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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента ***Чернобривця Яна Вячеславовича***

академічної групи ***125м-17-1***

спеціальності ***125 Кібербезпека***

спеціалізації[1]

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

на тему ***Підвищення рівня захищеності інформаційно-телекомунікаційної системи із технологією «Bring Your Own Device»***

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Начовний І.І.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту ***Чернобривецю Я.В.*** **академічної групи** ***125м-17-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації[1]

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

на тему ***Підвищення рівня захищеності інформаційно-телекомунікаційної системи із технологією «Bring Your Own Device»***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.2018 № 2025-л_____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***інформаційно-комунікаційні системи IT-компаній, які використовують технологію «Bring Your Own Device»***

Предмет досліджень ***методи забезпечення захисту інформації з обмеженим доступом***

Мета ***підвищення рівня захищеності інформації в інформаційно-комунікаційній системі із використанням технології «Bring Your Own Device»***

Вихідні дані для проведення роботи ***законодавство України та міжнародні стандарти у сфері кібербезпеки***

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна ***полягає в оцінки рівня захищеності інформації при використанні технології «Bring Your Own Device» та запропонуванні комплексного рішення реалізації концепції на підприємстві***

Практична цінність ***полягає в розробці комплексного рішення захисту ІзОД, що циркулює в інформаційно-телекомунікаційній системі, аналізі доцільності використання запропонованих засобів захисту інформації***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Закону України «Про інформацію», НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99, НД ТЗІ 3.7-001-99

5 ЕТАПИ ВИКОНАННЯ РОБІТ

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

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***очікується позитивним завдяки підвищенню захищеності ІзОД і зниженню ймовірності збитку від несанкціонованих дій зловмисників внаслідок залучення рекомендованих мір та засобів захисту ІзОД***

Соціальний ефект ***полягає в забезпеченні захисту корпоративної інформації від витоків через інсайдерів, підвищенні трудової дисципліни***

7 ДОДАТКОВІ ВИМОГИ

Завдання видано _____ Кагадій Т.С.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ Чернобривець Я.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: ___ с., __ рис., __ табл., 4 додатки, 38 джерел.

Об’єкт досліджень: інформаційно-телекомунікаційні системи IT-компаній, які використовують технологію «Bring Your Own Device».

Метою дипломної роботи є: підвищення рівня захищеності інформації в інформаційно-телекомунікаційній системі із використанням технології «Bring Your Own Device».

Предмет досліджень: методи забезпечення захисту інформації з обмеженим доступом.

В першому розділі дипломної роботи магістра було розглянуто: актуальність концепції BYOD, сучасні підходи реалізації технології BYOD на підприємстві, функціональні можливості цих рішень.

В спеціальній частині дипломної роботи магістра розглянуто рівень захищеності інформації відповідно функціональному профілю захищеності, який досягаються з використанням MDM-рішень та виявлені нереалізовані послуги. Запропоновано комплексне рішення впровадження BYOD.

Наукова новизна полягає в оцінки критеріїв захищеності які реалізуються з допомогою технології «Bring Your Own Device».

ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, КОНЦЕПЦІЯ BYOD, РІВЕНЬ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ, MDM-РІШЕННЯ.

РЕФЕРАТ

Пояснительная записка: ___ с., __ рис., __ табл., 4 приложений, 38 источников.

Объект исследований: информационно-телекоммуникационные системы IT-компаний, которые используют технологию «Bring Your Own Device».

Целью дипломной работы является: повышение уровня защищенности информации в информационно-телекоммуникационной системе с использованием технологии «Bring Your Own Device».

Предмет исследований: методы обеспечения защиты информации с ограниченым доступом.

В первой главе дипломной работы магистра было рассмотрено: актуальность концепции BYOD, современные подходы реализации технологии BYOD на предприятии, функциональные возможности этих решений.

В специальной части дипломной работы магистра рассмотрено уровень защищенности информации в соответствии функциональному профилю защищенности который достигаются с использованием MDM-решений и выявлены нереализованные услуги. Предложено комплексное решение внедрения BYOD.

