні мобільні додатки у відповідних магазинах готові працювати з політикою вкладень даних, які можна налаштувати на основі Intune. Це дозволяє запобігти обміну даними за допомогою додатків (таких як вбудовані програми пошти) і місця зберігання (наприклад, Dropbox), які не управляються IT-відділом. Всі ці функції вбудовані в Office 365. Щоб отримати ці переваги не потрібно розгортати додаткову інфраструктуру.

Часто при розгортанні Office 365 можна налаштувати обов'язкову реєстрацію пристрою в системі керування, якщо бажано використовувати корпоративні додатки, сертифікати, Wi-Fi та конфігурації VPN, які є типовими для організації.

Але якщо користувачеві просто потрібен доступ до корпоративної електронної пошти і документів, як це часто буває у випадку з особистими пристроями, можна зажадати, щоб він використовував додатки Office для мобільних пристроїв до яких застосовані політики захисту додатків на порталі, а реєстрацію пристрою можна не виконувати.

У будь-якому випадку дані Office 365 будуть захищені встановленими вами політиками.

2.5.3 Реалізація програми "Принесіть свій пристрій" для співробітників.

Концепція " приноси свій пристрій " (BYOD) продовжує набирати популярність в організаціях як спосіб зменшити апаратні витрати або запропонувати співробітникам широкий спектр інструментів для мобільних робіт. Сьогодні є майже кожен персональний телефон, так навіщо виконувати іншу? Основна проблема завжди була переконати співробітників зареєструвати свої персональні пристрої в системі управління через побоювання, що IT-фахівці зможуть переглядати дані на них і виконувати інші дії.

Якщо реєстрація пристрою не відповідає, Intune пропонує альтернативний підхід до BYOD, що дозволяє легко керувати застосунками корпоративних даних. Intune захищає корпоративні дані, навіть якщо заявка використовується для доступу як корпоративних, так і персональних даних, як і у випадку з офісом для мобільних додатків.

Адміністратор повинен настроїти доступ до Office 365 лише з Office для мобільних пристроїв і встановлення політик для застосунків, які захищають дані за допомогою шифрування та PIN коду. Ці політики захисту додатків запобігають втраті даних у некерованих додатках і розташуваннях зберігання, як всередині, так і зовні таких програм.

Наприклад, вони можуть заборонити користувачу копіювати текст з підприємства на особистий профіль електронної пошти, навіть якщо профіль налаштовано в Outlook Mobile. Аналогічні конфігурації можуть бути розгорнуті в інші послуги та програми, які необхідні для BYOD користувачів.

2.5.4 Видача корпоративних телефонів співробітникам

Сьогодні багато співробітників є мобільними, тому ефективність мобільних пристроїв надзвичайно важлива для підвищення конкурентоспроможності. Ці співробітники вимагають безшовних доступ до всіх корпоративних додатків і даних у будь-який час і з будь-якої точки. Треба і забезпечити безпеку ваших корпоративних даних і знизити витрати на адміністрування.

Intune пропонує масові підготовки та управління рішення, що інтегрується з основними платформами підприємства для управління пристроями, представленими на ринку, в тому числі Apple пристрій реєстрації та мобільний пристрій безпеки платформи Samsung Knox. Централізоване створення конфігурацій пристроїв з використанням Intune дозволяє значно автоматизувати підготовку корпоративних пристроїв.

Порядок видачи:

- організація видає співробітнику пристрій iPhone в запечатаній коробці.
- Співробітник включає його і проходить прийняту в організації процедуру настройки, в процесі якої йому необхідно пройти аутентифікацію.
- На пристрої iPhone налаштовуються політики безпеки.

- Потім співробітник запускає додаток корпоративного порталу Intune для доступу до додаткових корпоративних додатків, доступних йому.

2.5.5 Видача працівникам загальних планшетів для обмеженого використання

Співробітники все частіше користуються мобільними технологіями. Наприклад, загальні планшети стали звичайним явищем на робочих місцях співробітників роздрібних магазинів. В яких би цілях вони не застосовувалися, будь то для проведення процедури продажу або для миттєвої перевірки запасів, планшети допомагають підвищити якість взаємодії з клієнтами.

У цьому випадку особливу важливість має простота інтерфейсу. З цієї причини планшети зазвичай надаються співробітникам у режимі обмеженого використання. Наприклад, працівник може взаємодіяти тільки з одним бізнес-додатком. Intune дозволяє масово готувати і захищати такі загальні пристрої iOS і Android і централізовано керувати ними, налаштовуючи їх для обмеженого застосування.

2.5.6 Доступ з некерованих пристроїв та додатків

Іноді співробітникам потрібно використовувати пристрої, додатки або браузери, якими ви не можете управляти, наприклад загальнодоступні комп'ютери на торгових виставках або в вестибюлях готелів.

Чи слід дозволяти співробітникам доступ до корпоративної електронної пошти з таких пристроїв? При використанні Intune дозволяється доступ до електронної пошти тільки з пристроїв, якими керує ваша організація. Так забезпечується надійна перевірка

справжності співробітників і гарантуєтеся, що вони не залишать корпоративні дані на ненадійному комп'ютері

2.6 Управління мобільними додатками і захист додатків.

В організаціях, що підтримують BYOD, дуже поширене управління мобільними додатками (MAM) без використання управління мобільними пристроями (MDM). Можливо надати користувачам можливість доступу до електронної пошти зі служби Outlook Mobile (яка підтримує функції захисту MAM), розгорнувши політику умовного доступу в Exchange Online. Існують такі причини для управління тільки додатками на особистих пристроях:

1. Зручність роботи користувачів. При реєстрації в системі MDM виводиться безліч попереджень, які є обов'язковими відповідно до вимог платформи. В результаті користувач може відмовитися від доступу до електронної пошти з особистого пристрою. В системі MAM попереджень набагато менше - користувач бачить лише одне спливаюче вікно з повідомленням про те, що функції захисту MAM включені.
2. Відповідність вимогам. У деяких організаціях діють політики, які пред'являють більш низькі вимоги до можливостей управління особистими пристроями. Наприклад, система MAM дозволяє видаляти тільки корпоративні дані з додатків, в той час як система MDM дозволяє видаляти всі дані з пристроїв

