Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

напрям підготовки *125 Кібербезпека*
(код і назва напряму підготовки)

спеціальність *Кібербезпека*
(код і назва спеціальності)

освітній рівень *магістр*
(назва освітнього рівня)

кваліфікація *Професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Дослідження захисту інформації в корпоративній мережі при взаємодії з мобільними користувачами***

Виконавець: студент 6 курсу, групи 125м-16-1

Старченко Олег Олегович
(підпис) (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	к.т.н., доц. Флоров С.В.		
розділів:			
спеціальний	к.т.н., доц. Флоров С.В.		
економічний	к.е.н., доц. Волотковская Ю.А.		
Рецензент			
Нормоконтроль	к.т.н., доц. Галушко О.М.		

Дніпро 2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій

д.т.н., проф_____Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

спеціальності *Кібербезпека*
(код і назва спеціальності)

студенту 125м-16-1 Старченко Олег Олегович
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***«Дослідження захисту інформації в корпоративній мережі при взаємодії з мобільними користувачами»***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від «____» _____ №_____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***Безпека інформації, що передається зберігається та оброблюється при використанні мобільних пристроїв.***

Предмет досліджень ***Методи забезпечення інформаційної безпеки при використанні мобільних пристроїв.***

Мета НДР ***Підвищення інформаційної безпеки підприємств де кінцевий користувач має доступ і обробляє корпоративну інформацію за допомогою мобільних пристроїв.***

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

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна ***полягає в розробці вимог до хмарних сервісів, що забезпечують безпечний обмін інформацією з мобільними користувачами корпоративних мереж.***

Практична цінність ***отримані результати можуть бути використані для подальшого поліпшення бізнес процесів підприємства при одночасному підвищенні рівня захисту інформаційних активів.***

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 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

Результати досліджень мають бути подані у вигляді, що дозволяє безпосереднє використання для створення засобів захисту інформації в корпоративній мережі при взаємодії з мобільними користувачами.

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
1 Визначити вимоги до послуг, що надаються мобільним користувачам в сучасних корпоративних мережах	«11» вересня 2017 р.
2 Визначити засоби і методи автентифікації що забезпечують безпечний обмін інформацією між мобільними користувачами і корпоративною мережею	«22» жовтня 2017 р.
3 Побудувати модель загроз для підприємства, де використовують технологію хмарних обчислень	«2» листопада 2017 р.
4 Розробити гібридну архітектуру мережі підприємства що використовує хмарні технології для керування пристроями та обліковими записами мобільних користувачів	«28» листопада 2017 р.
5 Розробити рекомендації створення захищенної інформаційно-комунікаційної системи підприємства, що	«24» грудня 2017 р.

має мобільних користувачів корпоративних мереж	
6 Оформлення пояснювальної записки дипломної роботи	«10» січня 2018 р.

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***від реалізації результатів роботи очікується завдяки поліпшення бізнес процесів підприємства при одночасному підвищенні рівня захисту інформаційних активів.***

Соціальний ефект ***від реалізації результатів роботи очікується позитивним завдяки створенню умов для реалізації можливостей працівникам 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 видав _____ С.В. Флоров
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ О.О Старченко
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ДЕК _____

РЕФЕРАТ

Пояснювальна записка: 112 с., 1 рис., 5табл., 4 додатка, 53 джерела.

Об'єкт дослідження: безпека інформації, що передається, зберігається та оброблюється при використанні мобільних пристроїв.

Предмет досліджень: методи забезпечення інформаційної безпеки при використанні мобільних пристроїв. Ідея роботи: використання новітніх хмарних криптографічних технологій для забезпечення безпечного обміну інформації з мобільними користувачами корпоративних мереж

Мета дипломної роботи: підвищення інформаційної безпеки підприємств, де кінцевий користувач має доступ і обробляє корпоративну інформацію за допомогою мобільних пристроїв

Наукова новизна полягає в дослідженні методів забезпечення інформаційної безпеки на підприємствах, де використовуються мобільні пристрої для роботи з інформаційними активами підприємства.

Практичне значення полягає в дослідженні ефективності протидії загрозам несанкціонованого доступу до корпоративної інформації, яка оброблюється за допомогою мобільних пристроїв

У спеціальній частині переглянута архітектура взаємодії мобільних користувачів з інтрамережею підприємства, визначені загрози при підключенні мобільних користувачів, розроблені рекомендації щодо побудови гібридної інформаційно-комунікаційної системи з мобільними користувачами .

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

Напрямки подальших досліджень полягають у детальному аналізі існуючої нормативно-правової бази України і світу, стосовно застосування хмарних технологій для керування мобільними пристроями.

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ЛОКАЛЬНА ОБЧИСЛЮВАЛЬНА МЕРЕЖА, ХМАРНІ ТЕХНОЛОГІЇ, МОБІЛЬНИЙ КОРИСТУВАЧ, МОБІЛЬНІ ПРИСТРОЇ

РЕФЕРАТ

Пояснительная записка: 112 с., 1 рис., 5 табл., 4 приложения, 53 источника.

Объект исследования: безопасность передаваемой информации, хранимой и обрабатываемой при использовании мобильных устройств. Предмет исследований: методы обеспечения информационной безопасности при использовании мобильных устройств. Идея работы: использование новейших облачных криптографических технологий для обеспечения безопасного обмена информацией с мобильными пользователями корпоративных сетей. Цель дипломной работы: повышение информационной безопасности предприятий, где конечный пользователь имеет доступ и обрабатывает корпоративную информацию с помощью мобильных устройств

Научная новизна заключается в исследовании методов обеспечения информационной безопасности на предприятиях, где используются мобильные устройства для работы с информационными активами предприятия. Практическое значение состоит в исследовании эффективности противодействия угрозам несанкционированного доступа к корпоративной информации, которая обрабатывается с помощью мобильных устройств

В специальной части пересмотрена архитектура взаимодействия мобильных пользователей с интрасети предприятия, определенные угрозы при подключении мобильных пользователей, разработаны рекомендации по построению гибридной информационно-коммуникационной системы с мобильными пользователями. В экономическом разделе выполнен расчет экономической эффективности создания обоснованных рекомендаций защиты информации.

Направления дальнейших исследований заключаются в детальном анализе существующей нормативно-правовой базы Украины и мира, о применении облачных технологий для управления мобильными устройствами.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ОБЛАЧНЫЕ ТЕХНОЛОГИИ, МОБИЛЬНЫЕ ПОЛЬЗОВАТЕЛИ, МОБИЛЬНЫЕ УСТРОЙСТВА

THE ABSTRACT

Explanatory note: 112 p., 1 fig., 5 table ., 4 applications. 53 of the source.

Object of research: the security of the information transmitted stored and processed when using mobile devices.

Subject of research: methods of providing information security in the use of mobile devices

The idea of work: the use of the latest cloud cryptographic technologies to ensure the secure exchange of information with mobile users of corporate networks

The purpose of the thesis is to increase the information security of enterprises where the end user has access and processes corporate information using mobile devices.

The scientific novelty consists in researching the methods of providing information security at enterprises where mobile devices are used for work with information assets of the enterprise.

The practical significance is to investigate the effectiveness of counteracting the threats of unauthorized access to corporate information that is handled by mobile devices.

In the special part the architecture of interaction of mobile users from the intranet of the enterprise was reviewed, certain threats were encountered when connecting mobile users, recommendations for the construction of a hybrid information and communication system with mobile users were developed.

In the economic section, the calculation of the economic effectiveness of creating reasonable recommendations for the protection of information.

The directions of further research are in the detailed analysis of the existing regulatory framework of Ukraine and the world, on the application of cloud technologies for the management of mobile devices.

INFORMATION PROTECTION SYSTEM, LAN, COMPUTER TECHNOLOGIES, MOBILE USERS, MOBILE DEVICES

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

ЗМІСТ

ВСТУП

Доволі великий відсоток коштів підприємства та організації використовують на експлуатацію та технічне обслуговування локальних інформаційних систем, розробки та випуску програмних продуктів щоб збільшити ефективності праці підприємства шляхом організації прозорого документообігу та спільної праці над проектами.

З розвитком сучасних засобів мобільного зв'язку і збільшенням зони покриття операторами, мобільні пристрої і мобільні користувачі стають невід'ємною частиною корпоративних, реалізуючи сценарій «Візьми з собою свій власний пристрій» . 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 вживе заходів по захисту своїх інформаційних систем, тим більш дешевими й ефективними вони будуть для неї згодом.

Інформаційно-комунікаційна система 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 доступу до ресурсів корпоративної мережі мобільних користувачів.

РОЗДІЛ 1. ПОЛІТИКА БЕЗПЕКИ ПІДПРИЄМСТВА З МОБІЛЬНИМИ КОРИСТУВАЧАМИ

1.1 Вимоги до системи безпеки підприємства що мають у своєму складі мобільних користувачів

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.[14]

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 відповідальностей , 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 рубежі, 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.

1.2 Вимоги до служб, технологій та ролі сучасних операційних систем для мобільних корпоративних користувачів

Через те, що робочі ресурси в організації стають все більш і більш мобільними, в сучасні операційні системи 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 Windows 7 [7]. Після цього доступ до мережевих ресурсів істотно спрощується, де б користувачі не знаходились

Технологія DirectAccess в сучасних операційних системах є . одним з найбільш значних поліпшень, що стосуються мобільного доступу. Ця технологія надає віддаленому користувачеві можливість отримувати доступ до мережевих ресурсів, таким як загальні файлові ресурси, корпоративні додатки і т.п., без підключення до віртуальної приватної мережі (VPN).

Це 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.

Перше. Наявність 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. Крім того технологія DirectAccess працює тільки з певними клієнтами, наприклад 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 додатксів), 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.

Друге. Протокол IPv6. 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, сучасні

клієнтські і серверні операційні системи повністю 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.

Третє. Технологія Mobile Broadband, що підтримує пристрої мобільного широкосмугового зв'язку. Вона являє собою оновлену технологію для пристроїв і служб, які використовуються в роботі мобільних широкосмугових мереж (подібних AT & T, Sprint і Verizon).

Наприклад у Windows 7 за умови встановлення новітніх драйверів Mobile Brand як для пристроїв, так і для Windows, вставка карт Mobile Broadband в мобільну систему автоатично 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 подключенні адаптера Mobile Broadband тепер автоматично проводиться підключення користувача до Інтернету. При відключенні адаптера Mobile Broadband від системи Windows 7 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.

Четверте. Підтримка філій. До складу сучасних операційних систем 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 (напрікладWindows Server 2012 R2) 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 сучасних операційних серверних системах відносяться 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.

П’яте. Використання технології BitLocker для захисту сервера. Технологія BitLocker надає організує ціям можливість виконувати шифрування цілих розділів дисків з усіма що зберігаються на них файлами, документами і даними. Коли вона була вперше запропонована для серверних платформ було важко зрозуміти, навіщо може вимагатися шифрування дискового тому на сервері. Шифрувати вміст ноутбука, планшета або смартфона подібним методом мало сенс на випадок його крадіжки (щоб ніхто зміг отримати доступ до зберігаються на його жорсткому диску даними).[5]

Однак якщо подумати про тих серверах, які розміщуються у віддалених місцях і часто не в заблокованій серверної стійці 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 средах більшість. Технологія BitLocker дозволяє шифрувати все томи серверів і є надійним рішенням для організацій, що турбуються про можливу фізичну крадіжку даних з сервера

Шосте. Розподілене адміністрування. У віддалених або дочірніх офісах, в яких присутен 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.

Сучасні серверні платформи поставляють набір прав, який спеціально призначений для адміністраторів віддалених сайтів і дочірніх офісів. Це дає можливість вносити зміни, що стосуються тільки конкретного дочірнього офісу. Дана можливість, разом з усіма іншими засобами призначеними для дочірніх і віддалених офісів, забезпечити більш якісне IT-обслуговування в організаціях з багатьма офісами.

Сьоме. Роль Remote Desktop Services для тонких клієнтів. Напимклад у Windows Server 2012 R2 в 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 для приведення базової конфігурації Terminal Services в робочий стан потрібно встановлювати додаткові сторонні додатки, то в складу Windows Server 2012R2 входять всі необхідні технології.. 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.

Восьме. Роль Remote Desktop Services Web Access. 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 вебсторінці, 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.

Недоліком Remote Desktop Services Web Access як і раніше потрібно, щоб клієнтська або серверна система функціонувала під управлінням. Отримати доступ до Remote Desktop Services Web Access з браузера в системах Apple Macintosh і Linux неможливо. 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 2008 R2 Remote Desktop Services [3], 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 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: / /),

Дев'яте. Роль 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 офісні додатки, 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. Завдяки додаванню в компонент політик можливості визначати місцезнаходження в мережі 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.

Десяте. Роль Remote Desktop Services Connection Broker. (Сервіс обслуговання інфраструктури 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. Так наприкладWindows Server 2012 R2 VDI підтримує два різних режими: режим особистого робочого столу (Personalized Desktop) і режим пулу робочих столів (Pooled Desktop).[3] 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). 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 2008 R2 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.

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.

1.3 Вимоги до автентифікація в корпоративній мережі

В системі автентифікації зазвичай можна виділити кілька елементів:

- суб'єкт, який буде проходити процедуру автентифікації;
- характеристика суб'єкта - відмінна риса;
- господар системи аутентифікації, що несе відповідальність і контролює її роботу;
- сам механізм автентифікації, тобто принцип роботи системи;
- механізм, який надає або позбавляє суб'єкта певних прав доступу;[2]

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 автентифікації:

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 криптоаналіз).

2. Щось, що ми маємо - пристрій автентифікації. 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 автентифікації, 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 автентифікації. 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.

Автентифікація по багаторазовим паролів. Один із способів автентифікації 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.[2] Достовірна (еталонна) пара логін-пароль зберігається в спеціальній базі даних. Проста автентифікація має такий загальний алгоритм:

– суб'єкт запитує доступ до системи і вводить особистий ідентифікатор та пароль;

– ведені унікальні дані надходять на сервер автентифікації, де порівнюютьс з еталонними;

– при збігу даних з еталонними, автентифікація 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 криптографічно 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 хешірованних образ зберігаються на сервері автентифікації. 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 / passwd, 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.

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. Автентифікація 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.