Научная новизна заключается в оценке критериев защищенности реализуемых с помощью технологии «Bring Your Own Device».

ИНФОРМАЦИЯ С ОГРАНИЧЕНЫМ ДОСТУПОМ, ИНФОРМАЦИОННО-КОММУНИКАЦИОННАЯ СИСТЕМА, BYOD-ТЕХНОЛОГИЯ, УРОВЕНЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ, MDM-РЕШЕНИЯ.

ABSTRACT

Explanatory note: ___ p., __ fig., __ tab., 4 application, 38 sources.

Object of the research: information and communication system of the IT-companies that use technology «Bring Your Own Device».

The aim of the master thesis is to increase the protection of information in a telecommunications system technology «Bring Your Own Device».

Subject of the research: protection methods of the information with restricted access.

In the first chapter of the master thesis it has been considered: BYOD concept relevance, current approaches of the BYOD implementation technologies to the enterprise, the functionality of these solutions.

The specialized part of the master thesis is examining the level of information security according to the functional profile of security, which has been achieved, with the use of the MDM-solutions and moreover the unreleased services were discovered. The complex solution due to the BYOD implementation has been proposed.

Scientific novelty lies in the evaluation of the criterias for protection which have been implemented with the BYOD technology.

INFORMATION WITH RESTRICTED ACCESS, COMMUNICATIONS AND INFORMATION SYSTEMS, THE BYOD TECHNOLOGY, INFORMATION PROTECTION LEVEL, MDM-SOLUTIONS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС	–	автоматизована система;
ДСК	–	для службового користування;
ІБ	–	інформаційна безпека;
ІзОД	–	інформація з обмеженим доступом;
ІТ	–	інформаційні технології;
ІТС	–	інформаційно-телекомунікаційна система;
КЗЗ	–	комплекс засобів захисту;
ЗІ	–	захист інформації;
КСЗІ	–	комплексна система захисту інформації;
НСД	–	несанкціонований доступ;
НД ТЗІ	–	нормативний документ технічного захисту інформації;
ОС	–	обчислювальна система;
ПБ	–	політика безпеки;
ПЗ	–	програмне забезпечення;
AD	–	Active Directory;
BYOD	–	Bring Your Own Device;
IoE	–	Internet of Everything;
MDM	–	Mobile Device Management;
vDLP	–	Virtual Data Leak Prevention;
VPN	–	Virtual Private Network.

ЗМІСТ

с.

ВСТУП

Широке поширення підключених пристроїв впливає на роботу підприємства. Особливо не кількість підключених пристроїв, а з'єднання між ними. Під «з'єднанням» розуміємо взаємодію людей, процесів, даних і фізичних об'єктів, яке формує Всеохоплюючий Інтернет (Internet of Everything, IoE). Для реалізації переваг IoE потрібно сформувати відповідне ділове середовище, що покращує розвиток інновацій і підвищує продуктивності праці. Виходячи з цього, багато компаній дозволяють співробітникам працювати будь-яким зручним для них способом, в тому числі за допомогою особистих мобільних пристроїв.

Принцип BYOD (Bring Your Own Device), що припускає застосування в роботі особистих мобільних пристроїв, надає співробітникам можливість користуватися за допомогою свого пристрою будь-якими додатками і хмарними послугами. BYOD забезпечує оптимальне співвідношення між роботою та особистим життям, поширенням інновацій і зростанням продуктивності праці. Та існує ряд фахівців, які висловлюють побоювання з приводу того, що BYOD створює нові проблеми у сфері інформаційної безпеки і ускладнює управління різнорідними особистими пристроями і що ці негативні фактори можуть переважити його потенційні переваги.

Для перевірки ґрунтовності таких тверджень звернемося до даних, які отримав консалтинговий підрозділ Cisco IBSG після проведення дослідження, яке показало, що впровадження BYOD приносить компаніям користь, а саме підвищення кількості робочих годин працівників, зменшення витрат на організацію робочих місць робітника, отже, фінансову вигоду. Все залежить від практичної реалізації принципу BYOD [1].