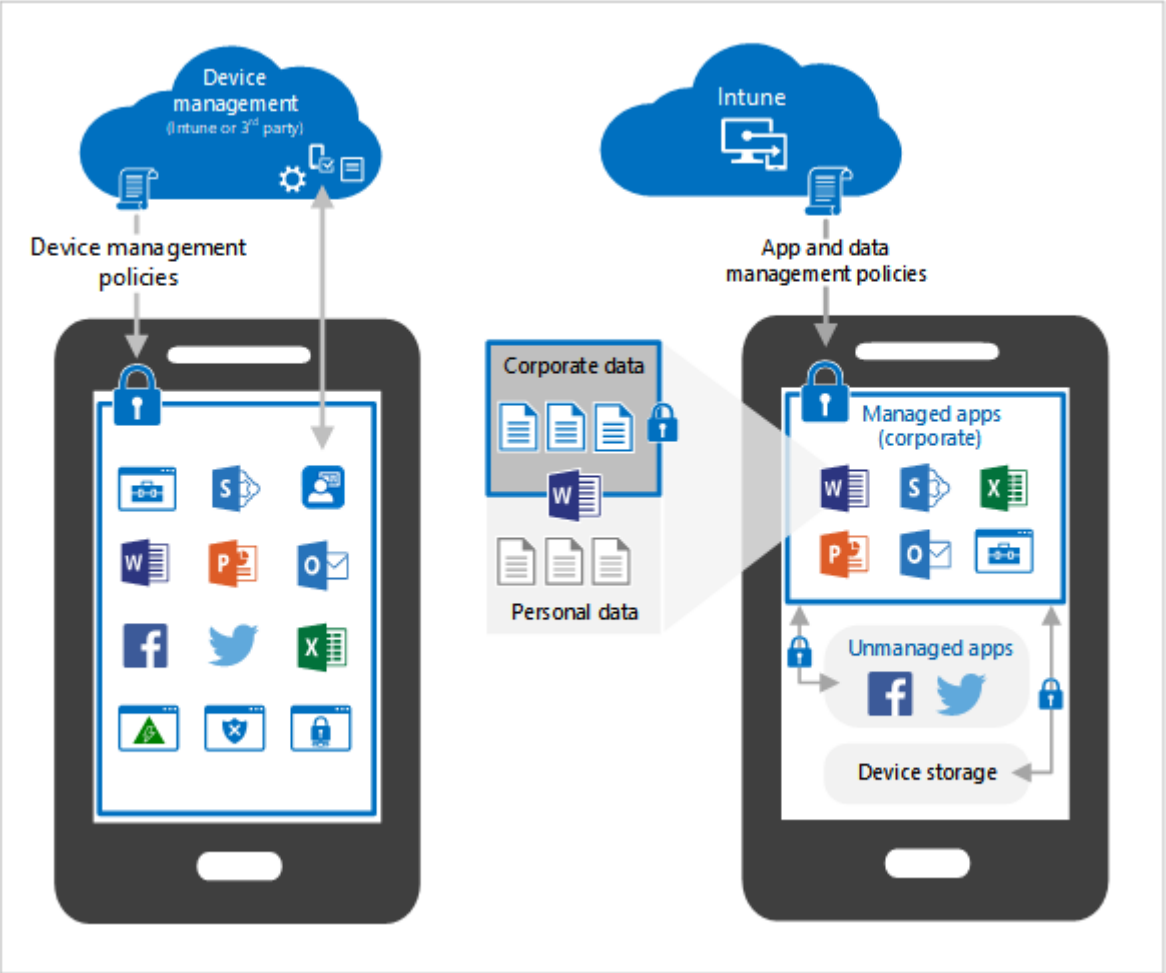

Рисунок 2.2 Управління пристроєм і управління додатками

2.7 Порівняння можливостей MAM і MDM по протидії загрозам

За допомогою умовного доступу можна надати користувачам можливість реєструвати свої пристрої або використовувати керовані програми, такі як Outlook Mobile. В обох випадках можна налаштовувати і інші умови:

1. хто саме намагається отримати доступ;
2. чи є розташування довіреною або недовірених;
3. рівень ризику при вході.
4. платформа пристрою

В таблиці 2.1 наведено порівняння цих сервісів по протидії загрозам

Таблиця 2.1 Усування загроз в разі використання MDM та MAM

Загроза	Стосується MDM	Стосується MAM
Несанкціонований доступ до даних	Вимагати членства в групі	Вимагати членства в групі
Несанкціонований доступ до даних	Вимагати реєстрації пристрою	Вимагати використання захищеного програми
Несанкціонований доступ до даних	Вимагати конкретне розташування	Вимагати конкретне розташування
Компрометація облікових записів користувачів	Вимагати багатофакторну аутентифікацію	Вимагати багатофакторну аутентифікацію
Компрометація облікових записів користувачів	Блокування користувачів з високим рівнем ризику	Блокування користувачів з високим рівнем ризику
Компрометація облікових записів користувачів	ПИН-код пристрою	ПИН-код пристрою
Компрометація пристрою або додатку	Вимагати відповідні вимоги до пристрою	Перевірка зняття захисту при запуску додатку
Компрометація пристрою або додатку	Шифрування даних на пристрої	Шифрування даних додатку
Втрата або крадіжка пристрої	Вилучення всіх даних з пристрою	Вилучення всіх даних з додатку

Продовження таблиці 2.1

Загроза	Стосується MDM	Стосується MAM
Випадкове надання загального доступу до даних або збереження даних в незахищеному місці	Обмеження резервного копіювання даних на пристрої	Обмеження операцій вирізання, копіювання і вставки
Випадкове надання загального доступу до даних або збереження даних в незахищеному місці	Обмеження операції "Зберегти як "	Обмеження операції "Зберегти як "
Випадкове надання загального доступу до даних або збереження даних в незахищеному місці	Відключити друк	Відключити друк

Управління мобільними додатками (MAM) в Intune - це набір функцій управління, що дозволяють публікувати, відправляти, налаштовувати, захищати, відстежувати і оновлювати мобільні додатки для користувачів.

MAM захищає корпоративні дані в самому додатку. За допомогою MAM без реєстрації ви можете керувати робочими або навчальними програмами, які містять конфіденційні дані, практично з будь-якого пристрою, включаючи особисті пристрої в рамках сценарію BYOD. Intune MAM дозволяє управляти багатьма бізнес-додатками, включаючи програми Microsoft Office.

Intune MAM підтримує дві конфігурації:

- Intune MDM і MAM. IT-адміністратори можуть керувати програмами тільки за допомогою MAM і політик захисту додатків на пристроях, зареєстрованих з використанням

управління мобільними пристроями Intune (MDM). Для управління додатками за допомогою MDM і MAM слід використовувати консоль Intune, яку можна знайти на порталі Azure за адресою https://portal.azure.com.

- MAM без реєстрації пристрою. MAM без реєстрації пристрою (MAM-WE) дозволяє IT-адміністраторам керувати програмами за допомогою MAM і політик захисту додатків на пристроях, які не зареєстровані з використанням Intune MDM. Це означає, що додатками можна управляти в Intune на пристроях, зареєстрованих з використанням сторонніх постачальників EMM. Для управління додатками за допомогою MAM слід використовувати консоль Intune, яку можна знайти на порталі Azure. Крім того, додатками можна управляти в Intune на пристроях, зареєстрованих з використанням сторонніх постачальників EMM (Enterprise Mobility Management) або зовсім не зареєстрованих в MDM.

2.8 Вибір рішення по управлінню мобільними пристроями

Існує три підходи до вирішення питання про управління пристроями.

- Першій підхід, для управління всіма аспектами пристроїв можна використовувати всі вбудовані можливості Intune. Цей варіант називається управлінням мобільними пристроями (MDM). У цьому випадку користувачі реєструють свої пристрої і взаємодіють з Intune за допомогою сертифікатів. IT-адміністратор може відправляти додатки на пристрої, обмежувати пристрою певної операційної системою, блокувати особисті пристрої та багато іншого. Якщо

пристрій буде втрачено або вкрадено, з нього можна видалити всі дані.

- Другий підхід полягає в управлінні додатками на пристроях. Такий варіант називається управління мобільними додатками (MAM). У цьому випадку користувачі звертаються до ресурсів організації зі своїх особистих пристроїв. При запуску цієї програми, наприклад електронної пошти або SharePoint, користувачам пропонується пройти додаткову перевірку справжності. якщо пристрій буде втрачено або вкрадено, з нього можна видалити всі дані організації.
- Третій підхід полягає в використанні як в управлінні мобільними пристроями так і в управління мобільними додатками.

2.9 Політики захисту додатків

Політики захисту додатків - це правила, які забезпечують захист корпоративних даних (Включаючи ті, які зберігаються в керованих додатках). Політика може бути або правилом, яке застосовується, коли користувач намагається отримати доступ або перемістити корпоративні дані, або набором дій, які заборонено виконувати або які відслідковуються, коли користувач працює з додатком.

2.9.1 Вимоги до керованих додатків Intune для використання політик захисту додатків

Згідно завдання дипломної роботи були визначені вимоги до керованих додатків Intune в разі використання політик захисту додатків:

- У користувача повинна бути обліковий запис Azure Active Directory (AAD).

- У користувача повинна бути ліцензію Microsoft Intune, призначену його облікового запису Azure Active Directory.
- Користувач повинен бути включений в групу безпеки, на яку поширюється політика захисту додатків. Ця ж політика захисту додатків повинна поширюватися і на певне використовуваним додатком.
- Політики захисту додатків треба створювати і розгортати в консолі Intune на порталі Azure.
- Користувач повинен увійти в додаток, використовуючи свій обліковий запис AAD.
- На пристрої користувача має бути встановлено мобільний додаток Outlook.
- У користувача повинні бути поштова скринька Office 365 Exchange Online і ліцензія, пов'язана з обліковим записом Azure Active Directory

В разі використання офісних додатків Word, Excel і PowerPoint необхідно виконати наступні вимоги:

- у користувача повинна бути ліцензія на пакет "Office 365 бізнес" або "Office 365 корпоративний", пов'язана з його обліковим записом Azure Active Directory.
- Підписка повинна включати додатки Office на мобільних пристроях і може включати хмарну обліковий запис зберігання з підтримкою OneDrive для бізнесу.
- Користувач повинен налаштувати кероване розташування за допомогою функції настроюваного збереження в параметрі політики захисту програми "Заборонити операцію" Зберегти як ". Наприклад, якщо кероване розташування - OneDrive, додаток OneDrive має бути налаштоване в додатку Word, Excel або PowerPoint користувача.

- Якщо кероване розташування - OneDrive, на додаток повинна поширюватися політика захисту яка розгорнута для користувача.

2.9.2 Функції захисту додатків

Підтримка множинної ідентифікації дозволяє пакету SDK для додатків Intune застосовувати політики захисту додатків тільки до робочої або навчальної облікового запису, що використовується для входу в додаток. Якщо вхід в додаток виконаний за допомогою особистий обліковий запис, дані залишаться без змін.

Підтримка множинної ідентифікації забезпечує загальнодоступний випуск додатків для корпоративного та особистого користування включаючи додатки Office з функціями захисту додатків Intune для корпоративних облікових записів.

Так як в Outlook реалізовано об'єднане подання повідомлень електронної пошти (особистих і корпоративних), додаток Outlook при запуску запитує PIN-код Intune.