Останнім часом все частіше застосовується, так звана, розширена або багатофакторна автентифікація. Вона побудована на спільному використанні декількох факторів автентифікації. 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 автентифікації необхідно перш за все відштовхуватися від необхідного ступеня захищеності, вартості побудови системи, забезпечення мобільності суб'єкта.

У таблиці 1.1 наведено порівняння методів автентифікації по критерію ризику.

Таблиця 1.1 - Порівняння методів аутентифікації по критерію ризику

Рівень ризику	Вимоги до системи	Технологія аутентифікації	Приклади застосування
Низький	Потрібно здійснити аутентифікацію	Рекомендується мінімальна вимога	Реєстрація на порталі в

	для доступу до системи, причому крадіжка, злом, розголошення конфіденційної інформації не матиме значних наслідків	використання багаторазових паролів	мережі Інтернет
Середній	Потрібно здійснити аутенифікацію для доступу до системи, причому крадіжка, злом, розголошення конфіденційної інформації заподіє невеликий збиток	Рекомендується мінімальна вимога - використання одноразових паролів	Проведення суб'єктом банківських операцій
Високий	Потрібно здійснити аутентифікацію для доступу до системи, причому крадіжка, лом, розголошення конфіденційної інформації завдасть значної шкоди	Рекомендується мінімальна вимога - використання багатофакторної аутентифікації	Проведення великий міжбанківськ их операцій керівним апаратом

1.4 Протоколи автентифікації мобільних користувачів

З точки зору інформаційної безпеки будь-якої віддалений користувач дповинен 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 LDAP 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. [2]

У сучасних серверних платформах реалізована підтримка наступних протоколів:

- протокол RADIUS (Remote Authentication Dial-In User Service);
- протокол EAP (Extensible Authentication Protocol);
- 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

Протокол автентифікації Remote Authentication Dial-in User Service (RADIUS) розглядається як механізм автентифікації 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), що забезпечує централізоване управління аутентифікацією, авторизацією і аудитом доступу на підставі інформації про користувачів, одержуваної від контроллеров домена.[3]

В рамках стандарту виділяються три компоненти протоколу:

- клієнт RADIUS. Клієнт RADIUS приймає від користувачів запити на автентифікацію. 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. При цьому в залежності від реалізації сервера RADIUS для перевірки автентичності використовуються різні бази даних облікових записів. Реалізований врамках 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 онможет використовуватися для організації процесу автентифікації в гетерогенних мережах. Так, наприклад, для автентифікації 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 2008R2 в рамках Служби перевірки автентичності в Інтернеті (Internet Authentication Service, IAS). Ця служба позиціонується як механізм централізованной

автентифікації та авторизації користувачів, використовують різні способи підключень до мережі. Служба IAS інтегрована з іншими;

– базовими службами Windows Server 2008R2, такими як служба маршрутизації та віддаленого доступу та служба каталогу Active Directory. Служба маршругізації 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 (безпроводовий доступ, комутовані підключення, а також VPN-підключення). Підтримка цього протоколу реалізована на багатьох сучасних платформах, що дозволяє використовувати його в міжплатформних рішеннях;

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 автентифікації (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

аутентіфікації, 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 аутентифицирующей інформації та відповідних відповідей кліента. Наприклад, якщо EAP використовується спільно зі смарт-картами, сервер удаленного доступу може окремо запросити у клієнта віддаленого доступа 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 2008 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 автентифікації. Необхідно, однак, пам'ятати про те, що для успішної автентифікації відповідний модуль повинен бути підключений як на сервері віддаленого доступу, так і на клієнті віддаленого доступу.[3]

Крім того 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 автентифікації. При цьому інфраструктура RADIUS може бути використана для передачі повідомлень протоколу EAP.

Щоб забезпечити перевірку справжності на базі EAP, необхідно:

– дозволити EAP як протокол автентифікації 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.

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 механизмів взаємної аутентифікації всіх учасників з'єднання.

Протокол автентифікації CHAP є стандартом Інтернету (RFC 1994) і підтримується безліччю виробників програмного забезпечення. У середовищі корпоративних мереж протокол CHAP може бути використаний для автентифікації клієнтів віддаленого доступу сторонніх виробників.

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.

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 кліент 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.[2] У середовищі корпоративних мереж 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).

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.[6]

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.

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 2008R2 Certificate Services, генерують сертифікати X.509 для використання клієнтами, що розпізнають формати S/MIME.

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 автентифікацію Kerberos для своїх транзакцій, додатки повинні зробити кілька звертань до бібліотек Kerberos.

Процес автентифікації складається з обміну необхідними повідомленнями із сервером автентифікації 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:

– одержання й установка сертифіката сервера;

– підтвердження установки;

– створення резервної копії сертифіката сервера;

– включення SSL для віртуальних каталогів IIS 8.0.

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 2008R2: 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.

1.5 Методи автентифікації при гібридної архітектурі

Сучасне покоління сучасних міжмережевих екранів надає наступні нові можливості аутентифікації [1]:

– Single Sign On (SSO), в якому користувач проходе одноразову аутентифікацію і може отримати доступ до будь якої кількості серверів, які знаходяться за міжмережевим екраном;

– двухфакторная аутентифікація з використанням аутентифікації на основі форм і клієнтських сертифікатів;

– справжності на основі форм підтримки для публікації будь-який веб-сервер;

– настроювані форми для аутентифікації на основі форм і форм для мобільних клієнтів, а також використання для кожного користувача-агента схеми аутентифікації;

– резервні з аутентифікацією на основі форм для звичайної перевірки автентичності, для не-браузер клієнта;

– релегування повноважень з використанням NTLM або Kerberos аутентифікацію;

– обмежене делегування;

– кешування повноважень;

– управління паролями, в яких сучасне покоління міжмережевих екранів може перевірити стан облікового запису користувача і повідомляє про це

користувачеві. Ця функція також може бути налаштований, щоб дозволити користувачам змінювати свої паролі:

– Secure Sockets Layer (SSL) обмеження клієнтських сертифікатів;

– можливість призначати різні цифрові сертифікати для кожного IP-адресу мережного адаптера;

– аутентифікацію на основі форм: ім'я користувача пароль / пароль, де пароль використовується для аутентифікації на міжмережевому екранів і пароль для аутентифікації що використовується делегаційно;

– підтримка служби каталогів аутентифікації з використанням Lightweight Directory Access Protocol (LDAP), що дозволяє активізувати аутентифікаційний каталог, коли міжмережевий екран входить в робочу групу, крім тих, що містяться на рахунках користувачів. Також підтримує кілька конфігурацій , в якому користувач може бути перевірен на інший набір LDAP-серверів.

– одноразовий пароль при підтримці віддаленого Dial-In User Service аутентифікації (RADIUS).

– за замовчуванням блокування делегування перевірки автентичності.

Single Sign On (SSO) дозволяє користувачам аутентифіцироватися один раз, і потім отримати доступ до всіх веб-сервера з тим же суфікс домену, що міжмережевий екран публікує на конкретний порт слухача, без повторной аутентификации.

Типовим прикладом є SSO користувач, який входить в Outlook Web Access, надання повноважень на формі. В одному з повідомлень електронної пошти, які користувач отримує, посилання на документ, який зберігається в

SharePoint Portal Server. Користувач натискає на посилання, і документ відкривається без додаткового запиту для перевірки автентичності. Цей приклад заснований на використанні стійких файлах куки.

Двофакторна автентифікація забезпечує підвищену безпеку, оскільки вона вимагає, щоб користувач відповідати двом критеріям аутентифікації: ім'я користувача / пароль, і знак або сертифікат, відомий як те, що ви маєте, то ви знаєте. Міжмережевий екран підтримує двухфакторную автентифікацію в наступних випадках:

- користувач має сертифікат;
- користувач має SecurID токен, що являє собою код доступу;
- користувач має одноразовий пароль токен, що являє собою код доступу.

Типовим прикладом двофакторної автентифікації з сертифікатом є використання смарт-карт. Смарт-карта містить сертифікат, який може перевірити на сервер, який містить ім'я користувача та відомості про сертифікат. Порівнюючи інформацію про користувача (ім'я користувача і пароль) до сертифікату за умови, сервер перевіряє повноваження і міжмережевий екран перевіряє справжність користувача. Двофакторна автентифікація з використанням сертифіката клієнта як правило не підтримується в форматі робочої групи.

Звичайна перевірка автентичності - широко застосовуваний метод, який полягає в зборі таких відомостей, як ім'я користувача і пароль. При звичайній перевірці достовірності відомостей про користувача відправляють та отримують у вигляді текстових символів, які можна прочитати. Хоча паролі і імена користувачів підлягають шифруванню, при звичайній перевірці достовірності шифрування не використовується. Користувачеві пропонується ввести ім'я та пароль для входу в обліковий запис корпоративної мережі.Міжмережевий екран отримує HTTP-запит з обліковими даними користувача і підтверджує їх за допомогою певного сервера перевірки

справжності (RADIUS або LDAP-сервер). Для вихідних запитів веб-проксі екран підтверджує облікові дані користувача і потім визначає правила доступу. Для вхідних запитів екран використовує облікові дані для перевірки справжності на опублікованому веб-сервері відповідно до налаштованим методом делегування. Веб-сервер повинен бути налаштований на використання схеми перевірки справжності, яка відповідає методу делегування, використовуваному екраном. Текстовий пароль кодується за допомогою Base64 до відправки по мережі, однак це не шифрування, і якщо пароль буде перехоплений в мережі аналізатором мережевих пакетів, неавторизовані користувачі можуть розкодувати і повторно використовувати пароль.

Перевага звичайної перевірки автентичності полягає в тому, що вона підтримується практично всіма HTTP-клієнтами. Недоліком є те, що при використанні звичайної перевірки автентичності веб-оглядачі передають паролі в незашифрованому вигляді. Спостерігаючи за діями користувача в мережі, зломщик або користувач-зловмисник може перехопити і розкодувати паролі за допомогою загальнодоступних засобів. Тому не рекомендується використовувати звичайну перевірку справжності, якщо користувач не впевнений, що зв'язок захищена, наприклад, при користуванні виділеною лінією або з'єднанням по SSL-протоколу [2].

Перевірка справжності Digest та Wdigest. Дайджест-перевірка справжності пропонує такі ж можливості, як і звичайна перевірка автентичності, але відрізняється більш захищеним способом передачі облікових даних. Перевірка справжності дайджест використовує протокол HTTP 1.1 згідно з визначенням RFC 2617.

Цей протокол підтримується не всіма браузерами. Якщо оглядач, не підтримує протокол HTTP 1.1, запитує файл при включеній перевірці достовірності Digest, запит відхиляється. Перевірка справжності Digest може використовуватися тільки в доменах Windows.

Дайджест-перевірка справжності успішно застосована, якщо на контролері домену в доменній службі Active Directory зберігається оборотна зашифрована (текстова) копія запиту пароля користувача. Щоб дозволити зберігання паролів в незашифрованому текстовому вигляді, необхідно в доменній службі Active Directory активувати настройку Зберігати пароль з використанням оборотного шифрування на вкладці обліковий запис. Також користувач може включити дану функцію, встановивши відповідну групову політику. Після настройки цього параметра необхідно встановити новий пароль для активації цієї функції, тому що старий пароль не може бути визначений.

W-дайджест, оновлена форма перевірки автентичності дайджест, використовується, якщо Міжмережевий екран встановлений в домені Windows Server 2008. Перевірка справжності W-дайджест не вимагає, щоб в доменній службі Active Directory зберігалася оборотна зашифрована копія пароля користувача.

Перевірка справжності Digest і WDigest здійснюється наступним чином:

– клієнт робить запит;

– міжмережевий екран відмовляє в доступі і пропонує клієнту ввести ім'я користувача і пароль для входу в обліковий запис Windows; Примітка. При використанні W-дайджест ім'я користувача та ім'я домену чутливі до регістру і повинні вказуватися точно так само, як вони відображені в доменній службі Active Directory. Крім цього для WDigest потрібно ввести значення для шляху доступу до URL. Наприклад, запит користувача http://host.domain.tld не обробляється, оскільки відсутня шлях доступу до URL;

– облікові дані користувача проходять односторонню процедуру, найменування якої відоме як хешування. На виході виходить зашифрований хеш або

профіль повідомлення. У нього додаються значення для ідентифікації користувача, комп'ютера користувача і домена. Щоб виключити застосування користувачем анульованого пароля, додається позначка часу. Це явна перевага перед звичайною перевіркою автентичності, оскільки знижується ймовірність перехоплення і використання пароля неавторизованим користувачем;

Вбудована перевірка справжності Windows використовує методи перевірки автентичності NTLM, Kerberos і Negotiate. Це більш безпечні форми перевірки справжності, оскільки ім'я користувача та пароль хешіруются до відправлення їх по мережі. Якщо включена перевірка справжності NTLM, Kerberos або Negotiate, оглядач користувача підтверджує пароль за допомогою обміну криптографічними даними з міжмережевим екраном та хешування.[2]

В залежності від налаштувань браузера перевірка справжності може не запитувати спочатку ім'я користувача та пароль. Якщо спочатку не вдається ідентифікувати користувача, оглядач запитує ім'я користувача та пароль для входу в обліковий запис корпоративної мережі, які він обробляє за допомогою вбудованої перевірки автентичності. Веб-браузер продовжує запитувати ім'я користувача та пароль до тих пір, поки користувач не введе достовірні відомості або не закриє діалогове вікно із запитом. Ім'я користувача необхідно вводити у форматі:
домен \ ім'я_користувача.

Наприклад для Windows систем якщо спочатку не вдається ідентифікувати користувача, оглядач запитує ім'я користувача та пароль для входу в обліковий запис Windows, які він обробляє за допомогою вбудованої перевірки автентичності Windows.

Міжмережевий екран продовжує запитувати ім'я користувача та пароль до тих пір, поки користувач не введе достовірні відомості або не закриє діалогове вікно із запитом.

Оскільки перевірка справжності для зовнішніх користувачів застосовує метод NTLM, рекомендується використовувати SSL-шифрування трафіку між екраном і клієнтом.

Перевірка автентичності на основі форм може використовуватися для вхідних запитів на опубліковані веб-сервери.