Для успішної реалізації BYOD потрібно організувати безпечний доступ, прості методи автентифікації і чіткі правила використання мобільних пристроїв і послуг. Більш широкий стратегічний підхід до BYOD надає компаніям ще

більше переваг, дозволяючи скорочувати операційні витрати, нарощувати продуктивність праці і економити критично важливий ресурс – час.

Детальний аналіз фінансових аспектів впровадження BYOD, проведений в Бразилії, Китаї, Німеччині, Індії, Великобританії і США, показав, що у всіх цих країнах компанії отримують істотні фінансові переваги від BYOD [2].

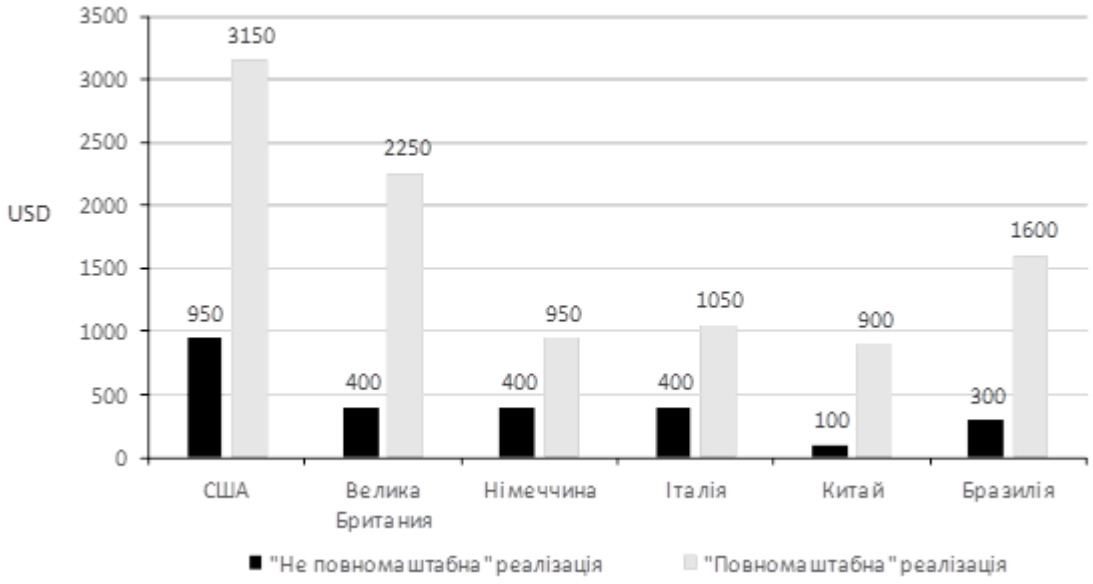

Рисунок 1 – Вигода підприємства від впровадження BYOD

Дослідивши дані з теми популярності BYOD можна оцінити не тільки ефективність і зрілість існуючих методів впровадження BYOD, а й спробувати з'ясувати, наскільки корисніше може стати повномасштабне використання даного принципу. Виходячи з рейтингів популярності виявилося, що до повномасштабного впровадження цієї концепції підійшло зовсім небагато компаній. На сьогоднішній день організації використовують лише п'яту частину (21%) можливостей повномасштабного BYOD.

Для отримання всіх переваг BYOD, компанія повинна накопичити критичну масу функцій BYOD і впровадити ефективні правила використання мобільних послуг, що враховують, в першу чергу, інтереси і можливості співробітників.