Персональний ідентифікаційний номер (ПІН-код) - це секретний код, який використовується для перевірки прав користувача на доступ до корпоративних даних в додатку.

Intune запитує PIN-код для додатка, коли користувач намагається отримати доступ до корпоративних даних. У додатках з підтримкою множинної ідентифікації (включаючи Word, Excel і PowerPoint) користувач повинен вводити ПІН-код при спробі відкрити корпоративний документ або файл. У додатках, що використовують єдину ідентифікацію (включаючи бізнес-додатки, керовані за допомогою інструменту упаковки для додатків Intune), ПІН код потрібно вводити при запуску, так як пакет SDK для додатків Intune завжди обробляє всі дані в додатку як корпоративні.

IT-адміністратор може визначити параметр "Перевіряти вимоги доступу повторно через (Хв) "в налаштуваннях політики захисту програми Intune за допомогою консолі адміністрування Intune. Цей параметр визначає період часу, через який виконується перевірка вимоги та надають допуск на пристрої, після чого знову з'являється вікні керування з ПІН-кодом.

Для зручності ПІН-код є загальним для додатків одного видавця. В iOS один ПІН-код використовується в усіх програмах одного видавця. В Android один ПІН-код використовується у всіх додатках.

Поведінка «Перевіряти вимоги доступу повторно через (хв)" після перезавантаження пристрою.» Таймер ПІН-коду відстежує кількість хвилин бездіяльності, що визначає час для наступного відображення ПІН-коду програми Intune. В iOS перезавантаження пристрою не зачіпає таймер ПІН-коду. Тому перезавантаження пристрою не впливає на кількість хвилин, яке користувач був неактивним в додатку iOS з діючою політикою щодо ПІН-кодів Intune. В Android таймер ПІН-коду скидається при перезавантаженні пристрою.

Тому після перезавантаження пристрою додатки Android з діючою політикою в відношенні ПІН-кодів Intune, найімовірніше, запросять ПІН-код додатка незалежно відзначення параметра "Перевіряти вимоги доступу повторно через (хв)".

Для пристроїв iOS, навіть якщо ПІН-код є загальним для додатків різних видавців, запит з'явиться знову при досягненні значення «Ще раз перевірити вимоги доступу через (хв)» для додатки, у якого немає основного фокуса введення. Наприклад, у користувача є додаток A видавця X і додаток B видавця Y, і ці два додатки спільно використовують один і той же ПІН-код.

Користувач працює з додатком A (на передньому плані); додаток B знаходиться в згорнутому стані. Після досягнення значення «Ще раз

перевірити вимоги доступу через (хв)», коли користувач перейде до додатка B, буде потрібно ввести ПІН-код.

Робота ПІН-коду Intune заснована на таймері бездіяльності (тобто значення параметра "Перевіряти вимоги доступу повторно через (хв) ". Таким чином, функція ПІН-коду Intune є незалежною від запитів ПІН-коду вбудованих додатків для Outlook і OneDrive, які часто за замовчуванням прив'язані до запуску додатка. Якщо користувач одночасно отримує обидва запиту на введення ПІН-коду, PIN-код Intune повинен мати пріоритет.

ПІН-код надає доступ до корпоративних даних тільки користувачам з відповідними повноваженнями. Отже, щоб налаштувати або скинути ПІН-код для додатка Intune, користувач повинен увійти з використанням своєї робочої або навчальної облікового запису. Ця перевірка справжності обробляється Azure Active Directory за допомогою безпечного обміну маркерами і не є прозорою для пакета SDK для додатків Intune. З міркувань безпеки рекомендується шифрувати корпоративні або навчальні дані. Шифрування пов'язане з ПІН-кодом для застосування; це окрема політика захисту додатків.

2.9.3 Шифрування даних додатків

IT-адміністратори повинні розгорнути політику захисту додатків, відповідно до якої дані додатки повинні шифруватися. В рамках політики IT-адміністратор також може визначити, коли зміст має бути зашифровано.

Відповідно до політики захисту додатків, визначеної IT-адміністратором, шифруються тільки ті дані, які відзначені як корпоративні. Дані вважаються корпоративними, якщо вони створені в корпоративному розташуванні. При роботі з додатками Office в Intune корпоративними вважаються такі розташування:

- електронна пошта (Exchange) або хмарне сховище (додаток OneDrive з обліковим записом OneDrive для бізнесу).
- У бізнес-додатках, керованих за допомогою інструменту упаковки для додатків Intune, всі дані вважаються корпоративними.

Intune може очищати дані додатків трьома способами: повне очищення пристрою, вибіркова очистка для управління мобільними пристроями і вибіркова очищення для управління мобільними додатками. Додаткові відомості про віддалену очищення для MDM см. В статті Видалення пристроїв шляхом очищення або припинення використання.

2.9.4 Рішення задач управління пристроями за допомогою панелей моніторингу

Панель моніторингу управління пристроями - це централізоване засіб для виконання завдань для мобільних пристроїв та управління ними. На цій панелі моніторингу знаходяться служби, що використовуються для управління пристроями, включаючи Intune і Azure Active Directory, а також для управління клієнтськими додатками.

На панелі моніторингу "Управління пристроями" можна виконувати такі завдання:

- Реєстрація пристроїв
- Завдання відповідності пристрою вимогам
- Управління пристроями
- Управління додатками
- Електронні книги по iOS
- Установка локального з'єднувача Exchange
- управління ролями
- Управління оновленнями програмного забезпечення

- Azure Active Directory
- Керування користувачами
- Управління групами і членами
- Усунення проблем

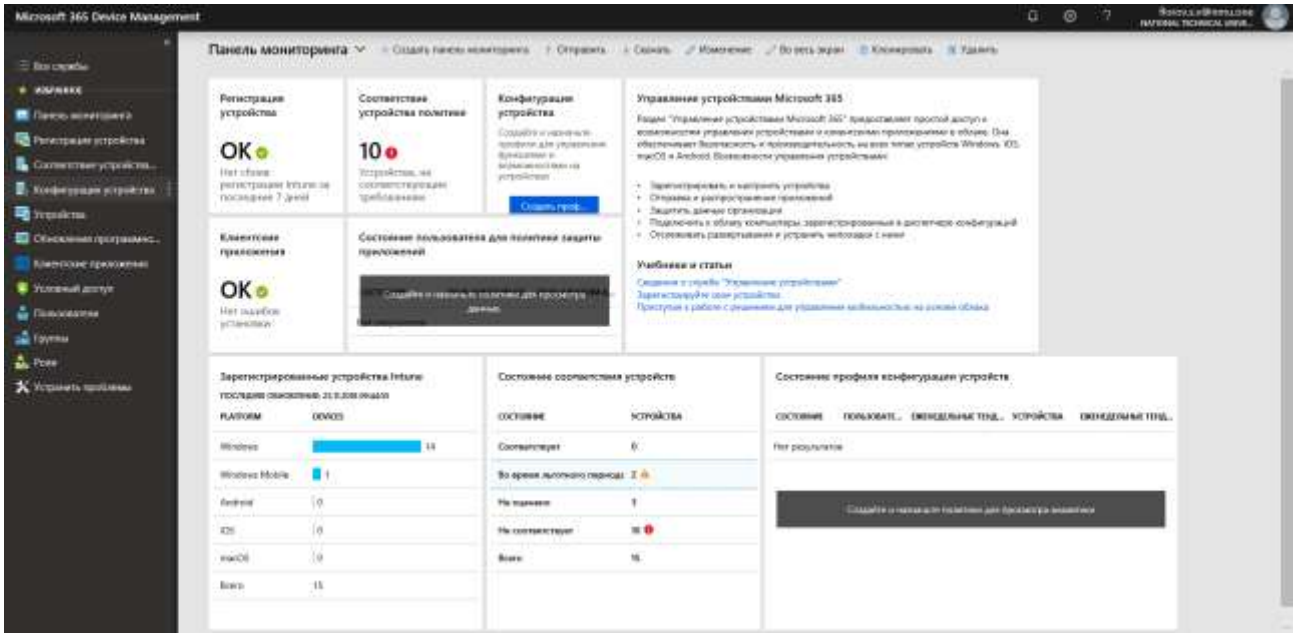

Рисунок 2.3 Панель моніторингу "Управління пристроями"

2.9.5 Рекомендації щодо плану впровадження Microsoft Intune

Згідно з завданням роботи було розроблено план впровадження установки і настройки Intune

Необхідні умови розгортання Intune:

- Підписка на Enterprise Mobility + Security (EMS) / Intune
- Підписка Office 365 (для додатків Office і додатків під управлінням політики захисту додатків)
- Сертифікат APNs Apple для включення управління платформою пристроїв iOS) Azure AD Connect для синхронізації служби каталогів