Існує три типи перевірки справжності на основі форм:

– форма для введення пароля. У цю форму вводяться ім'я користувача та пароль. Ці типи облікових даних необхідний для перевірки автентичності за допомогою доменної служби Active Directory, LDAP і RADIUS;

– форма для введення секретного коду. У цю форму вводяться ім'я користувача і секретний код. Ці типи облікових даних необхідний для перевірки одноразових паролів методами SecurID і RADIUS;

– форма для введення секретного коду та пароля. У цю форму

вводяться ім'я користувача і секретний код, а також ім'я користувача та пароль. Ім'я користувача і пароль використовуються при перевірці достовірності для доступу до Міжмережевий екран за допомогою методів перевірки справжності одноразових паролів SecurID або RADIUS, а ім'я користувача та пароль - при методі делегування.

Перевірка справжності сертифіката клієнта не підтримується для вихідних веб-запитань. Для вхідних запитів на опубліковані ресурси вимога сертифіката клієнта може підвищити безпеку опублікованого сервера користувача. Користувачі можуть отримати сертифікати клієнта в комерційному (CA) або внутрішньому центрі сертифікації організації користувача.

Сертифікати можуть бути у вигляді смарт-карт або використовуватися мобільними пристроями так, щоб вони могли підключатися до корпоративної мережі. Сертифікат повинен узгоджуватися з обліковим записом користувача. Коли користувачі роблять запити на опубліковані ресурси, сертифікат клієнта, відправлений в міжмережевий екран, передається на контролер домену, який визначає відповідність між сертифікатами та обліковими записами. міжмережевий екран повинен бути членом домену. Відомості передаються назад на міжмережевий екран для застосування відповідних правил політики міжмережевого екрану. Примітка. міжмережевий екран не може передавати сертифікати клієнта на внутрішній веб-сервер.

1.6 Механізми управління конфігурацією підключення мобільного користувача

Налаштування параметрів віддаленого доступу для конкретного користувача в сучасних корпоративних мережах може бути виконана двома способами: або за допомогою спеціальних атрибутів облікового запису користувача, або за допомогою політик віддаленого доступу.

Наприклад спеціальні параметри облікового запису користувача в Windows Server 2016 вся інформація про користувачів (у тому числі і виддалениних) розміщується в каталозі Active Directory у вигляді об'єктів [3], асоційованих з обліковими записами, або в локальній базі облікових записів. При цьому з кожним подібним об'єктом пов'язаний певний набір атрибутів. У тому числі є спеціальні атрибути, що дозволяють задати конфігурацію віддаленого доступу для конкретного користувача. Ці атрибути перераховані в таблиці 1.2

Таблиця 1.2 - Атрибути, що дозволяють задати конфігурацію віддаленого доступу для конкретного користувача

Параметри і групи параметрів	Опис

Дозвіл на віддалений доступ (VPN або модем) (Remote Access Permission (Dial-in or VPN))	Даний параметр є важливим з точки зору того, що він визначає, чи дозволений явно деякого користувачеві віддалений доступ чи ні. Адміністратор може використовувати цей параметр для того, щоб явно заборонити віддалений доступ або делегувати вирішення даного питання політики віддаленого доступу. В останньому випадку вибирається опція Управлення на основі політики віддаленого доступу (Control access through Remote Access Policy). Навіть в тому випадку, коли доступ явно дозволений, він може бути заборонений на інших рівнях (умовами політики віддаленого доступу, параметрами облікового запису користувача або властивостями профілю)
Перевірити код хто телефонує (Verify Caller-ID)	Якщо ця властивість дозволена, сервер перевіряє телефоний номер зухвалої сторони. Якщо він не відповідає визначеному номеру, спроба з'єднання відхиляється
Відповідний виклик сервера (Callback Options)	Якщо ця властивість дозволена, то при установці з'єднання сервер запитує у зухвалої сторони вказується нею телефонний номер або використовує телефонний номер, заданий мережевим адміністратором, а потім выдправляє відповідний виклик. Дана функціональна можливість дозволяє дотримати належний рівень безпеки при підключенні віддалених користувачів, дозволяючи дзвінки тільки з перевірених телефонних номерів
Статичний IP-адрес користувача (Assign a staticIP-address)	Якщо ця властивість дозволена, робочої станції, з якої віддалено підключається розглянутий користувач, призначається певний IP-адрес. Статичний IP-адрес може знадобитися, наприклад, для нормальної роботи спеціального програмного забезпечення.
Використовувати статичну маршрутизацію (Apply Static Routes)	Якщо ця властивість дозволена, можна визначати ряд статичних маршрутів IP, які додаються до таблиці маршрутизації сервера віддаленого доступу після установки з'єднання. Цей параметр призначений для облікових записів користувачів, з якими працюють маршрутизатори в разі маршрутизації з установкою з'єднання на вимогу

Налаштування параметрів облікового запису користувача, що використовуються для конфігурування віддаленого доступу, виконується на вкладці Вхідні звонкі Dial-in у вікні властивостей об'єкта, асоційованого з обліковим записом користувача, в оснащенні Active Directory-користувачі і комп'ютери (Active DirectoryUsers and Computers). У разі автономного сервера

віддаленого доступу для конфігурування аналогічних параметрів облікового запису використовується оснастка Локальні користувачі та групи (Local Users and Groups).

Як правило сучасна корпоративна мережа (наприклад під управлінням Windows Server 2012R2) включає вбудований центр сертифікації (Certificate Authority - CA), також відомий за назвою служб сертифікації (Certificate Services) [1]. Служби сертифікації можуть використовуватися для створення сертифікатів і наступного керування ними, вони відповідають за їхню дійсність. Служби Certificate Services можуть застосовуватися для перевірки зовнішніх PKI, таких як PKI незалежних поставників для розширення сервісу і захисту взаємодії з іншими організаціями [5].

Тип центру сертифікації що встановлюється і набудовується залежить від мети чи цілей, для яких призначена інфраструктура PKI. Служби сертифікації можуть бути встановлені як центр сертифікації одного з типів, перерахованих нижче:

– Enterprise Root Certification Authority(Кореневий центр сертифікації підприємства). Це найбільш довірений центр сертифікації в організації і він повинен бути встановлений до всіх інших центрів CA. Всі інші центри CA на підприємстві підкоряються кореневому центру CA. Для Windows Server 2012R2 кореневий центр сертифікації за замовчуванням зберігає свої сертифікати в Active Directory (AD);

– Enterprise Subordinate Certification Authority(Підлеглий центр сертифікації підприємства). Підлеглий центр сертифікації підприємства повинен одержати сертифікат від кореневого центра CA, а потім видати сертифікати всім користувачам і комп'ютерам на підприємстві. Центри CA цього типу часто застосовуються для розвантаження кореневого CA і, що більш важливо, їхнє застосування забезпечує великий ступінь захисту інфраструктури PKI;

– Standalone Root Certification Authority(Автономний кореневий центр сертифікації). Такий центр CA є коренем ієрархії не зв'язаної з доменною

інформацією підприємства, і тому його сертифікати не зберігаються в AD.Для різних цілей може бути встановлена безліч автономних центрів CA.);

– Standalone Subordinate Certification Authority(Автономний підлеглий центр сертифікації). Цей центр CA одержує сертифікат від автономного кореневого центра CA і може бути згодом задіяний для видачі сертифікатів користувачам і комп'ютерам, зв'язаним з окремим центром CA.

Сучасна інфраструктура PKI може працювати як в оперативному, так і в автономному режимі. Ключова відмінність між ними складається в необхідному рівні захисту, що необхідний підприємству.

1.7 Висновок до першого розділу

Використання захищеного віддаленого 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 бізнес процесів типу Пошта, Контакти, Календар, Задачі і 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:

1. Проаналізувати нормативну базу та загрози при підключенні до інтрамережі мобільних пристроїв користувачів.
2. Налаштувати архітектуру інтрамережі підприємства для безпечного доступу до ресурсів мобільних користувачів.

3. Розгорнути центр сертифікації підприємства з можливістю web-доступу для отримання клієнтських сертифікатів.
4. Налаштувати сервери інтрамережі підприємства на взаємодію з провайдерами хмарних служб контролю за пристроями мобільних користувачів

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ ПРИ ВЗАЄМОДІЇ З МОБІЛЬНИМИ КОРИСТУВАЧАМИ

Об’єктом дослідження є безпека інформації, що передається, зберігається та оброблюється при використанні мобільних пристроїв..

Предметом дослідження є методи забезпечення інформаційної безпеки при використанні мобільних пристроїв.

Наукова новизна полягає в дослідженні методів забезпечення інформаційної безпеки на підприємствах, де використовуються мобільні пристрої для роботи з інформаційними активами підприємства.

Практичне значення полягає в дослідженні ефективності протидії загрозам несанкціонованого доступу до корпоративної інформації, яка оброблюється за допомогою мобільних пристроїв.

Мета дипломної роботи полягає в підвищення інформаційної безпеки підприємств, де кінцевий користувач має доступ і обробляє корпоративну інформацію за допомогою мобільних пристроїв

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 та хмарних системах обчислень.

Економічний ефект від реалізації результатів роботи очікується завдяки поліпшення бізнес процесів підприємства при одночасному підвищенні рівня захисту інформаційних активів.

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

2.1 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу

Відповідно до документу: «НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу» встановимо критерії оцінки захищеності інформації у комп’ютерних системах від несанкціонованого доступу при використанні мобільних пристроїв для співробітників, що перебувають за межами контрольованої зони підприємства.

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають:

- порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах[31];
- базу (орієнтири) для розробки комп'ютерних систем, в яких мають

бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної КС повинен надавати послуги з захисту об’єктів від несанкціонованого ознайомлення з їх змістом (компроментації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об’єктів, аналіз прихованих каналів, конфіденційність при обміні.

Довірча конфіденційність

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об’єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Базова довірча конфіденційність

Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об’єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта.

Запити на зміну прав доступу до об’єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об’єкта.

КЗЗ повинен надавати користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об’єкта.

КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об’єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об’єктів під час їх експорту та імпорту.

Конфіденційність при обміні

Ця послуга дозволяє забезпечити захист об’єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна конфіденційність при обміні

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об’єктів і інтерфейсних процесів, до яких вона відноситься.

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об’єкті, який передається.

Критерії цілісності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

Довірча цілісність

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об’єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна довірча цілісність

Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об’єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта.

Запити на зміну прав доступу до об’єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об’єкта.

КЗЗ повинен надавати користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об’єкт.

Права доступу до кожного захищеного об’єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об’єктів під час їх експорту і імпорту.

Цілісність при обміні

Ця послуга дозволяє забезпечити захист об’єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна цілісність при обміні

Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об’єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об’єкті, який передається.

Критерії доступності

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати

спроможність КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Використання ресурсів

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

Одиночна ідентифікація і автентифікація

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ.

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму.

Розподіл обов'язків

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Розподіл обов'язків адміністраторів

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції.

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб

включати тільки ті функції, які необхідні для виконання даної ролі.

Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Автентифікація вузла

Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ.

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму.

Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

В ідеальному випадку вище перераховані критерії оцінки захищеності інформації, при використанні мобільного доступу, мають допомогти визначити вимоги з захисту інформації в комп'ютерних системах від несанкціонованого доступу, створити захищені комп'ютерні системи, оцінити придатність комп'ютерних систем для обробки критичної інформації при використанні мобільних технологій. Але, враховуючи особливості функціонування систем що мають мобільних користувачів можна передчасно зробити висновок, що забезпечити деякі критерії буде досить складно, а іноді неможливо.

2.2 Визначення вимог до послуг, що надаються мобільним користувачам в сучасних корпоративних мережах

Згідно з задачами роботи були визначені вимог, що надаються

мобільним користувачам в сучасних корпоративних мережах:

- Єдина точка входу та захищений доступ до внутрішніх і зовнішніх ресурсів підприємства.(Single Sign-On) з двофакторноїю аутентифікацією
- Можливість роботи з технологіями управління цифровими правами (Digital Rights Management - DRM)
- Можливість роботи з технологіями засобів захисту від витоків даних (Data Loss Prevention, DLP)
- Можливість роботи з технологіями виявлення електронних даних (eDiscovery)
- Можливість застосування і централізованого керування корпоративними політиками безпеки на рівні як користувача і так і належного йому пристроїв
- Контроль відповідності вимогам щодо стану критичних файлів операційної системи, корпоративних додатків, антивірусного захисту, оновлень тощо
- Можливість централізованого керування шифруванням на рівні файлової системи мобільного пристрою незалежно від операційної системи
- Можливість централізованого управління мобільними пристроями на фізичному рівні та рівні корпоративних додатків незалежно від операційної системи та географічного розташування пристрою
- Відповідність вимогам міжнародних і регіональних стандартів безпеки

Мережа підприємства може бути розбита на три зони : внутрішню, периметр і публічну . До внутрішньої зони ставитися мережі класу С підрозділів організації (бухгалтерія , відділ кадрів, та інше.) з максимальним захистом. Периметр становить мережу класу В , що забезпечує взаємодію внутрішніх мереж і надає деякі сервіси через Інтернет зовнішнім

користувачам. У публічну зону входять зовнішні мережі й користувачі (локальні мережі філій і їхніх співробітників), а також ресурси Інтернет.

Комп'ютерна мережа організації є невід'ємною частиною системи керування й забезпечення діяльності організації, і призначена для рішення завдань, пов'язаних із забезпеченням керування й функціонування організації, за допомогою інформаційних технологій.

До основних функцій КС системи відносять:

– оперативний обмін даних між підрозділами організації;

– використання співробітниками, при виконанні функціональних завдань, інформаційних ресурсів мережі;

– забезпечення доступу до ІНТЕРНЕТ;

– застосування електронної пошти;

– організація централізованого зберігання даних з різним рівнем доступу до інформації.

Комп'ютерну мережу центрального офісу утворять базові компоненти встаткування, програмного забезпечення й параметрів мережного й між мережної взаємодії:

1. Сервера:

1.1 Контролер домену;

1.2 Бази даних;

1.3 Поштовий;

1.4 Web-Сервер;

1.5 Міжмережевий екран

1.6 Сервер сертифікації

2. Комунікаційні пристрої:

2.1 кабелі;

2.2 сполучні пристрої;

3. Робочі станції;

4. Система резервування й засобу зберігання інформації;

5. Інформаційна інфраструктура:

5.1 Операційні системи;

5.2 протоколи мережного й міжмережної взаємодії;

5.3 прикладне програмне забезпечення загального доступу;

5.4 прикладне програмне забезпечення робочих станцій.

5.5 Політика застосовна до всіх об'єктів, які забезпечують засобу для інтерактивної взаємодії з користувачами. Вона розглядається як елемент системи, що виконує набір вимог до безпеки.