Найбільша проблема – проблема безпеки і керованості. Для мобільних платформ, наприклад, iOS, Android або будь-якої іншої, існує безліч вірусів, які можуть бути шкідливими як для конкретного пристрою, так і для корпоративної мережі в цілому. Мережа може стати більш вразливою для злому. Нерідко великі компанії навіть не замислюються про те, що їхні співробітники, використовуючи в роботі власні пристрої, фактично створюють проблему безпеки, якщо при цьому компанія не вводить відповідних BYOD-рішень.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність проблеми

Корпоративні користувачі все частіше використовують мобільні пристрої для роботи, однак компанії, які зважилися на застосування мобільних пристроїв в бізнес-цілях, повинні мати можливість керувати пристроями своїх співробітників. При роботі з мобільними пристроями в корпоративній мережі співробітники можуть навмисно чи мимоволі опублікувати конфіденційні відомості або використовувати ці пристрої неефективно.

Ідея мобільної віртуалізації (надання набору обчислювальних ресурсів або їх логічного об'єднання, абстрагованих від апаратної реалізації, що забезпечує при цьому логічну ізоляцію обчислювальних процесів, виконуваних на одному фізичному ресурсі) полягає в тому, щоб запустити два профілю на одному смартфоні або планшеті, що дає можливість розділити його простір на приватний і корпоративний. Перший тип мобільної віртуалізації працює на рівні «заліза» пристрою і вимагає співучасті мобільної компанії, а другий, впровадження захищеного додатка, що запускається на будь-якому пристрої. Перший варіант віртуалізації – на рівні виробника – дозволяє досягти більш високого рівня безпеки. Він має доступ до Bluetooth та інших мережевих підключень, чутливий до змін ПЗ на нову версію і набагато більш органічний з точки зору інтеграції з пристроєм. Використання цього способу означає, що виникає необхідність налагодження співпраці з виробником пристрою, а це значно збільшує цикли розробки – внаслідок великої кількості погоджень, довгих циклів продажів. Другий варіант віртуалізації передбачає оперативне розгортання на безлічі платформ і не вимагає узгоджень з виробником пристрою або оператором. Даний підхід поступається першому з точки зору безпеки і працює повільніше, потребує підвищених вимог до продуктивності пристрою.

Обидва підходи до мобільної віртуалізації мають таку спільну рису, що пристрій користувача поділяється на дві сутності – персональну та корпоративну. Віртуалізована (тобто корпоративна) частина зашифрована, що запобігає взаємодії зовнішніх додатків і сервісів з конфіденційними даними і корпоративним програмним забезпеченням. Персональна частина при цьому повністю відокремлена від корпоративної, і користувач може взаємодіяти з нею як зазвичай: фотографувати, завантажувати додатки, працювати з особистою поштою – без вводу будь-яких додаткових паролів. При викраденні пристрою, втраті або, наприклад, при неправильному вводі пароля до захищеної частини, IT-департамент має можливість стерти корпоративні дані вручну або автоматично [3].

Найпоширеніші підходи до реалізації технології: за допомогою віртуальних приватних мереж (Virtual Private Network, VPN), запропоноване розробниками засобів управління мобільними пристроями рішення класу Mobile Device Management (MDM) для забезпечення безпечної роботи з ними.

Найпростішим засобом захисту корпоративних даних при використанні мобільних пристроїв є системи захищеного віддаленого підключення через приватні віртуальні мережі (VPN), що дозволяють відмовитися від зберігання корпоративних даних на віддалених пристроях і отримувати доступ до інформації через захищене з'єднання і термінальну сесію. Ці рішення зручні також тим, що багато компаній вже встановили у себе шлюзи доступу до корпоративних мереж, через які можна працювати з інформацією із мобільних комп'ютерів на платформі традиційних операційних систем. Для підключення планшетних комп'ютерів і смартфонів достатньо встановити відповідні клієнтські частини для операційних систем iOS, Android, Windows Phone та ін.