- Локальний з'єднувач Intune для Exchange забезпечує умовний доступ для локальної організації Exchange, якщо це необхідно) Intune
- Certificate Connector (для розгортання сертифіката SCEP, якщо це необхідно)

Згідно з завданням роботи було визначено 13 окремих задач по розгортанню Intune:

- Задача 1. Необхідно оформити підписку на або Intune.
  - Необхідно зверніться до корпорації Майкрософт або службу облікових записів Майкрософт і повідоміть, про бажання придбати Intune.
- Задача 2. Підписатися на Office 365
  - Вона необхідна в тому випадку, якщо ви плануєте використовувати Exchange Online і управляти мобільними додатками Office за допомогою політик захисту додатків. Якщо у організації немає такої підписки, треба звернутися до корпорації Майкрософт або служби технічної підтримки облікових записів Майкрософт.
- Задача 3. Додавання груп користувачів в Azure AD
  - Залежно вимог і сценаріїв використання Intune може знадобитися додавання користувачів або груп безпеки в Active Directory або Azure Active Directory треба переглянути поточних користувачів і групи безпеки в Active Directory або Azure Active Directory і визначте, повністю чи вони відповідають вашим потребам організації. Нових користувачів і групи безпеки треба додавати в Active Directory і синхронізувати з Azure Active Directory за допомогою Azure

AD Connect

- Задача 4. Призначення користувальницьких ліцензій Intune і Office 365
    - Всім користувачам, яких торкнеться розгортання Intune і Office 365, необхідно призначити ліцензію. Призначити ліцензії Intune і Office 365 можна на порталі Центру адміністрування Office 365.

- Задача 5. Розгортання центру управління мобільними пристроями в Intune
    - Перед початком установки, настройки, реєстрації пристроїв і управління ними за допомогою Intune слід задати Intune в якості центру управління пристроями.

- Задача 6. Підключення платформи пристрою
    - За замовчуванням більшість платформ пристроїв, крім пристроїв Apple (iOS і Mac), включені. Перш ніж можна буде реєструвати пристрої iOS в Intune і управляти ними, потрібно включити цю платформу пристроїв. Для цього необхідно створити сертифікат MDM Push і додати його в Intune.
- Задача 7. Додавання і та розгортання політик умов
    - Intune підтримує політики умов. Додайте потрібні політики умов і поверніть його в цільових групах з урахуванням вимог і варіантів використання для розгортання Intune.
- Задача 8. Додавання і та розгортання політик зміни конфігурації
    - Intune підтримує два типи політик конфігурації - загальні і настроюються. Додайте потрібні політики конфігурації і поверніть його в цільових групах з урахуванням вимог і

варіантів використання для розгортання Intune.

- Задача 9. Додавання і та розгортання профілів ресурсів
    - Intune підтримує профілі електронної пошти, Wi-Fi і VPN. Додайте потрібні профілі і поверніть його в цільових групах з урахуванням вимог і варіантів використання для розгортання Intune.
- Задача 10. Додавання і та розгортання додатків
    - Intune підтримує розгортання веб-додатків, бізнес-додатків і додатків, опублікованих в магазині. Крім того, додатками з інтегрованим пакетом SDK Intune можна управляти, зіставивши їх з політиками захисту додатків. Додайте потрібні програми і поверніть його в цільових групах з урахуванням вимог і варіантів використання для розгортання Intune.
- Задача 11. Додавання і розгортання політик відповідності
    - Intune підтримує політики відповідності. Додайте потрібні політики відповідності і поверніть його в цільових групах з урахуванням вимог і варіантів використання для розгортання Intune.
- Задача 12. Включення політик умовного доступу
    - Intune підтримує умовний доступ до Exchange Online і локальної організації Exchange, SharePoint Online, Skype для бізнесу Online і Dynamics CRM Online. Необхідно увімкнути і налаштуйте потрібні політики умовного доступу з урахуванням вимог і варіантів використання для розгортання Intune.
- Задача 13. Реєстрація пристроїв
    - Intune підтримує платформи настільних і мобільних пристроїв Windows, iOS, Mac OS, Android. Зареєструйте потрібні

платформи мобільних пристроїв з урахуванням вимог і варіантів використання для розгортання Intune.

2.9.6 Рекомендації налаштування параметрів обмежень для Android пристроїв в Intune

2.9.6.1 Загальні параметри

- Копіювання і вставка між робочим і особистим профілями. контролює операції копіювання і вставки між робочими й особистими додатками. Треба вибрати «Блокувати», щоб заблокувати. Треба вибрати «Не налаштовано», щоб відключити блокування.
- Спільне використання даних між робочим і особистим профілем. використовується, щоб дозволити або заборонити обмін даними між додатками роботи та дозвілля профілів. Цей параметр керує доступними в додатках діями загального доступу, наприклад параметром Загальний доступ в додатку браузера Chrome. Цей параметр не застосовується до операцій копіювання і вставки в буфері обміну. На відміну від параметрів політики захисту додатків, параметри обмеженого використання пристроїв управляються на порталі Intune і використовують розділ робочого профілю Android для ізоляції керованих додатків. Треба вибрати один з наступних типів:
    - Обмеження загального доступу. Це поведінка для спільного використання за замовчуванням на пристрої, який залежить від використовуваної версії Android. За замовчуванням можна передавати дані з особистого профілю в робочий. Крім того, за замовчуванням заборонено передавати дані з робочого профілю в

особистий. Цей параметр дозволяє запобігти витік даних з робочого профілю в особистий. На пристроях під управлінням версії 6.0 або новішої версії Google не блокує передачу даних з особистого профілю в робочий.

- Додатки в робочому профілі можуть обробити запит на загальний доступ з особистого профілю. Використовується, щоб включити вбудовану функцію в Android, що дозволяє передавати дані з особистого профілю в робочий. Коли ця функція включена, запит на загальний доступ, ініційований з програми особистого профілю, зможе обмінюватися даними з додатками робочого профілю. Цей параметр представляє поведінка за умовчанням для пристроїв Android під керуванням більш ранніх версій, ніж 6.0.
- Дозволити загальний доступ за межами кордонів. Дозволяє загальний доступ через кордони робочого профілю в обох напрямках. При виборі цього параметра додатки в робочому профілі можуть обмінюватися даними з некерованими додатками особистого профілю. Цей параметр дозволяє обмін даних між додатками в робочому профілі та додатками в некерованою частині пристрою. Тому використовувати його потрібно з обережністю.

- Повідомлення для робочого профілю, коли пристрій заблоковано. Використовується, щоб дозволити або заборонити додаткам в робочому профілі відображати дані в повідомленнях при якщо пристрій було заблоковано.
- Дозволи зі стандартними програмами. Задає політику дозволів за замовчуванням для всіх додатків в робочому профілі.

Починаючи з Android версії 6, під час запуску програми користувачеві вам буде запропоновано надання певних дозволів, які потрібні додаткам. Цей параметр політики дозволяє вирішити, чи будуть користувачі отримувати запит на надання дозволів для додатків в робочому профілі. Наприклад, ви можете призначити додаток робочому профілю, якому потрібен доступ до відомостей про місцезнаходження. Як правило, додаток запросить у користувача дозвіл або заборона на доступ до таких даних для додатки. Треба використовувати цю політику, щоб автоматично надавати дозволи без запиту, автоматично скасовувати дозволи без запиту або надавати право вибору користувачеві. Виберіть один з наступних типів:

  - Пристрій за замовчуванням.
  - Командний рядок.
  - Вирішувати автоматично.
  - Забороняти автоматично.

- Додавання і видалення облікових записів. Заборона на додавання і видалення облікових записів вручну в робочому профілі для кінцевих користувачів. Наприклад, при розгортанні програми Gmail в робочому профілі Android ви можете заборонити кінцевим користувачам додавати або видаляти облікові записи в цьому робочому профілі.
- Обмін контактами через Bluetooth. Забезпечує доступ до робочих контактів з іншого пристрою, наприклад машини, пов'язаного з Bluetooth. За замовчуванням цей параметр не заданий, і контакти робочого профілю не відображаються. Виберіть Увімкнути, щоб дозволити обмін і відобразити контакти робочого профілю. Цей параметр застосовується до

пристроїв з робочим профілем Android з ОС Android версії 6.0 або більш пізньої. Якщо включити цей параметр, деякі пристрої Bluetooth можуть отримати дозвіл кешувати робочі контакти при першому підключенні. У разі відключення цієї політики після початкового зв'язування або синхронізації робочі контакти можуть бути не видалені з пристрою Bluetooth.