5.6 Політика припускає, що відповідальність за збереження персональних даних, може бути делегована користувачам.

5.7 Всім індивідуальним користувачам призначений унікальний ідентифікатор, по якому мережа пізнає користувача перед дозволом на виконання будь-яких подальших дій.

5.8 Права доступу (наприклад, читання, запис, виконання) призначені об'єктам даних щодо суб'єктів (користувачів). Якщо суб'єктові наданий доступ до об'єкта, то зміст цього об'єкта може бути вільно використовувано, щоб впливати на інші доступні об'єкти.

5.9 Доступ до об'єктів даних і дозволених дій щодо них може відбуватися тільки відповідно до обмежень доступу, заснованими на функціях (ролях), певних адміністратором системи. Адміністратор системи зіставляє кожного користувача з одним або більшою кількістю функцій, які мережа використовує, щоб приймати рішення доступу. Повноваження для прийняття функції надається й відміняється адміністратором системи. Набір операцій розподілений кожної функції адміністратором системи. Кожна операція включає дію або процедуру перетворення й набір зв'язаних елементів даних.

5.10 Політика підтримує поділ обов'язків, при якому функції не можуть перебувати в протиріччі. Ніякому окремому користувачеві не дозволено виконувати всі частини транзакції, що представляється набором операцій (дій) з наборами даних об'єктів. Ця можливість може бути надана тільки адміністраторові системи.

Політика заснована на керуванні захистом доступу, заснованої на

функціях (ролях), аналогу мандатного принципу доступу. Вона визначає всі групи користувачів, що мають право роботи в середовищі ЛОМ, їхні права й обов'язки. Наприклад застосування політики в мережі може буде засновано на засобах безпеки сімейства ОС Windows Server 2012 R2, які мають весь необхідний для реалізації політики набір функцій і засобів забезпечення безпеки.

2.2 Розробка архітектури корпоративної мережі що має мобільних користувачів

Результатом роботи з'явилася розробка архітектури захищеної мережі підприємства, що має гібридні властивості. Сучасні мережеві операційні системи широко застосовують гібридні рішення. Згідно з цими можливостями частина функціоналу корпоративної мережі виконуються в дата центрах в форматах SaaS або IaaS. Згідно з цією концепцією була запропонована архітектура мережі, що представлена на рис.2.1

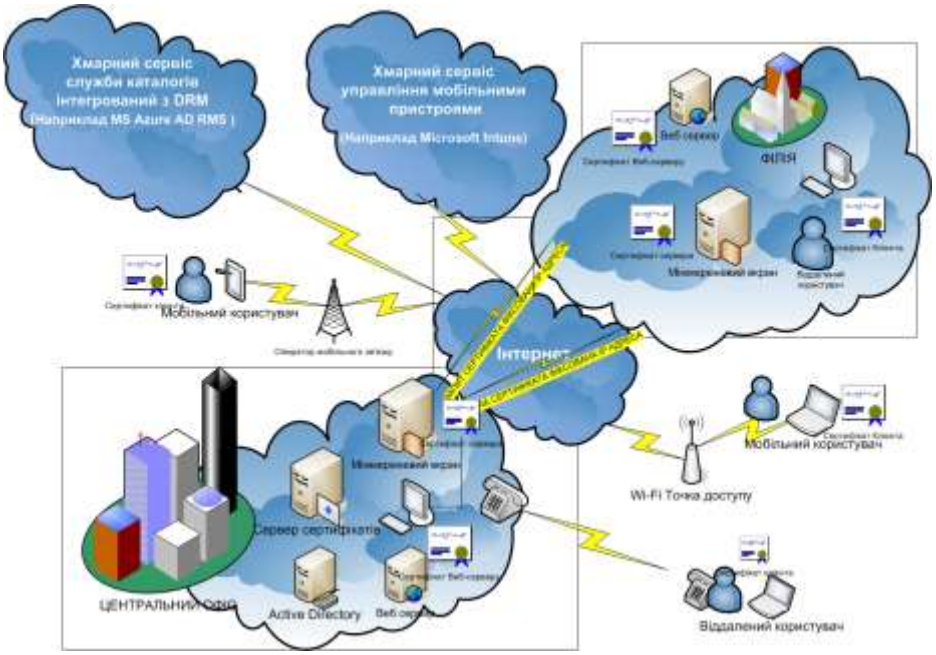

Рисунок 2.1 – Гібридна архітектура інформаційної системи підприємства яка має мобільних та віддалених користувачів.

При підключенні мобільних користувачів до інформаційної системи підприємства виникають проблеми:

- як віддалено керувати мобільними пристроями?
- чи є можливість заборонити запуск небажаних програм?
- як вибірково заборонити деякі інтерфейси і функції пристрою (камера, Bluetooth, Wi-Fi)?
- як забезпечити безпечну доставку, зберігання та видалення конфіденційної інформації на пристроях?
- чи є спосіб розповсюдження ПЗ на мобільні пристрої?
- як запобігти доступу пристроїв в Інтернет або до деяких сайтів?
- як заборонити підключення до корпоративної інфраструктурі певних пристроїв?
- чи можна віддалено знищити інформацію на мобільному пристрої?
- що робити, якщо пристрій вже втрачено або вкрадено?
- чи є можливість відключити некорпоративні поштові та користувальницькі додатки і сервіси?

Модель загроз при підключенні користувачів, що знаходяться поза межами фізичної мережі 2.2 .

Таблиця 2.2 − Модель загроз

№ п/п	Загрози	Інформація, що порушується				Вірогідні збитки
		К	Ц	Д	С	
1	Загроза перехоплення даних при проходженні інформації від мобільного пристрою при підключенні його до шлюзу провайдера мобільного зв'язку та Wi Fi	Так	Так	Так	Так	Суттєві

2	Загроза перехоплення даних при подальшому проходженню інформації через Інтернет	Так	Так	Так	Так	Суттєві
3	Ненавмисні помилки при вводі даних	Ні	Ні	Так	Так	Середні
4	Загроза навмисного несанкціонованого використання мобільного пристрою при крадіжці	Так	Так	Так	Так	Середні
5	Загроза ненавмисного використання мобільного пристрою (наприклад, при його втраті або крадіжці)	Ні	ні	Так	Так	Низькі
6	Загроза навмисного несанкціонованого використання документа поза корпоративної мережі (крадіжка інформації)	Так	Так	Так	Так	Критичні

2.3 Визначення служб , засобів та метод автентифікації в фізичній корпоративнній мережі, що забезпечують безпечний обмін інформацією з мобільними користувачами

Безпека на серверному рівні - одне з найважливіших понять для мережного середовища. Сервери в інфраструктурі не тільки виконують критичні мережеві служби на зразок системи доменних імен (Domain Name System - DNS) [39], протоколу динамічного конфігурації хостів (Dynamic Host Configuration Protocol - DHCP), пошуку в каталогах і аутентифікації, але і є централізованим місцем зберігання більшості, а то і всіх, критичних файлів в мережі організації. Тому так важливо скласти план забезпечення безпеки на серверному рівні і повністю розібратися в можливостях захисту сучасної сеерверної системи.

Кожен рядок коду повинен бути досліджен на предмет наявності можливих вразливих місць, а увагу було перенесено з розробки нових можливостей на забезпечення безпеки.

Так наприклад весь код продуктів Microsoft перевіряється в процесі

роботи середовища виконання з спільною мовою (Common Language Runtime - CLR). Ця середа виконує код програми, автоматично перевіряючи його на наявність проломів в безпеці, які можуть бути викликані помилками програмування. Крім того, ретельно перевіряються використовуються цими фрагментами повноваження, щоб переконатися, що код виконує тільки потрібні дії. Обмежуючи за допомогою цих технологій можливості зловживань і зменшуючи уразливість програмного забезпечення, середа Common Language Runtime знижує загальний ризик безпеки програмного забеспечення .

Заходи безпеки найбільш ефективні, коли вони застосовуються за рівнями. Наприклад, пограбувати будинок значно важче, якщо грабіжникові потрібно не тільки зламати парадні двері, а й впоратися зі сторожовим собакою і відключити домашню охоронну систему. Це ж відноситься і до безпеки сервера: система безпеки повинна складатися з декількох рівнів, щоб труднощі її злому зростала експоненціально. Так наприклад у Windows Server 2012 R2 органічно поєднуються необхідні рівні безпеки, в яких використовуються аутентифікація Kerberos, захист файлів NTFS і ввбудовані засоби безпеки, забезпечуючи таким чином готову систему безпеки. Для застосування додаткових компонентів безпеки необхідно розуміти особливості їх функціонування і встановити і настроїти їх елементи. Наприклад Windows Server 2012 R2 дозволяє додавати додаткові рівні безпеки і надає організаціям посилений захист без шкоди для функціональних можливостей.

Один з найбільш часто недооцінюємо, але, можливо, найбільш важливих компонентів безпеки сервера - реальна фізична безпека самого сервера. Найнадійніший, що не піддається злому веб-сервер безсилий, якщо зловмисник може просто відключити його від мережі. Ще гірше, якщо хто-небудь, увійшовши в систему важливого файлового сервера, зможе скопіювати секретні файли або вивести комп'ютер з ладу. Фізична безпека - обов'язкова умова для будь-якої організації, оскільки саме з

нею найчастіше пов'язана поява проломів у системі безпеки[14]. Незважаючи на це, у багатьох організаціях рівні фізичної безпеки важливих для виробничої діяльності серверів легко переборні або зовсім відсутні. Значить, неодмінною умовою забезпечення безпеки є розуміння того, що потрібно для захисту фізичного та логічного доступу до сервера.

Сервери повинні бути захищені фізично, тобто встановлені в закритому приміщенні з контрольованим доступом. Критичні для виробничого процесу сервери не варто поміщати біля ніг адміністраторів або в інших ненадійних місцях. Ідеальною з точки зору безпеки сервера середовищем є спеціальне приміщення або постійно замкнена шафа. Більшість компаній-виробників обладнання постачають свої вироби механізмами для фізичної блокування деяких або всіх компонентів сервера. В залежності від застосування інших рівнів безпеки може бути доцільним використовувати такі механізми для захисту середовища сервера.

Всі сервери повинні конфігуруватися так, щоб тільки адміністратори мали фізичний доступ до консолі для входу в систему. За замовчуванням це обмеження використовується в контролерах доменів, але на інших серверах - файлових серверах, допоміжних серверах і аналогічному обладнанні - такі типи входу в систему повинні бути спеціально заборонені. Щоб обмежити вхід в систему, необхідно заборонити локальний вхід в систему користувачів, які не є адміністраторами мережі.

Вихід адміністраторів з системи після запуску всіх робочих станцій і серверів мережі часто виявляється найбільш важко реалізовується і стомлюючої заходом безпеки. Якщо адміністратор забуде вийти з системи або просто ненадовго відійде від робочої станції, будь опинився поруч може без зусиль проникнути в інфраструктуру мережі.

Тому доцільно застосовувати стратегію входу в систему за допомогою команди Run As Administrator (Запуск від імені адміністратора) Windows Server 2008 R2. По суті це означає, що всі користувачі, включаючи IT-персонал, входять в систему з обмеженими стандартними обліковими

записами типу User (Користувач). Коли буде потрібно виконати адміністративну завдання, потрібний засіб або виконуваний файл можна викликати за допомогою команди Run As Administrator, яка надає цьому засобу адміністративні можливості облікового запису. Якщо адміністратор відійде від консолі робочої станції, не виходячи з системи, ситуація не буде небезпечною, оскільки консоль не надасть стороннім повний доступ до мережі з правами адміністратора.

Крім ручного застосування Run As можна настроїти комп'ютер адміністратора так, щоб при запуску адміністративних засобів кожен ярлик автоматично виконувався від імені адміністратора комп'ютера. Наприклад, за допомогою таких дій можна налаштувати оснастку Active Directory Users and Computers консолі MMC так, щоб вона завжди виконувалася з підвищеними повноваженнями.

У найбільш захищених інфраструктурах для дозволу входу в систему застосовуються так звані смарт-картки (smart card), які повністю підтримуються в Windows Server 2008 R2. Смарт-карти бувають різної форми, зазвичай це пластикова картка розміром з візитку з вбудованим в неї мікрочіпом і USB-роз'ємом. Кожному користувачеві видається унікальна картка і відповідний PIN-код. Вхід в робочу станцію зводиться до вставки картки в спеціальний зчитувальний пристрій та введення PIN-коду, який може бути комбінацією цифр і букв на кшталт пароля. Безпеку можна підвищити ще більше, вимагаючи автоматичного виходу користувача з консолі при витяганні смарт-карти. У такій ситуації користувачі вставляють в зчитувальний пристрій смарт-карту, закріплену на одязі ланцюжком або шнурком. Після введення PIN-коду вони входять в систему і виконують всі необхідні дії. Після цього користувачі просто витягують картку з пристрою, що зчитує, що призводить до автоматичного виходу із системи робочої станції. В цьому випадку практично неможливо забути вийти з системи, оскільки користувач, відходячи від комп'ютера, повинен фізично від'єднатися від нього.

Забезпечення безпеки кабелів завжди було складним завданням, але з'явилася недавно тенденція використання бездротових мереж ускладнила її ще більше. Багато організацій були приголомшені тим, якої шкоди може бути завдано мережі особою, яка має можливість підключитися через мережевий порт. Поява бездротових мереж ще більш спрощує доступ. Наприклад, зловмисник може просто під'їхати на автостоянку і отримати доступ до локальної мережі (Local Area Network - LAN) організації за допомогою ноутбука і стандартною карти бездротового зв'язку 802.11b. Стандартний протокол бездротового шифрування (Wireless Encryption Protocol - WEP), який використовується в бездротових мережах, практично марний, оскільки його можна зламати за кілька хвилин.

Управління мережевими портами і захист мережевих комутаторів є частиною стратегії безпеки. В організаціях з бездротовими мережами необхідно вживати більш суворі заходи безпеки. Впровадження бездротових мереж, в яких використовується протокол 802.1x, значно підвищує рівень мережевої безпеки. Microsoft використовує цей протокол для захисту своєї розгалуженої мережі, і Windows Server 2008 R2 повністю підтримує його.