Окремою проблемою є легальність установки клієнта VPN на ОС iOS – у деяких випадках для цього доводиться обходити засоби захисту операційної системи. Користувач не може отримати контроль над цією ОС і встановити на неї програмне забезпечення крім того, що є в Apple Store. Водночас далеко не всі

компанії можуть пройти процедуру включення їх клієнта в репозиторій додатків Apple, тому, щоб встановити агент на ОС iOS, потрібно обійти захист пристрою, що автоматично позбавляє власника пристрою гарантій з боку виробника. Міжнародні розробники засобів захисту на базі VPN, такі як Check Point або Stonesoft, домовляються з компанію Apple про поширення їх ПЗ через стандартний механізм встановлення додатків, але вони не реалізують потрібні деяким користувачам алгоритми шифрування і не мають сертифікатів. Тому зараз на ринку поки немає VPN-клієнта, який би повністю влаштовував всіх користувачів. Можливим варіантом вирішення даної проблеми є використання технології SSL-VPN, що дозволяє виконувати шифрування за допомогою стандартного протоколу HTTPS без встановлення спеціального клієнта. Всі перевірки в цьому випадку виконуються спеціальним сценарієм JavaScript, який може перевірити пристрій на наявність шкідливих програм і наприкінці сеансу видаляти з пам'яті пристрою інформацію, що містить конфіденційні дані. Теоретично клієнти цих виробників повинні працювати на мобільних пристроях, проте ефективність їх реалізацій досі не перевірена [4].

Для вирішення завдання централізованого управління корпоративними мобільними пристроями розробники платформ управління IT та засобів захисту запропонували окремий клас програмних продуктів – системи управління мобільними пристроями (Mobile Device Management, MDM). Ці продукти призначені для виконання автоматизованої установки на нове обладнання всього необхідного програмного забезпечення, налаштування, підтримки безпеки і захисту від витоків даних, моніторингу використання пристроїв і створення необхідного набору звітів, а також видалення всіх корпоративних даних з мобільних пристроїв у разі необхідності. Аналітики Gartner нарахували близько 60 компаній, що випускають продукти класу MDM, і в травні 2012 року був представлений список який включає 20 компаній, вирішення яких найбільш повно реалізують функціонал управління життєвим циклом мобільного пристрою [5].

Постачальників рішень MDM (таблиця 1.1) можна розділити на три групи: розробники засобів захисту, такі як Symantec, McAfee, Sophos, Trend Micro; виробники рішень для управління IT-системами, наприклад LANDesk, SAP, IBM, Amtel, Good Technology; компанії, для яких рішення MDM є основним бізнесом, до них відносяться MobileIron, AirWatch, Fiberlink і Zenprise. Крім того, сьогодні виробники засобів захисту нерідко купують спеціалізовані компанії з метою інтеграції їх технологій в свої продукти. Так, компанія McAfee придбала технологію управління мобільними пристроями разом з компанією Trust Digital, а Symantec базує свій продукт Mobile Management на розробках Odyssey Software. Виробники систем обробки подій і управління IT теж намагаються розширити свої системи засобами підтримки мобільних платформ. Функціональні можливості таких рішень, як IBM Worklight, SAPSybase Afari a або LANdesk Management Suite, досить функціональні, оскільки ці компанії мають великий досвід розробки систем управління. Однак сьогодні на ринку MDM поки лідирують спеціалізовані компанії, які мають чітку стратегію розвитку та можливості для її реалізації, та мало хто з них представлений в Україні [6].

Всі представлені сьогодні на ринку продукти MDM можна розділити на два типи. У першому варіанті, «не повномасштабна реалізація», для підключення нового пристрою до системи MDM потрібно встановити на нього додаток, що підтримує зв'язок з корпоративним сервером управління і контролює всі дії користувачів. При цьому ПЗ надає опис корпоративної політики безпеки і засоби моніторингу її дотримання, користувач працює із звичними йому додатками, а програма виконує тільки частину функцій MDM, які в основному пов'язані з дотриманням політики безпеки. У той же час управління життєвим циклом додатків і даних такі додатки не виконують. До цього варіанту відносяться продукти компаній AirWatch, BoxTone Fiberlink, MobileIron і Zenprise.