- Screen capture (Знімок екрану). Блокування створення знімків екрану в робочому профілі пристрою, а також заборона показу вмісту на пристроях відображення, у яких немає безпечного виведення відео.
- Display work contact caller-id in personal profile (Відображати ВД дзвонить, який є робочим контактом, в особистому профілі). Якщо цей параметр включений (не налаштований), відомості про абонента, який є робочим контактом, відображаються в особистому профілі. якщо цей параметр заблокований, номер абонента, який є робочим контактом, не відображається в особистому профілі. Застосовується до ОС Android 6.0 і пізніших версій.
- Camera (Камера). Блокування камери в робочому профілі пристрою. На роботу камери в особистому профілі цей параметр не впливає.

2.9.6.2 Пароль робочого профілю.

- Вимагати пароль робочого профілю. Застосовується до Android 7.0 і пізніших версій з включеним робочим профілем. Визначення політики секретного коду, яка застосовується тільки до додатків в робочому профілі. За замовчуванням кінцевий користувач може або використовувати два окремо визначаються ПІН-коду, або об'єднати

два ПІН-коду в один, при цьому буде використовуватися більш складний ПІН-код.

- Мінімальна довжина пароля. Введіть мінімальну кількість символів, яке повинно бути в паролі користувача (4-16).
- Максимальний час бездіяльності (в хвилинах), після закінчення якого робочий профіль блокується. Виберіть час, який повинен пройти до блокування робочого профілю. За закінчення цього часу для отримання доступу користувачеві необхідно буде заново ввести свої облікові дані.
- Число невдалих спроб входу перед очищенням пристрою. Введіть кількість спроб введення невірного пароля, перш ніж робочий профіль буде видалений з пристрою.
- Закінчення терміну дії пароля (днів). Введіть число днів до зміни пароля користувача (від 1-255).
- Необхідний тип пароля. Виберіть тип пароля, який повинен бути заданий для пристрою. Необхідно вибрати один з наступних типів:
    - Пристрій за замовчуванням.
    - Біометричний з низьким рівнем безпеки
    - Обов'язкове
    - Принаймні числа
    - Складні числа. Повторювані або послідовні числа, наприклад "1111" або "1234", що не допускаються.
    - Принаймні літери
    - Принаймні букви і цифри
    - Принаймні цифри, букви і символи
- Заборонити використання попередніх паролів. Введіть кількість спроб введення нових паролів, перш ніж можна буде використовувати повторно старий пароль (від 1-24).

- Розблокування за допомогою відбитків пальців. Забороняє користувачу використовувати сканер відбитків пальців, щоб розблокувати пристрій.
- Smart Lock і інші довірені агенти. Управляє функцією Smart Lock на сумісних пристроях. Ця функція телефону, яку іноді називають довіреною агентом, дозволяє відключати або обходити пароль робочого профілю, коли пристрій знаходиться в надійному розташуванні. Наприклад, можна обходити пароль робочого профілю, якщо пристрій підключається до певного пристрою Bluetooth. Використовуйте цей параметр, щоб заборонити користувачам налаштовувати функцію Smart Lock.

2.9.6.3 Пароль пристрою

- Мінімальна довжина пароля. Введіть мінімальну кількість символів, яке повинно бути в паролі користувача (4-14).
- Максимальний час бездіяльності (в хвилинах), після закінчення якого екран блокується.
- Виберіть час, який повинен пройти до автоматичного блокування неактивного пристрою.
- Число невдалих спроб входу перед очищенням пристрою. Введіть кількість спроб введення невірного пароля, перш ніж всі дані будуть видалені з пристрою.
- Закінчення терміну дії пароля (днів). Введіть число днів до зміни пароля користувача (від 1-255).
- Необхідний тип пароля. Виберіть тип пароля, який повинен бути заданий для пристрою. Оберіть один з наступних типів:
    - Пристрій за замовчуванням.
    - Біометричний з низьким рівнем безпеки обов'язкове.
    - Принаймні числа

- Числовий комплекс. Повторювані або послідовні числа, наприклад "1111" або "1234", не допускаються.
- Принаймні літери.
- Принаймні букви і цифри
- Принаймні цифри, букви і символи

- Заборонити використання попередніх паролів. Введіть кількість спроб введення нових паролів, перш ніж можна буде використовувати повторно старий пароль (від 1-24).
- Розблокування за допомогою відбитків пальців. Забороняє користувачу використовувати сканер відбитків пальців, щоб розблокувати пристрій.
- Smart Lock і інші довірені агенти. Управляє функцією Smart Lock на сумісних пристроях. Ця функція телефону, яку також називають довіреною агентом, дозволяє відключати або обходити пароль блокування екрану пристрою, коли пристрій знаходиться в надійному розташуванні. Наприклад, можна обходити пароль робочого профілю, якщо пристрій підключається до певного пристрою Bluetooth або знаходиться поруч з NFC-тегом. Використовуйте цей параметр, щоб заборонити користувачам налаштовувати функцію Smart Lock.

2.9.6.4 Підключення до мережі

- Параметр Always-on VPN (Постійна мережу VPN). Треба вибрати «Увімкнути», щоб клієнт VPN автоматично підключався і перепідключатися до цієї мережі VPN. При перезапуску або розблокуванні пристрою, а також при зміні бездротової мережі VPN-підключення не буде розірвано або буде відразу ж відновлено. Треба

вибрати «Не налаштовано Операцію», щоб відключити постійну мережу VPN для всіх клієнтів VPN.

- Клієнти VPN. Необхідно вибрати клієнт VPN, який підтримує AlwaysOn. В наявності є таке:
    - Cisco AnyConnect
    - F5 Access
    - Palo Alto Networks GlobalProtect
    - Pulse Secure
    - особливі налаштування:
        - ідентифікатор пакету. Необхідно ввести ідентифікатор пакета додатка в магазині Google Play. Наприклад, якщо додаток в магазині Google Play має URL-адресу https://play.google.com/store/details?id=com.contosovpn.android.prod то ідентифікатор пакета буде com.contosovpn.android.prod
- Режим блокування. Необхідно вибрати «Увімкнути», щоб весь мережевий трафік йшов тільки через тунель VPN. Якщо підключення до VPN не встановлено, пристрій не матиме доступу до мережі. Необхідно вибрати « Не налаштовано Операцію», щоб дозволити проходження трафіку через тунель VPN або по мобільної мережі.

2.10 Висновок

Розроблені рекомендації щодо розгортання служб та засобів Windows Server 2016, що забезпечують реалізацію мети роботи.

Все це створює можливість віддаленого та мобільного доступу по захищеним каналом до сервісів корпоративної мережі таких як:

- Web доступ до внутрішніх і зовнішніх сайтів;
- Dial-Up доступ до корпоративної мережі;
- корпоративна електронна пошта;

- дистанційні корпоративні додатки (RemoteApps);
- віддалений доступ до сховищ даних;
- Web доступ до віддалених робочих столів (термінальний сервіс);
- Web доступ до віртуальних робочих столів (HiperV);
- доступ до файлових серверів по VPN із шифруванням трафіка на всіх етапах передачі інформації.
- керований доступ до хмарных севысів

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Завданням даної роботи є розробити обґрунтуванні рекомендацій захисту інформації. У даному розділі були виконані наступні розрахунки:

1) розрахунок капітальних витрат;
2) розрахунок поточних витрат;
3) визначена величина можливого збитку;
4) визначені та проаналізовані показники економічної ефективності системи інформаційної безпеки.

На підставі отриманих результатів було зроблено висновок щодо економічної ефективності створення обґрунтуванних рекомендацій захисту інформації.

3.1 Визначення трудомісткості розробки обґрунтованих рекомендацій захисту інформації.

Трудомісткість створення обґрунтуванних рекомендацій визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації.

Формула для розрахунку трудомісткості має наступний вигляд:

$$t = t_{тз} + t_в + t_а + t_{пр} + t_{опр} + t_д, \text{ годин,} \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку алгоритму;

$t_в$ – тривалість вивчення технічного завдання, літературних джерел за темою тощо;

$t_а$ – тривалість розробки блок-схеми алгоритму;

$t_{пр}$ – тривалість програмування за готовою блок-схемою;

$t_{опр}$ – тривалість опрацювання обґрунтуванних рекомендацій;

$t_д$ – тривалість підготовки технічної документації.

Складові трудомісткості визначаються на підставі умовної кількості операторів Q, яка розраховується за формулою:

$$Q = q \cdot c\,(1 + p), \quad \text{штук}, \tag{3.2}$$

де q – очікувана кількість операторів;
c – коефіцієнт складності обґрунтуванних рекомендацій;
p – коефіцієнт корекції методів в процесі їх опрацювання.

Коефіцієнт складності рекомендацій c визначає відносну складність рекомендації щодо типового завдання, складність якого дорівнює одиниці.

Діапазон його зміни – 1,25…2,0.

Коефіцієнт корекції рекомендацій p визначає збільшення обсягу робіт за рахунок внесення змін в алгоритм або програму внаслідок уточнення технічного завдання. Його величина знаходиться в межах 0,05...0,1, що відповідає внесенню 3...5 корекцій і переробці 5-10% готової програми.