Організації, яким не вистачає часу або ресурсів для впровадження протоколу 802.11x, можуть ефективно захистити бездротову мережу, просто розмістивши точки бездротового доступу зовні брандмауера і вимагаючи доступ по віртуальної приватної мережі (Virtual Private Network - VPN) через брандмауер. Навіть якщо зловмисник зможе зламати ключ WEP, йому вдасться підключитися тільки до ізольованого фрагменту, який не має вихід в іншу мережу.

У сучасних серверних операційних системах є вбудована підтримка нового набору служб і інтерфейс програмування додатків (API), званий захистом мережевого доступу (Network Access Protection - NAP)[39]. NAP підтримує можливість обмеження мережевих клієнтів на основі загальної працездатності (health) їх систем. Якщо, приміром, на клієнта, який намагається підключитися до мережі, не встановлені свіжі виправлення

безпеки або антивірусні бази, ця технологія забороняє підключення таких клієнтів до мережі. Серверна роль NAP називається сервером мережевих політик (Network Policy Server - NPS).

Система NAP управляє рядом певних політик працездатності і проводить ці політики на клієнтах, у яких є власний локальний агент працездатності системи. Особлива увага приділяється ролі сервера мережевих політик і її використання для обмеження доступу до середовища за допомогою протоколу динамічного конфігурації хостів (Dynamic Host Configuration Protocol-DHCP), IPSec, 802.IX і віртуальної приватної мережі (Virtual Private Network - VPN).

NAP в складається з ряду компонентів, призначених для обмеження клієнтського доступу до мереж за допомогою різних механізмів начебто контролю над тим, хто отримує IP-адресу з DHCP-сервера або хто випускає сертифікат IPSec. Сама технологія NAP розроблена незалежною від області застосування і містить опублікований набір інтерфейсів API, які дозволяють стороннім постачальникам, таким як виробники мережних пристроїв і компанії-розробники ПЗ, розробляти власні набори пристроїв, інтегрованих з пристроями операційної системи.

Технологія захисту мережевого доступу була розроблена у відповідь на небезпеки, що підстерігають комп'ютери, на яких не встановлені найсвіжіші виправлення безпеки або відсутні інші елементи захисту - наприклад, свіжі версії антивірусного ПЗ або локальний програмний брандмауер. Такі системи є першочерговими кандидатами на компрометацію і часто стають об'єктами атак шпигунського ПО - тобто особливо уразливими. Надання цим клієнтам необмеженого доступу до мережі неприпустимо.

Скомпрометовані системи у внутрішній мережі являють собою дуже великий ризик безпеки, тому що зловмисники можуть легко управляти ними і скомпрометувати важливі дані.

У NAP є три основні характеристики:

1. Відповідність політиці працездатності. Основою платформи NAP є можливість усунення проблеми. Тому функції відповідності політиці працездатності в платформі NAP виконують такі механізми перевірки відповідності, як служба поновлення операційної системи, агенти центру управління конфігурацією системи. Наприклад Windows Server 2012 R2 може автоматично адресувати клієнти на сервер виправлення, перш ніж надати їм повний доступ до мережі. Наприклад, клієнт без свіжих виправлень може бути відправлений на сервер оновлення для установки потрібних виправлень.

2. Перевірка стану працездатності. Агенти в клієнтських системах дозволяють відслідковувати і протоколювати конкретний стан окремих клієнтів. Адміністратор платформи NAP завжди може сказати, скільки систем в мережі не містять останніх виправлень, працюють без включених брандмауерів, а також дізнатися багато іншої статистики стану працездатності. В деяких випадках стан працездатності просто зазначається, в інших випадках таким клієнтам блокується мережевий доступ.

3. Обмеження доступу. Базовим принципом ефективної роботи платформи NAP є можливість обмеження доступу до мереж на основі результатів перевірки стану працездатності. Ступінь дозволеного доступу може бути дуже різним. Наприклад, клієнти можуть мати доступ до окремих систем для виконання виправлень безпеки, але не до інших клієнтам. В NAP Windows Server 2012R2 є можливості настроюваного обмеження доступу, що дозволяє адміністраторам створювати гнучкі політики.

2.4 Рекомендації щодо вибору методів автентифікації для мобільних користувачів

Середовище сучасних серверних систем та міжмережевих екранів надає наступні можливості автентифікації:

– єдиний вход Single Sign On (SSO)

– двухфакторна автентифікація з використанням автентифікації на основі форм і клієнтських сертифікатів.

– настроювані форми для автентифікації на основі форм і форм для мобільних клієнтів, а також використання для кожного користувача-агента схеми автентифікації [14].

– резервні з автентифікацією на основі форм для звичайної перевірки автентичності, для не-браузер клієнта.

– делегування повноважень з використанням NTLM або Kerberos автентифікацію.

– кешування повноважень.

– управління паролями, в яких міжмережевий екран може перевірити стан облікового запису користувача і повідомляє про це користувачеві. Ця функція також може бути налаштований, щоб дозволити користувачам змінювати свої паролі.

– Secure Sockets Layer (SSL) обмеження клієнтських сертифікатів.

– обмежене делегування

– можливість призначати різні цифрові сертифікати для кожного IP-адресу мережного адаптера.

– автентифікації на основі форм: ім'я користувача passcode/ password, де passcode використовується для автентифікації на між мережевому екрані, а password для делегування повноважень.

– підтримка служби каталогів автентифікації з використанням Lightweight Directory Access Protocol (LDAP),

– одноразовий пароль при підтримці віддаленого Dial-In User Service автентифікації (RADIUS).

– блокування делегування перевірки автентичності за замовчуванням

Згідно технічному для завданню були разработані рекомендації щодо вибору методів автентифікації для віддалених користувачів при використанні сервісів корпоративної мережі у середовищі Windows Server 2008 R2.

Підсумки представлені в таблиці 2.3

Таблиця 2.3 - Рекомендації щодо вибору методів аутентифікації для віддалених користувачів

Послуги	Тип користувача	Метод аутентифікації
Web доступ до внутрішніх і зовнішніх сайтів	мобільний	2 і 8
	віддаленний	1 і 5
Dial-Up доступ до корпоративної мережі	віддаленний	13
Корпоративна електронна пошта	мобільний	3
	віддаленний	1 і 5
Дистанційні корпоративні додатки (RemoteApps)	мобільний	2, 5 , 8 , 12
	віддаленний	5. 8, 12
Віддалений доступ до сховищ даних	віддаленний	8, 12
Web доступ до віддалених робочих столів (термінальний сервіс)	мобільний	2, 5 , 8 , 12
	віддаленний	2, 5 , 8 , 12
Доступ до файлових серверів по VPN (Direct Access)	мобільний	2, 8.12

2.5 Рекомендації щодо розгортання розгортання служби управління цифровими правами

Інфраструктура відкритих ключів (PKI)[5] - це система цифрових сертифікатів, центрів сертифікації й центрів реєстрації, які перевіряють і підтверджують дійсність кожного об'єкта, що приймає участь в електронній транзакції з використанням криптографії з відкритими ключами. Стандарти для PKI усе ще розвиваються, незважаючи на те, що вони широко реалізовані як необхідний елемент електронної торгівлі

Інфраструктура PKI підтримує ієрархічну модель центрів сертифікації, що є масштабованою та забезпечує погодженість із безліччю, що збільшується, комерційних і інших продуктів для центрів сертифікації.

У найпростішій формі ієрархія сертифікації складається з одного центра сертифікації. Але ієрархія часто містить кілька центрів сертифікації з чіткими відносинами "батько-нащадок". У цій моделі дочірній підлеглий центр сертифікації сертифікується за допомогою сертифікатів, виданих його батьківським центром сертифікації й прив'язують відкритий ключ до його посвідчення. Центр сертифікації, що перебуває на вершині ієрархії, називається кореневим центром сертифікації. Дочірній центр сертифікації кореневого центра сертифікації називається підлеглим центром сертифікації.

Якщо користувач довіряє кореневому центру сертифікації (його сертифікат перебуває в сховище користувача для сертифікатів довірених кореневих центрів сертифікації), він довіряє й всім підлеглим центрам сертифікації ієрархії, що володіє дійсним сертифікатом центра сертифікації. Отже, кореневий центр сертифікації є дуже важливою крапкою довіри в організації й повинен бути відповідним чином захищений.

Існує кілька практичних причин для створення декількох підлеглих центрів сертифікації, у тому числі:

- використання. Сертифікати можуть бути видані для декількох цілей, наприклад для захищеної електронної пошти й для перевірки дійсності в мережі. Політика видачі для цих застосувань може бути різної, і це розходження є основою для адміністрування цих політик;- підрозділи організації. Політики видачі сертифікатів можуть відрізнятися залежно від ролі об'єкта в організації. І знову можна створити підлеглі центри сертифікації для поділу й адміністрування цих політик;
- географічні підрозділи. Об'єкти організацій можуть перебувати в багатьох фізичних місцях. Для мережної взаємодії між цим місцями можуть знадобитися окремі підлеглі центри сертифікації для багатьох або для всіх площадок;
- балансування навантаження. Якщо інфраструктура PKI буде використовуватися для видачі великої кількості сертифікатів і керування ними, використання тільки одного центра сертифікації може привести до

помітного мережного навантаження для цього єдиного центра сертифікації. Використання декількох підлеглих центрів сертифікації для видачі сертифікатів того самого виду ділить мережне навантаження між центрами сертифікації;

- резервне копіювання й відмовостійкість. Кілька центрів сертифікації підвищують імовірність постійної наявності в мережі працюючих центрів сертифікації, готових відповісти на запити користувачів;

Ієрархія центрів сертифікації може також надати ряд переваг з погляду адміністрування, у тому числі:

- гнучка конфігурація середовища безпеки центрів сертифікації для настроювання балансу між безпекою й зручністю використання. Наприклад, можна використовувати спеціальне криптографічне устаткування на кореневому центрі сертифікації, використовувати кореневий центр сертифікації у фізично захищеній області або автономно. Такий підхід може бути неприйнятним для підлеглих центрів сертифікації через міркування вартості або зручності;

- можливість "виключити" конкретну частину ієрархії центрів сертифікації, не впливаючи на встановлені довірені відносини. Наприклад, можна легко завершити роботу й відкликати виданий сертифікат, пов'язаний з конкретним підрозділом, не впливаючи на інші частини організації.

У корпоративних мережах підтримується кілька методів видачі сертифікатів користувачам і комп'ютерам: одержання сертифіката через web-інтерфейс, запит сертифіката за допомогою Майстра, автоматичне розгортання й одержання сертифіката через агента.

Одержання сертифіката через web-інтерфейс (web-enrollment).[9] Цей метод може застосовуватися для одержання комп'ютерних і користувальницьких сертифікатів. Щоб цей метод був доступний, перед установкою на сервер Служби сертифікації необхідно спочатку встановити веб сервер. Для одержання сертифіката клієнт повинен набрати в рядку браузера адресу веб-інтерфейсу центра сертифікації і додержуватися

інструкцій Майстра. Для мобільних користувчів звертатися двічі − один раз для відправлення запиту на одержання сертифіката, а другий раз − для установки сертифіката (якщо запит був успішно підтверджений адміністратором).

Запит сертифіката за допомогою Майстра (Request New Certificate wizard) може застосовуватися для одержання комп'ютерних і користувальницьких сертифікатів

Автоматичне одержання комп'ютерних сертифікатів (Automatic certificate request). Цей метод розгортання застосовувався в мережах Windows для автоматичної видачі тільки комп'ютерних сертифікатів [15].

Для настроювання автоматичного одержання комп'ютерних сертифікатів застосовується групова політика видачи сертифікатів для домена.

Автоматичне розгортання (Autoenrollment). За допомогою цього методу можна організувати автоматичну видачу комп'ютерних і користувальницьких сертифікатів, якщо в якості клієнтської операційної системи використовується Windows.

Треба визначити, чи буде автономний центр сертифікації втримувати вхідні запити сертифікатів на очікуванні або видавати сертифікат автоматично. У більшості випадків з міркувань безпеки всі вхідні запити сертифікатів, адресовані ізольованому центру сертифікації, позначаються як очікуючи.

Треба настроїти модуль політики на автоматичне підтвердження всіх запитів на сертифікати або на приміщення запитів у чергу доти, поки адміністратор не перегляне ці запити й не почне необхідні дії. Вибір буде залежати від вимог до безпеки при видачі сертифікатів, від одержувачів сертифікатів і від ряду інших факторів.

Рекомендується така політика видачі, відкликання та відновлення клієнтських сертифікатів для мобільних користувачів:

- сертифікат не експортується і встановлюється тільки на пристрій, з якого прийшов запит;

- запит на видачу через веб-інтерфейс можливий тільки інтрамережі філіалу, яка має фіксовану публічну IP-адресу;
- термін дії та оновлення сертифікату визначається посадовою інструкцією служби безпеки підприємства (від 1 години до 1 місяця);
- миттєве відкликання сертифікату та блокування облікового запису користувача згідно команди уповноваженої персони служби безпеки підприємства (офіцера безпеки);
- для повторної видачі або відновлення сертифікату треба аудіовізуальне підтвердження уповноваженої персони служби безпеки з інтрамережі філії, з якої користувач отримав попередній сертифікат.

Кожний сертифікат видається з конкретним періодом дії. Відкликаний сертифікат стає непридатним для використання в системі безпеки до витікання вихідного строку його дії. Існує декілька причин, по яких сертифікат може стати недостовірним у якості облікових даних безпеки до витікання його строку. Наприклад:

- компроментація або можлива компроментація закритого ключа суб'єкта сертифіката;
- компроментація або можлива компроментація закритого ключа центра сертифікації;
- виявлення того, що сертифікат був отриманий шахрайським образом;
- зміна статусу суб'єкта сертифіката як довіреного суб'єкта;
- зміна ім'я суб'єкта сертифіката.

Не завжди можна зв'язатися із центром сертифікації або з іншим довіреним сервером, щоб одержати відомості про дійсність сертифіката.

Для ефективної підтримки перевірки статусу сертифікатів у клієнта повинна бути можливість доступу до даних відкликання, щоб визначити, чи діє сертифікат або він був відкликаний. Для підтримки різних сценаріїв служба сертифікатів підприємства підтримує методи відкликання сертифікатів, що є галузевим стандартом. Серед них публікація списків відкликаних сертифікатів

(CRL) і різницевих CRL[15], які могли бути доступні клієнтам з різних місць, включаючи служби сертифікатів, веб-сервери та загальні файлові мережні ресурси.