Таблиця 1.1 – Виробники MDM-рішень

Компанія-виробник	Платформи, що підтримуються	Типи компанії
MobileIron	Android, BlackBerry, iOS, Mac OS X, Symbian, WebOS, Windows Phone	Спеціалізована
AirWatch	Android, BlackBerry, iOS, Mac OS X, Symbian, Windows Phone/Mobile	Спеціалізована
Fiberlink	Android, BlackBerry, iOS, Mac OS X, Symbian, Windows 7,8,10/Phone/Mobile	Спеціалізована
Zenprise	Android, BlackBerry, iOS, Symbian, Windows Mobile	Спеціалізована
Good Technology	Android, BlackBerry, iOS, Windows Phone	IT–управління
BoxTone	Android, BlackBerry, iOS	Спеціалізована
IBM	Android, iOS, Mac OS X, Symbian, Windows 7,8,10/ Mobile/Phone, Linux, UNIX	IT–управління
SAP	Android, iOS, Symbian, Windows 7,8,10/Mobile, Palm	IT–управління
Symantec	Android, iOS, Windows Phone/Mobile	Безпека
McAfee	Android, iOS, BlackBerry, Windows Phone/Mobile	Безпека
Sophos	Android, iOS, BlackBerry, Windows Phone	Безпека
Trend Micro	Android, iOS, BlackBerry, Windows Mobile	Безпека
НИИ СОКБ	Symbian	Спеціалізована

Другий варіант, «повномасштабна реалізація», передбачає встановлення на пристрій спеціального набору програмного забезпечення, за допомогою якого можна підключатися до корпоративних сервісів. У цьому випадку на мобільному пристрої фактично створюється захищене середовище, через яке користувач отримує доступ до корпоративних даних. При цьому йому доводиться освоювати новий набір додатків, який входить до складу самого рішення. На пристрої створюються два робочі середовища: персональне, доступ до якого має користувач, і корпоративне, контрольоване IT-адміністраторами

компанії. Рішення цього класу пропонують компанії Good Technology, Excitor і SAP [7].

Архітектура рішень MDM передбачає три рівні: мобільний клієнт, сервер управління та хмарний сервіс від виробника. Є рішення, максимально сконцентровані на клієнті, продукти з багатим серверним функціоналом, а також рішення на базі хмарних сервісів, наприклад продукт «MaaS360» (Мобільність як сервіс, Mobility as a Service) компанії Fiberlink. Обираючи архітектуру того чи іншого рішення, покупець повинен оцінити, що йому зручніше самостійно обслуговувати сервіс управління мобільними пристроями співробітників або передати цю роботу сторонньої компанії-оператору.

Мінімальні функції вирішення MDM – встановлення на пристрій та налаштування програм, контролюючих відвідування сайтів, відправку SMS і виконання дзвінків на вказані номери. Крім того, важливою частиною рішення є видалення корпоративних даних з мобільного пристрою. У разі «не повномасштабної реалізації» додатку видалення може виконуватися при отриманні спеціального SMS, а «повномасштабної реалізації» самостійно видаляє з пристрою свій захищений контейнер.

1.2 Функціональність MDM-систем

1 Локальний репозиторій додатків. Контроль за встановленням додатків шляхом їх завантаження та встановлення тільки з корпоративного сховища, що містить лише перевірені програми. Управління репозиторієм програм забезпечується серверною частиною MDM-рішення. Слід зазначити, що виробники мобільних пристроїв, наприклад Apple, дозволяють своїм корпоративним клієнтам створювати подібні репозиторії.

2 Контроль доступу, SMS і телефонних дзвінків. Такий контроль може знадобитися компанії для захисту своїх мобільних співробітників від шкідливих програм, які змушують пристрій відсилати платні SMS або здійснювати дзвінки, хоча цей функціонал компанія може використовувати і для контролю за діями співробітників. Наприклад, передбачена можливість

читання SMS текстів, що відправляються співробітником, а також фіксації телефонних номерів і тривалість розмов.