Для даної роботи умовна кількість операторів була розрахована за наступним даним: q = 40, c = 1,5, p = 0,07.

$$Q = 40 \cdot 1{,}5\,(1 + 0{,}07) = 64 \text{ штуки}.$$

Отже, умовна кількість операторів для даних обґрунтуванних рекомендацій дорівнює 64 штукам.

Оцінка тривалості складання технічного завдання на розробку обґрунтуванних рекомендацій $t_{тз}$ становить 16 годин.

Тривалість вивчення технічного завдання, опрацювання довідкової літератури з урахуванням уточнення ТЗ і кваліфікацію виконавця оцінюється за формулою:

$$t_в = \frac{Q \cdot B}{(75...85) \cdot k}, \quad \text{годин,} \tag{3.3}$$

де В – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, В = 1,2...1,5;

k – коефіцієнт, що враховує кваліфікацію виконавця і визначається стажем роботи за фахом.

Для даної розробки: В = 1,4; k = 1,0. Виходячи з цього тривалість вивчення технічного завдання дорівнює:

$$t_в = \frac{64,2 \cdot 1,4}{77 \cdot 1,0} = 1,17 \text{ годин.}$$

Аналогічно розраховуються наступні показники:

Тривалість розробки блок-схеми алгоритму:

$$ta = \frac{Q}{(20...25) \cdot k}, \text{ годин,} \tag{3.4}$$

$$ta = \frac{64,2}{25 \cdot 1,0} = 2,57 \text{ годин.}$$

Тривалість складання програми за готовою блок-схемою:

$$tпр = \frac{Q}{(20...25) \cdot k}, \text{ годин.,} \tag{3.5}$$

$$tпр = \frac{64,2}{25 \cdot 1,0} = 2,57 \text{ годин.}$$

Тривалість опрацювання обґрунтуванних рекомендацій:

$$tопр = \frac{1,5Q}{(4...5) \cdot k}, \text{ годин,} \tag{3.6}$$

$$tопр = \frac{1,5.64,2}{4,5 \cdot 1,0} = 21,4, \text{ годин.}$$

Тривалість підготовки технічної документації:

$$t_{Д} = \frac{Q}{(15...20) \cdot k} + \frac{Q}{(15...20)} \cdot 0,75 \qquad (3.7)$$

$$t_{Д} = \frac{64,2}{18 \cdot 1,0} + \frac{64,2}{18} \cdot 0,75 = 6,24.$$

Виходячи з отриманих даних трудомісткість створення обґрунтуванних рекомендацій дорівнює:

t = 16 + 1,17 + 2,57 + 2,57 + 21,4 + 6,24 = 49,95 годин.

3.2 Розрахунок витрат на створення обґрунтуванних рекомендацій

Витрати на створення обґрунтуваних рекомендацій Кпз складаються з витрат на заробітну плату виконавця розробки Ззп і вартості витрат машинного часу, що необхідний для опрацювання обґрунтуваних рекомендацій на ПК Змч:

$$К_{пз} = З_{зп} + З_{мч}. \qquad (3.8)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{ЗП} = t \cdot З_{пр}, \quad грн, \qquad (3.9)$$

де t – загальна тривалість створення обґрунтуванних рекомендацій, годин; t=50 годин

Зпр – средньогодинна заробітна плата виконавця з нарахуваннями, грн/годину. Зпр = 20 грн.

$$З_{зп}=49,95 \cdot 20 = 999 \text{ грн.}$$

Вартість машинного часу для налагодження обґрунтуванних рекомендацій на ПК визначається за формулою:

$$З_{мч}= t_{опр} \cdot С_{мч}+ t_{d}, \quad грн, \qquad (3.10)$$

де $t_{опр}$ – трудомісткість налагодження обґрунтуванних рекомендацій на ПК, годин;

$t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн,} \qquad (3.11)$$

де P – встановлена потужність ПК, кВт; P = 0,4 кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година, $С_е$=0,26 грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.,

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн., $К_{лпз}$ = 3000грн;

$F_р$ – річний фонд робочого часу, $F_р$ =1920.

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

Річну суму амортизації визначаємо за формулою:

$$А = \frac{С_{поч} \cdot Н_а}{100}, \text{ грн,} \qquad (3.12)$$

де $Н_а$ – річна норма амортизації на ПК, частки одиниці.

Мінімально допустимий строк корисного використання ПК складає 2 роки, тобто річна норма амортизації не має перевищувати:

$$Н_а = 1/Т_а \cdot 100\%, \quad (3.13)$$

$$Н_а = 1/2 \cdot 100\% = 50\%.$$

де $Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці. Строк дії права користування ліцензійним програмним забезпеченням не може складати менш ніж 2 роки, тобто $Н_{апз}$ не має перевищувати:

$$Н_{апз} = 1/Т_а \cdot 100\%, \quad (3.14)$$

$$Н_{апз} = 1/2 \cdot 100\% = 50\%.$$

Отже, вартість 1 години машинного часу ПК, становить:

$$С_{мч} = 0.4 \cdot 0.26 + \frac{3500 \cdot 0,5}{1920} + \frac{3000 \cdot 0,5}{1920} = 1,79 \quad \text{грн},$$

$$З_{мч} = 21.4 \cdot 1.79 + 6.24 = 44.55 \quad \text{грн}.$$

Відповідно до отриманих даних, вартість створення обґрунтуванних рекомендацій дорівнює:

$$К_{пз} = 999 + 44,55 = 1043,55, \text{ грн}.$$

Визначена таким чином вартість створення рекомендацій Кпз є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, \quad (3.16)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн. $К_{пр}$ = 6 тис. грн;

$К_{зпз}$ –вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн., $К_{зпз}$ = 3 тис. грн.;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн, $К_{аз}$ =14 тис. грн;

Розрахунок затрат наведен у таблиці 3.1

Таблиця 3.1 - Розрахунок затрат

$К_{зпз}$	Вартість	$К_{зпз}$
Windows 10	1.5 тис. грн	3 тис. грн
Windows Server 2016	1.5 тис. грн	
$К_{аз}$	Вартість	$К_{аз}$
ПК Server	8 тис. грн	14 тис. грн
ПК Server	8 тис. грн	

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн, $К_{навч}$= 2 тис. грн.;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн, $К_{н}$ = 2 тис.грн;

Відповідно до заданих даних розраховуємо капітальні витрати:

К = 6000 + 3000 + 1043,55 + 14000 + 2000 + 2000=28043 грн.

3.2 Розрахунок поточних витрат

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{ тис. грн.} \quad (3.17)$$

Витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки ($С_{в}$) не перевищують 10% від капітальних витрат : $С_{в}$=2804 грн.

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{єв} + С_{е} + С_{ел} + С_{о} + С_{тос}, \text{ грн.} \quad (3.18)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо Сн = 3000грн.

Річний фонд амортизаційних відрахувань ($С_а$) визначаються у відсотках від суми капітальних інвестицій і дорівнює:

$$С_а = (28043*50)/100=14022 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод} \text{ , грн.} \qquad (3.19)$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

$$С_з = 2000 + 200=2200 \text{ , грн.}$$

До річного фонду заробітної плати додається єдиний внесок на загальнообов'язкове державне соціальне страхування – консолідований страховий внесок, збір якого здійснюється відповідно до класів професійного ризику виробництва, до яких віднесено платників єдиного внеску, з урахуванням видів їх економічної діяльності.

Для працівників які працюють на підприємствах, у юридичних осіб – підприємцях або у фізичних осіб, що забезпечують себе роботою самостійно на умовах трудового договору встановлюється ставка єдиного соціального внеску 3,6%.

Отже, єдиний внесок дорівнює 2200*0,036=79,2 грн.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е \text{ , грн,} \quad (3.20)$$

де Р – встановлена потужність апаратури інформаційної безпеки - 0,4кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки – 1920;

$Ц_е$ – тариф на електроенергію - 0,26 грн/кВт·годин.

$$С_{ел} = 0,4 \cdot 1920 \cdot 0,26 = 199,68 \text{ грн.}$$

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу ($С_о$) не передбачаються.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначається за даними організації або у відсотках від вартості капітальних витрат (1-3%). $С_{тос}$ = 280,4 грн.

$$С_к = 3000 + 14022 + 2200 + 79,2 + 199,68 + 280,4 = 19781,28 \text{ грн.}$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) визначаються, користуючись даними про вагові частки статей витрат у сукупній вартості системи інформаційної безпеки. $С_{ак}$=12899 грн.

Отже, річні поточні витрати на функціонування системи інформаційної безпеки складають:

С =2804 + 19781,28+ 12899= 35484,28 грн.