CRL являють собою повні і захищені цифровим підписом списки сертифікатів, які були відкликані. Ці списки публікуються періодично й можуть витягати й кешуються клієнтами (на основі настроєного часу життя CRL), а потім використовуватися для перевірки статусу відкликання сертифіката.

Тому що CRL можуть бути більшими, залежно від кількості сертифікатів, виданих і відкликаних центром сертифікації, проміжні CRL називаються різницевими CRL. Різницеві CRL містять тільки сертифікати, відкликані з моменту публікації останнього регулярного CRL. Це дозволяє клієнтам одержувати різницеві CRL меншого розміру й швидше створювати повний список відкликаних сертифікатів. Використання різницевих CRL також дозволяє частіше публікувати дані про відкликання, тому що завдяки малому розміру різницевого CRL для його передачі звичайно не потрібно так багато часу, як для повного CRL.

Сертифікати можуть бути відкликані з багатьох причин, включаючи наступні:

- ключ був скомпроментований;
- центр сертифікації, що видав сертифікат, був скомпроментований;
- сертифікат більше не є дійсним для своєї мети або був замінений іншим сертифікатом;
- клієнт більше не має права на цей сертифікат.

Кожний сертифікат має термін дії. По закінченні терміну дії сертифікат більше не розглядається як прийнятне посвідчення особи. Оснащення «Сертифікати» дозволяють за допомогою майстра відновлення сертифікатів обновляти сертифікат, виданий центром сертифікації підприємства під керуванням Windows, перед закінченням або після закінчення строку його дії.

Можна обновити сертифікат з тим же набором ключів, що

використовувався раніше, або з новим набором ключів. Вибір конкретного варіанта залежить від декількох факторів, включаючи термін дії сертифіката, довжину існуючого або майбутнього ключа, значення даних, захищених парою ключів, а також імовірність захвата закритого ключа зловмисником.

Перед відновленням сертифіката необхідно знати наступне.

- центр сертифікації, що видає сертифікат;
- (необов'язково.) постачальників служби криптографії (CSP), якого варто використовувати для створення пари ключів, якщо для сертифіката необхідна нова пара з відкритого ключа й закритого ключа.

Система повинна видати попередження, якщо термін дії сертифікатів користувачів або комп'ютерів минув або близький до закінчення. У більшості випадків функція автоматичної реєстрації обновляє такі сертифікати при наступному підключенні до мережі й вході в систему.

Відновлення сертифіката з тим же ключем забезпечує максимальну сумісність із попереднім використанням відповідної пари ключів, але не підвищує безпеки сертифіката або пари ключів. Керування сертифікатами користувачів можуть здійснювати відповідний користувач або адміністратор. Управляти сертифікатами, виданими комп'ютеру або службі, може тільки адміністратор або користувач, якому були надані відповідні дозволи.

Відновлення сертифіката з новим ключем дозволяє продовжити використання існуючого сертифіката й зв'язаних даних, одночасно підвищивши надійність ключа сертифіката. Це доцільно в тому випадку, якщо застосування нового сертифіката може привести до порушення роботи й, якщо, існуючий сертифікат не був скомпроментований.

Для виконання цієї процедури необхідно бути, як мінімум, членом групи Користувачі або Адміністратори локальної системи.

Багато організацій зіштовхуються з проблемою управління їх інтелектуальною власністю після її розповсюдження. Кілька серйозних витоків внутрішньої секретної листування у великих корпораціях

продемонстрували необхідність управління та обмеження у випадках поширення конфіденційної корпоративної інформації.

Джерело проблеми полягає в тому, що історично комп'ютерні системи добре справляються з обмеженням доступу до інформації для неавторизованих осіб, а після авторизації управління діями з інформацією втрачається. Авторизовані особи можуть копіювати документи "на винос", відправляти секретну інформацію по електронній поштою, у них можуть пропадати ноутбуки - і взагалі може існувати безліч різних способів втрати контролю над конфіденційною інформацією організації.

Наприклад у Windows системах така служба інтегрована з службою каталогів. Служба Active Directory RMS призначена для повернення можливостей контролю в такі організації. Вона дозволяє уповноваженому персоналу обмежувати можливості пересилання, друку, копіювання та зазначення строку придатності документів. Крім того, інтеграція зі службою доменів Active Directory дозволяє дешифрувати інформацію тільки особам, спеціально зазначеним у політиках. Служба управління правами Active Directory (Active Directory Rights Management Services - AD RMS) являє собою технологію управління цифровими правами (Digital Rights Management - DRM), що дозволяє встановлювати обмеження на управління, пересилання та перегляд вмісту. В RMS використовується технологія PKI для шифрування такого вмісту, як документи та поштові повідомлення, і навіть для перегляду цієї інформації без можливості її друку, копіювання-вставки та/або перенаправлення. Наприклад AD RMS в Windows Server 2012 R2 є удосконаленням технології сервера управління правами Windows (Windows Rights Management Server), яка розвивається вже декілька років. Крім вже існуючих можливостей у ній посилена інтеграція зі службою доменів Active Directory і підвищена масштабованість.

2.6 Вимоги до провайдерів хмарних сервісів, що забезпечують безпечний обмін інформації із мобільними користувачами корпоративних мереж. Нові сценарії роботи користувачів корпоративних мереж

При роботі в гібридних системах користувачі реалізують такі сценарії:

- доступ до корпоративних систем через Інтернет
- доступ до корпоративних систем для підрядників, партнерів, постачальників і т.д. (не співробітників компаній)
- робота з мобільних пристроїв незалежно від операційних систем
- умовний доступ до систем з керованих корпоративних пристроїв
- шифрування документів при обміні всередині компанії і з зовнішніми одержувачами
- аналіз роботи користувачів всередині корпоративної мережі
- контроль мобільних пристроїв незалежно від операційних систем

Хмарні служби можуть допомогти організаціям керувати і захищати мобільні пристрої, додатки і ПК на платформах Windows, Windows Phone, Apple IOS, і платформи Google Android. Хмарні технології не вимагає додаткової інфраструктури, однак організації можуть використовувати послугу, щоб розширити існуючу інфраструктуру управління в хмарі. На додаток до підвищення безпеки пристрою шляхом забезпечення оновлення та політики управління, хмарні сервіси (наприклад як Microsoft Intune) можуть допомогти організаціям надати співробітникам доступ на своїх власних пристроїв до додатків і ресурсів, необхідних, що реалізувати принцип Bring Your Own Programs Device (BYOD). реальністю.

Організації що надають такі сервіси вимагають довіри, але перш, ніж клієнти дають цю довіру, вони хочуть знати відповідь на такі питання, як:

- Хто може отримати доступ до даних і як ми її використовуємо?
- Де провайдер серввісу зберігають свої дані?
- Як їх дані закріплені в центрі обробки даних і при їх переміщеннях?
- Чи є впевненість у конфіденційності своїх даних і хто володіє

такими даними?

- Які організації незалежно один від одного перевіряють провайдера сервісу?

Безпека для провайдера починається в центрі обробки даних . Провайдер сервісу повинен контролювати фізичний доступ персоналу до центрів обробки даних за допомогою перевірки автентичності дворівневу, включаючи читачів доступу до проксі-карт і біометричні зчитувачі. На щоквартальній основі, співробітник служби безпеки провайдера повинен відправляти звіти персоналу з повноваженнями затверджувати дані про доступ центру. Уповноважений персонал регулярно переглядати список, щоб переконатися, що всі люди в цьому списку як і раніше потребують доступу і мають найменший рівень привілейованого доступу, необхідні для виконання своїх посадових обов'язків.

Незалежні реєстратори і акредитаційні організації повинні регулярно перевіряти центри обробки даних провайдера на підтримку міжнародно признаних різних сертифікатів До них відносяться:

- ISO 27001
- ISO 27018
- SOC 1 Type 2
- SOC 2 Type 2
- CSA STAR 1

Безпека повинна бути є безперервним процесом, а не стійким станом. Таким чином, досвідчений і навчений персонал має постійно підтримувати, розширювати та переглядавати нашу інфраструктуру. Провайдер сервісу повинен використовувати сучасне програмне забезпечення та пристрої для проектування, будівництва та експлуатації мереж, що реалізують концепцію BYOD.

Безпека починається з людей. Починаючи з процесу найму на роботу, усі

співробітники і субпідрядники, які мають доступ до даних клієнтів пройти через чергу стандартних перевірок, як це дозволено законом, які включають в себе огляд освіти кандидатів, зайнятості та кримінальної історії. На додаток до стандартних перевірок для всіх нових співробітників, персонал повинен пройти додаткові перевірки, якщо вони хочуть мати доступ до даних клієнтів або керувати ключовими фізичні або логічні засоби управління доступом. Наприклад додаткова перевірка для дата центрів США включає в себе перевірку на відповідність списків експортного контролю, таких як Управління іноземними активами Список управління бюро промисловості та безпеки, Список управління з питань оборони торгівлі.

Провайдер повинен дотримуємося принципів поділу обов'язків і найменших привілеїв.. Співробітники несуть відповідальність за їх обробку даних про клієнтів. Провайдер повинен підсилювати цю відповідальність через процес, який включає в себе використання унікальних імен користувачів, на основі ролей доступу та двофакторної автентифікації (наприклад, смарт-карти і RSA токени). Як і в разі фізичного доступу до центрів обробки даних, провайдер повинен розглядати можливості логічного доступу, щоб гарантувати, що тільки належний доступ надається до даних клієнтів, таких як контактна інформація, комп'ютерних деталей, а також інформацію про користувачів.

2.7 Вимоги до адміністрування мобільними пристроями користувачів

Тільки адміністратор може скористатися порталом адміністратора для завантаження програмного забезпечення клієнта. Кінцеві користувачі з існуючими обліковими рахунками можуть завантажити і встановити клієнтське програмне забезпечення від компанії після того, як вони завершують самостійної реєстрації процесу.

Установка клієнтських додатків вимагає підвищених дозволів, яка допомагає захистити комп'ютер від шкідливих установок. (Адміністратор - користувач може розгорнути клієнтське програмне забезпечення для стандартних

користувачів за допомогою групової політики або системи електронного поширення програмного забезпечення [ESD], наприклад як System Center 2012 Configuration Manager від Microsoft.) Якщо організації вважають за краще поширювати клієнтське програмне забезпечення, використовуючи файловий ресурс загального доступу або системи ESD, вони слід вжити заходів для запобігання несанкціонованому доступу

Кожна мобільна платформа використовує свої власні патентовані процеси і моделі безпеки для забезпечення безпеки установки клієнта на мобільних пристроях. Наприклад, заходи безпеки в Windows Store, Google Play і Apple App Store сприяють безпеці клієнтського програмного забезпечення. Для Windows Phone, Android і мобільних пристроїв IOS, провайдер сервісу повинен використовувати Secure Sockets Layer (SSL) для забезпечення безпеки зв'язку між кожним пристроєм і провайдера. Сервіс провайдера повинен взаємодіяти з прошивкою пристроїв, використовуючи службу повідомлення Apple. Сервіс провайдера використовує сертифікат, який адміністратор повинен завантажити з Apple Push Portal, щоб поговорити зі службою керування пристроями Apple Mobile. Для Windows Phone і пристроїв Windows RT, він використовує повідомлення служби Windows і Android пристроїв, використовується Google Cloud Messaging. Провайдер повинен надати доступ наступних веб додатків:

- Порталу облікових записів. Цей портал вносить інтерфейс управління сервісами та облікового запису користувача в сервісі провайдера онлайн. Адміністратор облікового запису використовує цей портал для управління обліковими записами користувачів, груп користувачів, доменні імена, паролі (якщо налаштоване) та передплатити послуг.
- Консолі адміністратора. Ця консоль дозволяє адміністраторам встановлювати політики, завантажити програмне забезпечення та оновлення програмного забезпечення, а також керувати комп'ютерами віддалено.
- Порталу підприємства. Користувачі повинні мати можливість бачити

стан свого пристрою, завантажити програмне забезпечення, а також зв'язатися з IT-підтримки своєї компанії через веб-портал компанії. Щоб отримати доступ до порталу підприємства, користувачу повинен бути наданий доступ адміністратором для регістрації свого пристрію.

Всі три портали використовують SSL для забезпечення безпеки зв'язку з веб-браузером. Сесії повинні мати період не активності, тобто після періоду відсутності активності, закінчився сеанс користувача, а користувач повинен увійти в портал знов.

2.8 Вимоги до ідентифікації та автентифікація

Провайдер повинен використовувати хмарну каталог LDAP (наприклад Azure Active Directory) в якості своєї платформи автентифікації. Для того, щоб надати користувачам єдиного входу (SSO) досвід, підприємства можуть підключати свої локальної директорії до хмари. Адміністратор провайдера потім додає користувачів до групи користувачів , даючи їм безперешкодний доступ до сервісу, коли вони підписують в корпоративну мережу. Наприклад Microsoft надаї два варіанти для перевірки автентичності при підключенні до AD Azure: Федерація з AD FS і Password Sync. З AD FS, користувачів облікові дані ніколи не покидають мережу домену поки з Password Sync хеш паролів користувачів синхронізуються з хмарою.

2.9 Політики та конфігурації поширювані на мобільні пристрої

Настройки пристроїв або управління додатками, сертифікати, VPN і Wi-Fi профілі є прикладами політики та конфігурацій, які адміністратор провайдера сервісу повинен визначити і розгорнути. Цей зміст, а також отримана інформація відповідність від кожного керованого пристрою, також зберігається провайдером.

Провайдер не повинен збирати інформацію, що відноситься до

діяльності користувачів, в тому числі:

- журнали телефонів
- контакти, електронна пошта, календар
- документи
- текстові повідомлення (SMS) повідомлення
- відео / фотографії
- інформація GPS
- веб-історія перегляду

2.10 Вимоги до місцезнаходження даних та незалежна перевірка сервісу

Провайдер сервісу повинен мати регіоналізовану стратегію центру обробки даних. Країна замовника або регіон, який адміністратор вводить клієнта під час початкового налаштування послуг, визначає місце розташування основного сховища даних для цього клієнта. Наприклад, якщо клієнт в Сполученому Королівстві створює підписку на сервіс провайдера , їх підписка будуть створені і дані про клієнтів зберігаються в центрі обробки даних, розташованої в країні Європейського союзу. Щоб забезпечити доступність послуг, провайдеру слід методологію забезпечити безперервність бізнесу, яка дозволяє центрам обробки даних перехід на інший ресурс в межах даного регіону:

- Первинний дата центр. Це основний центрі обробки даних, де дані прикладного програмного забезпечення і клієнтів, що працюють на програмному забезпеченні розташовані. Наприклад для всіх клієнтів, розташованих в Північній Америці, первинні центри обробки даних розташовані в Сполучених Штатах. Якщо в Північній Америці клієнтам є доступ на підписку сервісу з іншого регіону, таких, як Європейський союз, вони як і раніше будуть використовувати дані, що зберігаються в Північній Америці. Якщо ви підписалися на сервіс з регіону, крім Північної

Америки, то веб-сторінки і дані, які ви переглядаєте, буде знаходитися в центрі обробки даних цього регіону.