3 Видалення даних. У разі втрати корпоративного пристрою спрацьовує команда знищення всіх даних і повернення пристрою до заводських налаштувань. Команда ініціюється за допомогою спеціально сформованого SMS, а сам компонент захисту спрацює автоматично при підключенні пристрою до мережі Інтернет. У разі «повномасштабної реалізації» рішення MDM видалення даних виконується разом із захищеним контейнером.

4 Визначення місцезнаходження. Сучасні мобільні пристрої мають засоби геолокації, що можна використовувати в корпоративних додатках, визначаючи, наприклад, маршрути переміщення співробітників для оптимізації часу доставки вантажів, оперативного реагування на виклики клієнтів [8].

Список типових функцій MDM-рішень може бути розширений кожним виробником, наприклад, компанія MobileIron пропонує платформу Virtual Smartphone Platform – аналог віртуальних робочих столів, але не для мобільних пристроїв. Крім того, далеко не всі виробники рішень MDM реалізують на мобільних пристроях шифрування, якщо воно не передбачене базовою платформою, проте, з точки зору захисту корпоративної інформації, це є важливим функціоналом MDM, тому навіть саму абревіатуру MDM розшифровують іноді як «управління мобільними даними» (Mobile Data Management). Недоліком також є відсутність, наприклад, функції із супроводження додатків на мобільному пристрої та їх захисту від шкідливих кодів.

Слід зазначити, що в рішеннях західних постачальників продуктів MDM не вітається перехоплення SMS, фіксація телефонних номерів або збір відомостей про становище телефону без згоди його власника, тому акцент робиться на тому, що при видаленні засобів MDM власник пристрою в обмін на повернення повного контролю над телефоном позбавляється корпоративного захисту та доступу до ресурсів підприємства. Така ситуація пов'язана з концепцією «принеси свій пристрій» (Bring Your Own Device, BYOD), що

припускає, що співробітник добровільно встановлює на свій мобільний пристрій MDM-клієнт для отримання доступу в корпоративну мережу. При цьому він також добровільно може дане програмне забезпечення видалити і повністю повернути собі контроль над своїм пристроєм.

Бездротові мережі стали невід'ємною частиною життя сучасної людини, у якої тепер з'явилася можливість користуватися публічними і корпоративними сервісами в будь-якому місці, однак мобільність, як і будь-яке нововведення, крім переваг таїть у собі і небезпеки. Зникнення пристрою, помилки при завданні параметрів, використання публічних мереж при роботі з конфіденційною інформацією – все це може призвести до витоку цінних даних. Без надійних платформ управління мобільними пристроями сучасному підприємству не обійтися [9].

З кожним роком все більше організацій надають своїм співробітникам доступ до корпоративних ресурсів, що дозволяє їм виконувати свою роботу як в офісі, так і віддалено, використовуючи планшети і смартфони. У теперішній час телефони, що застосовуються для роботи, управляються операційними системами Apple і Android, причому в Apple Store налічується близько 500 тис. додатків, а в Android Market – близько 200 тис. Наявність великої кількості додатків є великою перевагою, проте не слід забувати і про можливі небезпеки, такі як крадіжка або втрата смартфона, робота у відкритих мережах і таять в собі потенційні загрози політиці корпоративної інформаційної безпеки.

Для підтримки мобільних пристроїв адміністраторам організацій необхідно мати надійну платформу, що підтримує управління пристроями співробітників і параметрами їх безпеки [10].

1.3 Критерії вибору мобільної платформи

При виборі мобільної платформи, яка буде використовуватися співробітниками для доступу до корпоративної частини підприємства слід керуватися низкою критеріїв (підтримка яких забезпечить «повномасштабну» реалізацію технології та забезпечить її подальшу підтримку):

– безпека файлів. Інформація, що знаходиться за межами офісу, повинна зберігатися в зашифрованому вигляді і передаватися по захищеному протоколу. Із зростанням попиту на мобільні пристрої (такі які постійно знаходяться в мережі) зростає і розвитку різного роду ПЗ, що спрямоване на знищення інформації. Адміністратору повинна бути доступна інформація про файли, що знаходяться на пристроях працівників, а також терміни їх зберігання;