3.3 Оцінка можливого збитку від атаки на вузол

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин; він складає 32 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин; $t_в$ = 16 годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин, $t_{ви}$= 32 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць, $З_о$ = 2500 грн;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць, $З_с$ = 2000 грн;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.) , $Ч_о$ =1;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі , $Ч_с$ =5 осіб;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин - 2000грн;

I – число атакованих вузлів – 5 штук;

N – середнє число атак на рік - 6 атак.

Упущена вигода від простою атакованого вузла становить:

$$U = П_п + П_в + V, \qquad (3.21)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_П, \quad (3.22)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

$П_п$= (5*2000)/176*32 = 1818,18 грн.

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \quad (3.23)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ви}, \quad (3.24)$$

$П_{ВИ}$= (5*2000)/176*32 = 1818,18 грн.

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_В, \text{ грн}, \quad (3.25)$$

$П_{ПВ}$=(5*2000)/176*16=909,09 грн,

$П_в$ = 1818,18 + 909,09 + 2000=4727,27 грн.

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла:

$$V = \frac{O}{F_Г} \cdot (t_П + t_В + t_{ВИ}), \text{ грн,} \qquad (3.26)$$

де $F_г$ – річний фонд часу роботи організації становить близько 2080 ч.

V = 2000/2080*(32+16+32) = 76,92 грн.

Отже, упущена вигода від простою атакованого вузла становить:

U = 1818,18 + 4727,27 + 76,92=6622,37 грн.

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації дорівнює:

$$В = \sum_i \sum_п U, \text{ грн,} \qquad (3.27)$$

В = 5*6*6622,37=198671,12 грн.

3.4 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$Е = В \cdot R – С, \text{ тис. грн,} \qquad (3.28)$$

Е = 198671,12·0,3 – 20000=39601,33 грн =39,601 тис. грн.

де В – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці, R=0,3;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

3.5 Визначення показників ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \qquad (3.29)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, тис. грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

Отже, отримуємо результат:

$$ROSI = \frac{39601.33}{28043} = 1.4.$$

Організація здійснює фінансування капітальних інвестицій у систему інформаційної безпеки за рахунок банківського кредиту, тому в якості бажаного значення $E_н$ приймається величина плати за кредит $N_{кр}$.

Проект визнається економічно доцільним, тому що виконується наступна умова: розрахункове значення коефіцієнта повернення інвестицій перевищує величину банківської кредитної ставки з урахуванням інфляції:

$$ROSI > (N_{кр} + N_{інф})/100, \qquad (3.30)$$

де $N_{кр}$ – банківська кредитна ставка = 13%;

$N_{інф}$ – річний рівень інфляції = 9,1%;

Отже, 1,4 > (13+9,1)/100 > 0,22

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \quad \text{років.} \tag{3.31}$$

За існуючими умовами, термін окупності складає один рік:

$$T_O = \frac{1}{1.4} = 0.71 рік.$$

3.6 Висновок

У даному розділі були проведені розрахунки витрат на проект системи захисту інформації. Також була визначена економічна ефективність створення обґрунтованих рекомендацій захисту інформації . Відповідно до розрахунків, виконаних в даному розділі, проект системи інформаційної безпеки є економічно доцільним, спираючись на те, що розрахункове значення коефіцієнта повернення інвестицій ROSI перевищує величину банківської кредитної ставки з урахуванням інфляції і дорівнює 1,4. Термін окупності капітальних інвестицій складає 7 місяців.

ВИСНОВКИ

Відповідно з завданням у дипломній робот визначені загрози при підключенні до інтрамережі зовнішніх користувачів.

Визначені протоколи мережевого і транспортного рівня які використовуютьс в об'єкті дослідження. Визначені методи аутентифікації в середовищі Windows Server 2016. Проаналізована можливості Windows Server 2016 с метою визначення служб і засобів, що забезпечують безпечний обмін інформацією між віддаленими користувачами і корпоративною мережею. Розроблені рекомендації щодо розгортання служб та засобів Windows Server 2016, що забезпечують реалізацію мети роботи.

Все це створює можливість віддаленого та мобільного доступу по захищеним каналом до сервісів корпоративної мережі таких як:

- Web доступ до внутрішніх і зовнішніх сайтів;
- Dial-Up доступ до корпоративної мережі;
- корпоративна електронна пошта;
- дистанційні корпоративні додатки (RemoteApps);
- віддалений доступ до сховищ даних;
- Web доступ до віддалених робочих столів (термінальний сервіс);
- Web доступ до віртуальних робочих столів (HiperV);
- доступ до файлових серверів по VPN

із шифруванням трафіка на всіх етапах передачі інформації В економічному розділі визначені витрати на необхідну техніку і ПЗ для реалізації проекту та ефект від його впровадження.

На підставі проведеного аналізу економічної ефективності впровадження розробки, можна зробити наступні висновки:

1. Розробка є актуальною на ринку інформаційних технологій;

2. Розробка забезпечує високий рівень безпеки інтрамережі підприємства при підключення віддалених і мобільних користувачів.

ПЕРЕЛІК ПОСИЛАНЬ

1 Raina K, PKI Security Solutions for Enterprise: Solving HIPAA, E-Paper Act and Other Compliance Issues.: Wiley Publishing Inc., 2009.

2 RFC2559 LDAP V2 Operational Protocols.

3 Горбатов В.С., Полянская О.Ю. Основы технологии PKI. М.: Горячая линия − Телеком, 2003.

4 CCITT. Recommendation X.800: Security Architecture for Open Systems Interconnection for CCITT Applications. Geneva, 1991.

5 Kiran S., Lareau P., Lloyd S. PKI Basics − A Technical Introduction // A PKI Forum Note. November 2002.

6 Adams C., Lloyd S. Understanding PKI. Concepts, Standards and Deployment Consideration. Second Edition. Addison-Wesley, 2003.

7 Кадощук И. Как нам организовать PKI // Сетевой журнал − 2000 − № 9.

8 Kuhn D.R., Hu Vincent C., Polk W.T, Chang Shu-Jen. Introduction to Public Key Technology and the Federal PKI Infrastructure // National Institute of Standards and Technology − February, 2001.

9 RFC2527. Certificate Policy and Certification Practices Framework.

10 Jarupunphol P., Mitchell C. PKI implementation issues in B2B e-commerce EICAR // Conference Best Paper Proceedings, 2003.

11 Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security. − М.: Бином-Пресс, 2002.

12 Рапоза Д. Незнакомая PKI, PC Week/RE, январь 2001.

13 SET Secure Electronic Transaction. Specification. Book 3: Formal Protocol Definition. May 31, 1997.

14 Security Service API: Cryptographic API Recommendation Second Edition, NSA Cross Organization CAPI Team July 1, 1996.

15 PKCS#11 Cryptographic Token Interface (Cryptoki).

16 PKI Interoperability Framework. PKI Forum White Paper.

17 Extensible Markup Language (XML) 1.0 (Third Edition).

18 OASIS Security Services (Security Assertion Markup Language − SAML) TC.

19 XML Key Management Specification (XKMS 2.0).

20 Raina K, PKI Security Solutions for Enterprise: Solving HIPAA, E-Paper Act and Other Compliance Issues.: Wiley Publishing Inc., 2003.

21 Татарчук М.І. Корпоративні інформаційні системи. Навчальний посібник. – К.: КНЕУ, 2005. – 291 с.

22 Ричард Э. Смит. Аутентификация: от паролей до открытых ключей – СПб., 2002. – 370-371 с

23 Моримото, Рэнд, Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Microsoft Windows Server 2016. Полное руководство. : Пер. с англ. — М. ,2017. — 1456 с.

24 Управление сертификатами (Электрон. Ресурс)/Способ доступа: URL: http://technet.microsoft.com/ru-ru/library/cc771377%28WS.10%29.aspx - Загол. з екрану.

25 Шаблоны сертификатов (Электрон. Ресурс)/Способ доступа: URL: http://technet.microsoft.com/ru-u/library/cc730705%28WS.10%29.aspx - Загол. з екрану.

26 Обзор PKI предприятия (Электрон. Ресурс)/Способ доступа: URL: http://technet.microsoft.com/ru-u/library/cc771026%28WS.10%29.aspx - Загол. з екрану.

27 DocOnline. Независимый портал о СЭД (Електрон. ресурс)/Спосіб доступу: URL: http://www.doc-online.ru. – Загол. з екрана.

28 Мировой рынок систем електронного документооборота (Електрон. ресурс) /Спосіб доступу: URL: http://www.citforum.ru/ – Загол. з екрану.

29 Внедрение систем электронного документооборота: проблемы и решения (Електрон.ресурс) /Спосіб доступу: URL: http://www. iteam.ru/ – Загол. з екрану.

30 Ефимов А.Н. Программа для ЭВМ как объект гражданского оборота. Московский оценщик °1, 1999

31 Федотова М.А. Сколько стоит бизнес? Методы оценки, М. Перспектива 1996.