- Резервне копіювання даних. Центр обробки даних резервного копіювання використовується для цілей аварійного перемикання. Всі первинні центри обробки даних мають резервні центри обробки даних, в тому ж регіоні. Якщо центр первинних даних перестає функціонувати будь-якої причини, послуга призначена, щоб зробити резервного копіювання. Клієнти можуть не отримувати повідомлення, коли відбувається перехід на інший ресурс. Залежно від конкретної служби, яка зазнає невдачі, перехід на інший ресурс не може привести до вимкнення служби.

Провайдер сервісу повинен бути сумісним з багатьма світового класу промисловим стандартам, і це підтверджується третіми особами. Незалежна перевірка може включає в себе:

• Сертифікування міжнародної організації зі стандартизації (ISO) ISO 27001 є одним з кращих показників безпеки, доступних по всьому світу.

• Провайдер повинен реалізувати строгий набір фізичних та логічних процесів управління що визначає 27001 ISO. Провайдер також повинен прийти однаковий міжнародний кодекс практики хмарної конфіденційності ISO / IEC 27018, який регулює обробку персональних даних постачальниками хмарних послуг. ISO 27018 є першим міжнародним набір елементів управління конфіденційності в хмарі і і провайдер обов'язково повинен прийняти цю практику.

• Відповідність положенням «US to EU Safe Harbor» які являють собою угоду між Сполученими Штатами і Європейським Союзом, що дозволяє організаціям самостійно сертифікувати дотримання вимог щодо захисту даних, щодо збору, використання і зберігання даних, забезпечення передачі юридичних даних з ЄС в США на додаток до сертифікованих по Safe Harbor ЄС. Провайдер сервісу має пропонувати клієнтам ЄС "Типові положення", які є стандартизовані договірні положення, що забезпечують договірні

гарантії навколо передачі особистих даних, які покидають європейський економічний простір (ЄЕП).

2.11 Висновок до другого розділу

Опрацювавши критерії, розглянуті у даному розділі, для створення захищеної інформаційно-комунікаційної системи підприємства, що має мобільних користувачів розроблено наступний алгоритм:

- Розгорнути службу каталогів в фізичній мережі підприємства
- В фізичній мережі підприємства розгорнути веб сервери, що забезпечують роботу служб мережі
- Розгорнути міжмережеві екрани
- Розгорнути Центр Сертифікації
- Сконфігурувати політики видачі сертифікатів користувачів і комп'ютерів.
- Отримати сертифікати користувачам та встановити сертифікати на сервери, робочі станції та мобільні пристрої
- Розгорнути шифровану файлову система систему в фізичній локальній мережі
- Сконфігурувати політики застосування електронних документів
- Розгорнути локальну службу управління застосування цифрових документів в фізичній локальній мережі
- Інтегрувати локальну службу каталогів з хмарою
- Інтегрувати локальну службу управління застосування цифрових документів з хмарою
- Застосувати хмарний сервіс централізованого управління мобільними пристроями

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Визначення трудомісткості розробки обґрунтованих рекомендацій захисту інформації.

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

Формула для розрахунку трудомісткості має наступний вигляд:

$$t = t_{тз} + t_{в} + t_{кпед} + t_{icцд} + t_{рсцд} + t_{рцс}, \text{ годин}, \quad (3.1)$$

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

$t_{в}$ – тривалість вивчення технічного завдання, літературних джерел за темою тощо;

$t_{кпед}$ – тривалість конфігурування політики застосування електронних документів;

$t_{icцд}$ – тривалість інтегрування локальної служби цифрових документів з хмарою;

$t_{рсцд}$ – тривалість розгортання локальної служби управління застосування цифрових документів;

$t_{рцс}$ – тривалість розгортання центру сертифікації.

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

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

де q – очікувана кількість операторів;

c – коефіцієнт складності обґрунтованих 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 обґрунтованих 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:

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

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

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

Для даної розробки: B = 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 конфігурування політики застосування електронних документів $t_{кпед}$ = 12 годин

Тривалість інтегрування локальної служби цифрових документів з хмарою $t_{ісцд}$ = 20 годин

Тривалість розгортання локальної служби управління застосування цифрових документів:

$$t\,рсцд = \frac{1{,}5Q}{(4...5)\cdot k},\ \text{годин}, \qquad (3.4)$$

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

Тривалість розгортання центру сертифікації $t_{рцс}$ = 32 год.

Виходячи з отриманих даних трудомісткість створення обґрунтованих рекомендацій дорівнює:

t = 16 + 1,17 + 12 + 20+ 21,4 + 32 = 102,57 год.

3.2 Розрахунок витрат на створення обґрунтованих рекомендацій

Витрати на створення обґрунтованих рекомендацій Кпз складаються з витрат на заробітну плату виконавця розробки Ззп: $К_{пз} = З_{зп}$.

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:

$$З_{зп} = t \cdot З_{пр},\ \text{грн}, \qquad (3.5)$$

де t – загальна тривалість створення обґрунтованих рекомендацій, годин; t=102,57 годин

Зпр – средньогодинна заробітна плата виконавця в листопаді 2017 року з нарахуваннями, грн/годину. Зпр = 57 грн/год.

$$З_{зп}=102,57 \cdot 57 = 5847 \text{ грн.}$$

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

$$З_{мч}= t_{опр} \cdot С_{мч} \text{ грн,} \quad (3.6)$$

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

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot Ce + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн,} \quad (3.7)$$

де P – встановлена потужність ПК, кВт; P = 1,5 кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година, $С_е$=1,25 грн/кВт·година;

$Ф_{зал}$ – балансова вартість ПК на початок поточного року, 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 (Microsoft Windows Server 2012 R2 Standard Edition), грн., $К_{лпз}$ = 19 464 грн;

$F_р$ – річний фонд робочого часу серверу, $F_р$ =8760.

Балансова 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:

$$A = \frac{Ф_{зал} Н_а}{100}, \text{ грн,} \quad (3.8)$$

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:

$Н_а = 1/Т_а \cdot 100\%$,

$$Н_а = 1/2 \cdot 100\% = 50\%.$$

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:

$$Н_{апз} = 1/Т_а \cdot 100\%,$$

$$Н_{апз} = 1/2 \cdot 100\% = 50\%.$$

Отже, вартість 1 години машинного часу ПК, становить:

$$С_{мч} = 1{,}5 \cdot 1{,}69 + \frac{7500 \cdot 0{,}5}{8760} + \frac{19464 \cdot 0{,}5}{8760} = 4{,}07 \quad \text{грн/год}$$

$$З_{мч} = 4{,}07 * 102{,}57 = 417 \text{ грн.}$$

Відповідно до отриманих даних, вартість створення обґрунтуванних рекомендацій дорівнює:

$$К_{пз} = 5847 + 417 = 6264 \text{ , грн.}$$

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

Додаткові капіталовкладення

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, \qquad (3.9)$$

де $К_{зпз}$ – 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, $К_{аз}$ =4 тис. грн;

Розрахунок затрат наведене у таблиці 3.1

Таблиця 3.1 - Розрахунок затрат

$К_{зпз}$	Вартість	$К_{аз}$	Вартість
WindowsServer 2012R2	19,464 тис. грн	ПК Server	18 тис. грн
Windows Intune	363 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 = 3000 + 19464 + 363 + 18000 + 4000 + 2000 + 6264 =53091 грн.

3.3 Розрахунок поточних витрат

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

$$С = С_в + С_к + С_{ак}, \text{ тис. грн.} \quad (3.10)$$

$С_в$ - витрати модернізацію системи інформаційної безпеки

$С_к$ - витрати на керування системою інформаційної безпеки

Витрати модернізацію системи інформаційної безпеки ($С_в$) не перевищують 10% від капітальних витрат):

$С_в$=5309 грн.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{єв} + С_е + С_{ел} + С_{тос}, \text{ грн.} \quad (3.11)$$

$С_а$ - річний фонд амортизаційних відрахувань

$С_з$ - річний фонд заробітної плати інженерно-технічного персоналу

$С_е$ - вартість електроенергії, що споживається апаратурою

$С_{тос}$ - витрати на технічне й організаційне адміністрування

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

$$С_а = (53091 * 50)/100 = 26545 \text{ грн.}$$

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

$$С_з = З_{осн} + З_{дод} \text{ , грн} \qquad (3.12)$$

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.

$$С_з = 738*12*1,22 = 10804 \text{ , грн.}$$

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.

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е \text{ , грн,} \qquad (3.13)$$

де Р – встановлена потужність апаратури інформаційної безпеки - 1,5кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки – 8760 год.

$Ц_е$ – тариф на електроенергію - 1,25 грн/кВт·годин.

$$C_{ел} = 1,5 * 8760 \cdot 1,69 = 22206 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($C_{тос}$) визначається за даними організації або у відсотках від вартості капітальних витрат (1-3%). $C_{тос} = 504,6$ грн.

$$C_к = 22206 + 10804 + 26545 + 504,6 = 60060 \text{ грн.}$$

3.4 Економічне обґрунтування

Для обґрунтування економічної доцільності використаємо підрахування чистої приведеної вартості.

Чиста приведена вартість (NPV) Поточна вартість майбутніх грошових потоків інвестиційного проекту, розрахована з урахуванням дисконтування, за вирахуванням інвестицій. r - ставка дисконтування (вартість капіталу, залученого для інвестиційного проекту).

$$NPV = \sum \frac{Bn}{(1+r)^n} - K \geq 0 \qquad (3.14)$$

де Вп –грощовий потік данного року

К – витрати на впровадження рекомендацій

n – кількість років, 2 рока

r – ставка дисконтування, ставка НБУ 14,5%

$$Bn \sum \frac{1}{(1+r)^n} - K \geq 0$$

$$\text{Вп} \geq \frac{\text{К}}{\sum \frac{1}{(1+\text{r})^{\text{n}}}}$$

$$\text{Вп} = \text{П} - \text{С}$$

$$\text{П} \geq \frac{\text{К}}{\sum \frac{1}{(1+\text{r})^{\text{n}}}} + \text{С}$$

К = 53091 грн, r=0,145, n=2, С= 60060 грн

$$П \geq 53091 * 1{,}63 + 60060$$

$$Прибб \geq 146600 \text{ грн}$$

3.5 Висновок до третього розділу

В даному розділі було підраховано трудоємкість, капітальні та поточні витрати на впровадження рекомендацій у функціонуючу систему.

Трудоємкість на створення обґрунтованих рекомендацій становить 102,57 годин.

Капітальні затрати на створення обґрунтованих рекомендацій становлять 53091 грн. Поточні витрати становлять 60060грн.

Скориставшись формулою підрахунку чистої приведеної вартості визначили що дана система доцільна на підприємствах де річний чистий прибуток після оподаткування перевищує 146600 грн

ВИСНОВКИ

Ідея роботи полягала у використанні новітніх хмарних криптографічних технологій для забезпечення безпечного обміну інформації з мобільними користувачами корпоративних мереж.

Наукова новизна полягала в дослідженні методів забезпечення інформаційної безпеки на підприємствах, де використовуються мобільні пристрої для роботи з інформаційними активами підприємства. Практичне значення полягає в дослідженні ефективності протидії загрозам несанкціонованого доступу до корпоративної інформації, яка оброблюється за допомогою мобільних пристроїв.

Дипломна робота виконана відповідно до мети та завдань. Розроблені рекомендації по вибору сервісів служб, засобів, та їх процедур їх розгортання , що забезпечують безпечний обмін інформації із мобільними користувачами корпоративних мереж.

Для цього були:

1. Визначені вимоги до послуг, що надаються мобільним користувачам в сучасних корпоративних мережах.
2. Визначені загрози при підключенні до інтрамережі мобільних користувачів та визначити профіль захищеності.
3. Розроблена гібридна архітектуру мережі підприємства що використовує хмарні технології для керування пристроями та обліковими записами мобільних користувачів.
4. Визначені служби , засоби і методи автентифікації що забезпечують безпечний обмін інформацією між мобільними користувачами і корпоративною мережею.
5. Розроблені рекомендації по вибору хмарних сервісів служб, що забезпечують безпечний обмін інформації із мобільними користувачами корпоративних мереж.

6. Розроблено алгоритм створення захищеної інформаційно-комунікаційної системи підприємства, що має мобільних користувачів
7. Розроблені рекомендації Розгорнути локальну службу управління застосування цифрових документів в фізичній локальній мережі
8. Розроблені рекомендації щодо інтегрування локальної служби каталогів з хмарою
9. Розроблені рекомендації щодо використання хмарної служби управління застосування цифровими правами.
10. Розроблені рекомендації щодо застосування хмарного сервісу централізованого управління мобільними пристроями.
11. Проведено розрахунок економічної ефективності рішення і виявлено, що дані рекомендації доцільні для підприємств де річний чистий прибуток після оподаткування перевищує 180974 грн

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

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

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

3 Моримото, Рэнд, Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Microsoft Windows Server 2012 R2. Полное руководство. : Пер. с англ. — М. ,2013. — 1456 с.

4 Шаблоны сертификатов (Электрон. Ресурс)/Спосіб доступа: URL: http://technet.microsoft.com/ru-ru/library/cc730705%28WS.10%29.aspx

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

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

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

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

9 Автоматизация документооборота. Внедрение системы електронного документооборота (Електрон.ресурс) /Спосіб доступу: URL: http: http://www. directum.ru/425833.shtml/ – Загол. з екрана.

10 Матвієнко О., Цивін М. Основи організації електронного документообігу. Навчальний посібник. – К.: ЦУЛ, 2008.-112с.

11 Необходимость внедрения систем електронного документооборота (Електрон.ресурс) /Спосіб доступу: URL: http://chief.nnov.ru – Загол. з екрана.