32 Долин П.А. Справочник по технике безопасности. М.: Энергоиздат, 1982. – 800 с.

33 Методичні вказівки до виконання дипломного проекту для студентів з напряму підготовки 1701 „Електротехніка / Укл. І.В. Шереметьєва, Л.В. Тимошенко.-Дніпропетровськ: НГА України, 2001.- 32 с.

34 Методичні вказівки з виконання розрахунково частини розділу "Охорона праці в дипломних проектах студентів інституту електроенергетики. Частина І / Уклад: В.І. Голінько, В.Ю. Фрундін, Я.Я. Лебедев, В.С. Колесник , Дніропетровськ: Національний гірничий університет. - 2004. - 32 с.

35 Стандарт вищого навчального закладу. Кваліфікаційні роботи випускників. Загальні вимоги до дипломних проектів і дипломних робіт./ Упорядн.: В. О. Салов, О. М. Кузьменко, В. І. Прокопенко.- Дніпропетровськ: НГУ, 2002.- 52 с.

36 Мєшков В.І. Загальні вимоги до оформлення магістерських дипломних робіт і дипломних проектів спеціалістів для студентів галузей знань 1701 «Інформаційна безпека» та 0509 «Радіотехніка, радіоелектронні апарата та зв'язок». Методичні вказівки. − Д.: Державний ВНЗ «Національний гірничий університет». 2013. − 32 с.

ДОДАТОК А. ПЕРЕЛІК МАТЕРІАЛІВ ДИПЛОМНОЇ РОБОТИ

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат		
2	А4	Список умовних скорочень		
3	А4	Зміст		
4	А4	Вступ		
5	А4	Розділ 1		
6	А4	Розділ 2		
7	А4	Розділ 3		
8	А4	Висновки		
9	А4	Перелік посилань		
10	А4	Додаток А		
11	А4	Додаток Б		
12	А4	Додаток В		
13	А4	Додаток Г		

ДОДАТОК Б. КОПІЯ ТЕЗ ДОПОВІДІ

Ткачик О.С. студент гр. 125м-17-2
Науковий керівник: Флоров С.В., к.т.н., доцент кафедри безпеки інформації та телекомунікацій
(*Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна*)

ВІДДАЛЕНЕ УПРАВЛІННЯ ІНФОРМАЦІЄЮ У КОРПОРАТИВНИХ МОБІЛЬНИХ ПРИСТРОЯХ

Інформація та підтримують її інформаційні системи є цінними виробничими ресурсами організації. Їх доступність, цілісність та конфіденційність можуть мати особливе значення для забезпечення працездатності підприємства. З розвитком сучасних засобів мобільного зв'язку і збільшенням зони покриття операторами, мобільні пристрої і мобільні користувачі стають невід'ємною частиною корпоративних мереж Організації стикаються зі зростаючою загрозою порушення режиму безпеки, що виходить від цілого ряду джерел. Для кожної конкретної інформаційної системи політика безпеки повинна бути індивідуальною. Вона залежить від технології і способів обробки інформації, використовуваних програмних і технічних засобів, архітектури локальної мережі, структури організації та виду її діяльності, а також інших факторів. Інформаційних систем і мереж можуть загрожувати такі небезпеки, як комп'ютерне шахрайство, шпигунство, саботаж, вандалізм, а також інші джерела відмов і аварій..

Згідно [1], найбільш актуальними для корпоративних интрасетей використовують мобільні пристрої, є наступні фактори:

- Різке збільшення віддалених мобільних користувачів корпоративних интрасетей, що використовують технології Wi-Fi, GPRS, 3G, 4G.
- У користувачів корпоративних інформаційних систем з'явилися мобільні пристрої нового покоління (iPhone, iPad, Android, Windows 10), що істотно підвищило ймовірність несанкціонованого доступу в интрасеть підприємства за рахунок втрати контролю користувача над мобільним пристроєм.
- Поява технологій і обладнання, що дозволяють перехопити і дешифрувати трафік від віддаленого користувача в интрасеть підприємства.
- У зв'язку з цим виникла необхідність в захисті трафіку від мобільних пристроїв до локальної мережі підприємства.
- Виникла необхідність в централізованому управлінні доступом до web-сервісів интрамережі підприємства при виникненні підозри про зміну його власника або компрометації пароля шифрування. Увімкнувши служби шифрування Office 365, з’являється можливість шифрувати переписку з сторонніми користувачами. Адміністратори можуть задавати алгоритми шифрування і підписування документів.
- Надання доступу користувачам. Послуги Office 365 захищаються на наступних рівнях: ЦОД, мережевий, логічний, рівень зберігання та передачі. Office 365 інтегрується з локальної службою каталогів Active Directory і іншими системами зберігання і ідентифікації каталогів.

Одним з ефективних варіантів розв'язання проблеми є:

1. Розгортання інфраструктури відкритого ключа в інтрамережі підприємства.

2. Отримання та встановлення сертифікатів на мобільні пристрої користувачів корпоративної інтрамережі.
3. Забезпечення віддаленого управління інформацією в разі втрати контролю користувача над мобільним пристроєм.
4. Розробка програмного забезпечення, що дозволяє встановлювати сертифікати на мобільні пристрої користувачів.
5. Розгортання в домені підприємства служби Mobile Administration Web tool, що дозволяє блокувати інформацію на на мобільних пристроях при виникненні підозри у втраті контролю.

В корпоративних мережах під керуванням Windows управління функцією дистанційного стирання пам'яті, виконуваної пакетом Messaging and Security Feature Pack, здійснюється за допомогою інструменту веб-адміністрування ActiveSync Mobile Administrative Web Tool. Цей інструмент дозволяє управляти процедурою дистанційного стирання пам'яті загублених, вкрадених або іншим чином потрапили в чужі руки мобільних пристроїв, підключених до серверів по бездротових з'єднань.

При гібридному способи розгортання корпоративної мережі необхідно використовувати хмарний сервіс Mobile Device Management який дозволяє взяти під контроль мобільні пристрої співробітників.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Моримото, Рэнд, Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Microsoft Windows Server 2016. Полное руководство. : Пер. с англ. — М. ,2017. — 1456 2.
2. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. Утверждено приказом Департамента специальных телекоммуникационных систем и защиты информации Службы безопасности Украины от 28 апреля 1999 г. № 22. // Официальный сайт Службы безопасности Украины. Способ доступа: URL: http: // www.dstszi.gov.ua/.
3. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» (Электрон. ресурс)/Способ доступа: URL: http://www.dstszi.gov.ua/dstszi
4. ISO/IEC 27005:2005 «Інформаційні технологій. Методи захисту. Система управління інформаційною безпекою. Вимоги» (Электрон. Ресурс)/Способ доступа: URL: http://www.dstszi.gov.ua/dstszi/control
5. MDM Migration Analysis Tool/(Електрон. ресурс)/Способ доступа: URL: https://www.microsoft.com/enus/download/details.aspx?id=7887&fa43d42b-25b5-4a42-fe9b-1634f450f5ee=True

ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

ДОДАТОК Г. ВІДГУК НА МАГІСТЕРСЬКУ ДИПЛОМНУ РОБОТУ

на тему:

Розробка рекомендацій щодо захисту інформації в корпоративній мережі на платформі Windows Server 2016 при взаємодії з мобільними користувачами студента групи 125м-17-2 Ткачика Олексія Сергійовича.

Дипломна робота за спеціальністю 125 «Кібербезпека» Ткачика О.С представлена пояснювальною запискою на стор., містить рис., табл., додатка, джерела.

Об'єкт дослідження: Корпоративна комп'ютерна мережа третього класу на платформі Windows Server 2016.

Мета дипломної роботи: на підставі аналізу можливостей Windows Server 2016 і протоколів, що використовуються в об'єкті дослідження, розробити рекомендації з вибору методу аутентифікації зовнішніх та мобільних користувачів та процедуру розгортання служб та засобів Windows Server 2016 забезпечують безпечний обмін інформацією.

У спеціальній частині запропонована архітектура взаємодії зовнішніх та мобыльних користувачів з інтрамережею підприємства, визначені загрози при підключенні мобільних користувачів.

Наукова новизна полягає в розроблці рекомендацій щодо розгортання служб, засобів і методів аутентифікації в середовищі Windows Server 2016.

В економічному розділі виконаний розрахунок економічної ефективності запропонованих рішень.

В якості недоліків слід відзначити наступне: недотримання графіка проведення розробки, нечіткість окремих висновків і визначень.

В цілому дипломна робота виконано у відповідності до вимог, які пред’являються до дипломних робіт магістра і заслуговує оцінки "добре", а Ткачик Олексій Сергійович присвоєння йому кваліфікації професіонала із організації інформаційної безпеки.

Керівник роботи к.т.н., доц. Флоров С.В.