12 Лазарєв Г.П., Кльоцкін С.М., Хорошко В.О. Шляхи вирішення проблем інформаційної безпеки в Україні // Захист інформації. – 2000. – № 2. – С. 4-9.

13 Дудикевич В.Б., Зачепило В.С., Хома В.В. Правові основи захисту інформації: Конспект лекцій. – Львів: Видавництво Національного університету «Львівська політехніка», 2002. – 168 с.

14 Ворожко В.П., Корченко О.Г. Захист інформації з обмеженим доступом. Збірник нормативних документів. – К.: КУЦА, 1999. – 283 с.

15 Домарев В.В. Безопасность ИТ. Методология создания систем защиты. – М. – СПб. – Киев, 2002. – 688 с.

16 Закон України про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки (Електрон. ресурс)/Спосіб доступу:URL:http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16. – Загол. з екрана.

17 Конституція України (Електрон. ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua– Загол. з екрана.

18 Закон України «Про інформацію» (Електрон. ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua– Загол. з екрана.

19 Закон України «про електронні документи та електронний документообіг» (Електрон. Ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua/uk/doc/laws.– Загол. з екрана.

20 Закон України «Про електронний цифровий підпис» (Електрон. ресурс)/Спосіб доступу: URL: http://www.ucrf.gov.ua/uk/doc/laws.– Загол. з екрана.

21 Постанова КМ України № 1451 «Про затвердження положення про центральний засвідчувальний орган» (Електрон. ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua/cgi-bin/laws.– Загол. з екрана.

22 Постанова КМ України № 903 «Про затвердження порядку акредитації центру сертифікації ключів» (Електрон. ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua/cgi-bin/laws.– Загол. з екрана.

23 Постанова КМ України № 1454 «Про затвердження порядку обов'язкової предачі документованої інформації» (Електрон. Ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.– Загол. з екрана.

24 Постанова КМ України № 1452 Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності (Електрон. ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.– Загол. з екрана.

25 Постанова КМ України № 1453 Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади (Електрон. ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.– Загол. з екрана.

26 Наказ державного комітету архівів України №49 (Електрон. ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.– Загол. з екрана.

27 Постанова КМ України № 1453 «Про затвердження порядку наявності електронного документа (електронних даних) на певний момент часу» (Електрон. ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.– Загол. з екрана.

28 Закон України «Про науково-технічну інформацію» (Електрон. Ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.– Загол. з екрана.

29 Закон України «Про державну таємницю» (Електрон. ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.– Загол. з екрана.

30 Указ Президента України «Про положення про порядок здійснення криптографічного захисту інформації в Україні» (Електрон. Ресурс)/Спосіб доступу: URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.– Загол. з екрана.

31 Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (Електрон. ресурс)/Спосіб доступу: URL: http://www.ucrf.gov.ua/uk.– Загол. з екрана.

32 Постанова КМ №373 «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» (Електрон. ресурс)/Спосіб доступу: http://www.kmu.gov.ua/control.– Загол. з екрана.

33 НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» (Електрон. ресурс)/Спосіб доступу: URL: http://www.dstszi.gov.ua/dstszi.– Загол. з екрана.

34 ДСТУ 3396.1-96 «Захист інформації технічний захист інформації. Порядок проведення робіт» (Електрон. Ресурс)/Спосіб доступу: URL: http://www.dstszi.gov.ua/dstszi/control.– Загол. з екрана.

35 ISO/IEC 27005:2005 «Інформаційні технологій. Методи захисту. Система управління інформаційною безпекою. Вимоги» (Електрон. Ресурс)/Спосіб доступу: URL:http://www.dstszi.gov.ua/dstszi/control.– Загол. з екрана.

36 Анализ рисков и управление ими (Електрон. Ресурс)/Спосіб доступу: URL: bank.gov.ua/B_zakon/Draft/02022010/27001.pdf.– Загол. з екрана.

37 Информационная безопасность на службе ITIL (Електрон. Ресурс)/Спосіб доступу: URL: http://www.compress.ru/article.aspx.– Загол. з екрана. Управление бизнес-процессами (Електрон. Ресурс)/Спосіб доступу: URL: http://citcity.ru.– Загол. з екрана.

38 Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Яхтсмен, 1996. – 192 с.

39 Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. М.: МИФИ, 1995. – 285с.

40 Самохвалов Ю.Я., Темпіков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації: Навчальний посібник / За ред. проф. Хорошка В.О. – К.: НАУ, 2002. – С. 207.

41 Политики информационной безопасности / С.А. Петренко, В.А. Курбатов и др. – М.: компания АйТи, 2006. – 400 с.

42 С.Н. Ардатский, О.С. Бартунов Управление доступом в сложных информационных системах. – Образовательные порталы Росси. Выпуск 1. - 2005.-187 с.

43 Лазарєв Г.П. , Кльоцкін С.М., Хорошко В.О. Шляхи вирішення проблем інформаційної безпеки в Україні // Захист інформації. – 2000. – № 2. –4-9.

44 Брайловський М.М., Хорошко В.О., Чирков Д.В., Захист економічної інформації. Навчальиий посібник / За ред. проф. Хорошка В.О. – К.: НАУ, 2001. – 287 с.

45 НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі» // Урядовий кур'єр. – 1999. – № 113. – С. 18.

46 Overview of data loss prevention policies. [Electronic resource] – Acess : https://support.office.com/en-us/article/Overview-of-data-loss-prevention-policies-1966b2a7-d1e2-4d92-ab61-42efbb137f5e?ui=en-US&rs=en-US&ad=US.

47 Защита от потери данных. [Електронний ресурс] – Режим доступу : https://technet.microsoft.com/ru-ru/library/jj150527(v=exchg.150).aspx

48 Включение аудита почтовых ящиков в Office 365. [Електронний ресурс] – Режим доступу : https://technet.microsoft.com/library/dn879651.aspx

49 Перегляд звітів журналу аудиту. [Електронний ресурс] – Режим доступу : https://support.office.com/uk-ua/article/Перегляд-звітів-журналу-аудиту-b37c5869-1b47-4a82-a30d-ea20070fe527?ui=uk-UA&rs=uk-UA&ad=UA

50 Мониторинг, составление отчетов и трассировка сообщений в Exchange Online. [Електронний ресурс] – Режим доступу : https://technet.microsoft.com/ru-ru/library/jj200725(v=exchg.150).aspx
51 Планирование eDiscovery. [Електронний ресурс] – Режим доступу : https://technet.microsoft.com/ru-ru/library/ff453933(v=office.14).aspx
52 Защита от спама в Office 365. [Електронний ресурс] – Режим доступу : https://support.office.com/ru-ru/article/Защита-от-спама-в-Office-365-6a601501-a6a8-4559-b2e7-56b59c96a586
53 Security and Compliance: Customer Controls for Information Protection in Office 365. [Електронний ресурс] – Режим доступу : http://download.microsoft.com/download/F/2/B/F2B9D8BB-30C3-427C-8FBE-E687D986BD91/Whitepaper%20-20Customer%20controls%20for%20Information%20protection%20in%20Office%20365.docx

ДОДАТОК А. ПЕРЕЛІК МАТЕРІАЛІВ ДИПЛОМНОЇ РОБОТИ

1 Титульна сторінка.
2 РЕФЕРАТ.
3 СПИСОК СКОРОЧЕНЬ.
4 ЗМІСТ.
5 ВСТУП.
6 СТАН ПИТАННЯ.
7 СПЕЦІАЛЬНАЯ ЧАСТИНА.
8 ЕКОНОМІЧНА ЧАСТИНА.
9 ВИСНОВКИ.
10 ПЕРЕЛІК ПОСИЛАНЬ.
11 Додаток А.
12 Додаток Б.
13 Додаток В.
14 Додаток Г.
15 Презентація дипломної роботи.
16 Оптичний носій.

ДОДАТОК Б. КОПІЯ НАУКОВОЇ СТАТТІ

ВІДДАЛЕНЕ УПРАВЛІННЯ ІНФОРМАЦІЄЮ В РАЗІ ВТРАТИ КОНТРОЛЮ КОРИСТУВАЧА НАД МОБІЛЬНИМ ПРИСТРОЄМ

Автор: Старченко Олег Олегович
Науковий керівник: Флоров Сергій Володимирович
Державний ВНЗ «Національний гірничий університет», http://www.nmu.org.ua/ua/,
E-mail: Starchenko.Ol.O@nmu.one

У статті розглянуто варіанти впровадження хмарних сервісів на підприємстві, їх переваги та внутрішні та клієнтські засоби забезпечення безпеки.

Ключові слова – Microsoft Office, Microsoft Office 365, хмарні обчислення, AES, SSL, TLS, Active Directory.

З розвитком сучасних засобів мобільного зв'язку і збільшенням зони покриття операторами, мобільні пристрої і мобільні користувачі стають невід'ємною частиною корпоративних интрасетей. 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.

Згідно [1], найбільш актуальними для сучасних корпоративних интрасетей є наступні фактори:

- Різке збільшення віддалених мобільних користувачів корпоративних интрасетей, що використовують технології Wi-Fi, 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 управління корпоративними інформаційними ресурсами користувача, фізично розташованих на його мобільному пристрої. також повідомлень, зашифрованих за допомогою інструментів шифрування від сторонніх розробників (наприклад, PGP).

В результаті проведених досліджень був вироблений наступний порядок вирішення даної проблеми:

- Розгорнути службу каталогів в фізичній мережі підприємства
- В фізичній мережі підприємства розгорнути веб сервери, що забезпечують роботу служб мережі
- Розгорнути міжмережеві екрани
- Розгорнути Центр Сертифікації
- Сконфігурувати політики видачі сертифікатів користувачів і комп'ютерів.
- Отримати сертифікати користувачам та встановити сертифікати на сервери, робочі станції та мобільні пристрої
- Розгорнути шифровану файлову система систему в фізичній локальній мережі
- Сконфігурувати політики застосування електронних документів
- Розгорнути локальну службу управління застосування цифрових документів в фізичній локальній мережі
- Інтегрувати локальну службу каталогів з хмарою
- Інтегрувати локальну службу управління застосування цифрових документів з хмарою
- Застосувати хмарний сервіс централізованого управління мобільними пристроями

Управління функцією дистанційного стирання пам'яті, виконувалося пакетом Messaging and Security

Feature Pack за допомогою за допомогою інструменту веб-адміністрування ActiveSync Mobile Administrative Web tool. Цей інструментарій дозволяє управляти процедурою дистанційного стирання пам'яті загублених, вкрадених або іншим чином потрапили в чужі руки мобільних пристроїв, підключених до серверів по бездротових з'єднаннях

ВИСНОВОК

Наведені в даній статті технології і процедури дозволяють:

- організувати захищені канали, які блокують можливість перехоплення і дешифрування даних;
- швидко, якісно і надійно забезпечити бізнес процеси і робочий простір для мобільних користувачів інтрамежі підприємства;
- централізовано керувати інформацією на мобільних пристроях користувачів інтрамежі підприємства при виникненні підозри про втрату контролю.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Get the most from Office with Office 365 [Електронний ресурс]. – Режим доступу: https://products.office.com/en-us/compare-all-microsoft-office-products (дата звернення 05.04.2017), вільний.
2. Средства безопасности Office 365 [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/ru-RU/download/confirmation.aspx?id=26552 (дата звернення 05.04.2016), вільний.

ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

ДОДАТОК Г. ВІДГУК КЕРІВНИКА ДИПЛОМНОЇ РОБОТИ

«Дослідження захисту інформації в корпоративній мережі при взаємодії з мобільними користувачами»

студента групи 125м-16-1 Старченко Олега Олеговича

Дипломна робота за спеціальністю 125 «Кібербезпека» Старченко О.О представлена пояснювальною запискою на 110 стор., містить 1 рис., 4 табл., 2 додатка, 53 джерела.

Мета дипломної роботи – підвищення інформаційної безпеки підприємств, де кінцевий користувач має доступ і обробляє корпоративну інформацію за допомогою мобільних пристроїв. Тема і зміст дипломної роботи повністю відповідає технічному завданню на дипломну роботу.

У пояснювальній записці сформульована постановка завдання та ідея роботи, проаналізовані моделі розгортання та обслуговування хмарних технологій. У спеціальній частині досліджено методів забезпечення інформаційної безпеки при використанні мобільних пристроїв, визначено загрози при підключенні до інтрамережі мобільних користувачів. Розроблено гібридна архітектуру мережі підприємства що використовує хмарні технології для керування пристроями та обліковими записами мобільних користувачів, визначені служби. Розроблені рекомендації по вибору хмарних сервісів служб, що забезпечують безпечний обмін інформації із мобільними користувачами корпоративних мереж. В економічній частині було проведено розрахунок економічної ефективності рішення. 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 Старченко Олега Олегович присвоєння йому кваліфікації професіонала із організації інформаційної безпеки.

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

РЕЦЕНЗІЯ НА МАГІСТЕРСЬКУ ДИПЛОМНУ РОБОТУ

«Дослідження захисту інформації в корпоративній мережі при взаємодії з мобільними користувачами»

студента групи 125м-16-1 Старченко Олега Олеговича

Дипломна робота за спеціальністю 125 «Кібербезпека» Старченко О.О представлена пояснювальною запискою на 110 стор., містить 1 рис., 4 табл., 2 додатка, 53 джерела.

Мета дипломної роботи – підвищення інформаційної безпеки підприємств, де кінцевий користувач має доступ і обробляє корпоративну інформацію за допомогою мобільних пристроїв. Тема і зміст дипломної роботи повністю відповідає технічному завданню на дипломну роботу. У пояснювальній записці сформульована постановка завдання та ідея роботи, проаналізовані моделі розгортання та обслуговування хмарних технологій.

У спеціальній частині досліджено методів забезпечення інформаційної безпеки при використанні мобільних пристроїв, визначено загрози при підключенні до інтрамережі мобільних користувачів. Розроблено гібридна архітектуру мережі підприємства що використовує хмарні технології для керування пристроями та обліковими записами мобільних користувачів. Розроблені рекомендації по вибору хмарних сервісів служб, що забезпечують безпечний обмін інформації із мобільними користувачами корпоративних мереж. В економічній частині було проведено розрахунок економічної ефективності рішення. 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 Старченко Олега Олегович присвоєння йому кваліфікації професіонала із організації інформаційної безпеки.

Рецензент