– підтримка безпечного обміну інформацією. Співробітникам повинна бути доступна можливість обміну інформацією з зовнішніми особами, наприклад партнерами і клієнтами, а безпека комунікацій не повинна обмежуватися конкретним доменом;

– наявність безпечного середовища для додатків. Ця вимога найбільш актуально у випадках, коли на пристроях співробітників зберігається важлива комерційна інформація. Безпечне середовище (корпоративний профіль) дозволяє утримувати конфіденційні дані в спеціальному сховищі, що відповідає підвищеним вимогам безпеки і керованому адміністратором підприємства, який може перевести їх в режим «тільки для читання» або видалити з пристрою;

– підтримка роботи з великими файлами. Мобільні платформи повинні відповідати цій вимогі, оскільки в даний час часто необхідно передавати відео обсягом у кілька гігабайтів або зображення високої чіткості;

– прозорість управління платформою. Адміністратори мобільних платформ повинні мати можливість призначати різні права доступу та політики безпеки для різних відділів і робочих груп. Контроль роботи за мобільними співробітниками дозволяє відстежувати зміни вмісту файлів, їх публікацію та інші фактори;

– відповідність рівня безпеки світовим стандартам. Рівень забезпечуваної безпеки мобільної платформи повинен відповідати вимогам місцевих регуляторів [11].

Таблиця 1.2 – Особливості мобільних ОС

Вид пристрою	ОС	Підтримка додатків	Переваги	Недоліки
Телефони	Apple iPhone	HTML, додатки, відсутня підтримка Flash	Популярність, широкий базовий функціонал, стабільність ОС	Відсутне шифрування, закрита ОС, жорсткі запити Apple App Store
	RIM BlackBerry	HTML, Flash, Java, додатки BlackBerry	Високий рівень безпеки, велика кількість ПЗ	Велика кількість розмірів екранів
	Android	HTML, Flash, додатки Android	Популярність, велика кількість ПЗ	Обмеження виробника на модифікацію
Планшетний ПК	iPad	HTML, HTML5, додатки	Популярність, широкий базовий функціонал, стабільність ОС	Відсутне шифрування, закрита ОС, жорсткі запити Apple App Store
	BlackBerry Playbook	HTML, HTML5, Flash, Java	Зв'язок з системами захисту підприємства	Обмежені функціональні можливості
	Android Tablets	HTML, HTML5, Flash, Java, додатки Android	Популярність, велика кількість ПЗ	Обмежені функціональні можливості

При виборі платформи підтримки мобільності для конкретного підприємства треба враховувати наступні рекомендації:

– необхідно сформулювати основні вимоги до системи і цілі її впровадження (в більшості випадків – це підвищення продуктивності праці співробітників);

– обрати підтримувані операційні системи з урахуванням їх переваг та недоліків;

– організувати тісну співпрацю кадрових служб, що відповідають, частіше за підвищення кваліфікації працівників, і підрозділів IT-необхідно

переконатися в безпеці платформи і врахувати психологічні особливості роботи з мобільними пристроями, щоб бути впевненими в готовності співробітників до використання мобільної платформи.

На теперішній час найпоширеніший рішення в галузі мобільної віртуалізації представлені трьома компаніями, при цьому кожне з них відрізняється власним підходом до реалізації технології [12].

Рішення компанії Enterproid під назвою «Divide». Користувач відкриває додаток на своєму Android-смартфоні, вводить пароль і отримує доступ до корпоративної частини операційної системи. IT-департамент контролює встановлення додатків, встановлює політики безпеки і може при необхідності видалити віртуальну машину з пристрою. Доступ до персональної частини пристрою у компанії відсутній; таким чином, співробітники не будуть заперечувати проти впровадження нової технології захисту. Особливості продукту Enterproid – це використання 256-бітного алгоритму шифрування (AES) вбудованої пам'яті і карт зберігання даних, або віртуальних «контейнеризацій» даних додатків, можливість фонової установки додатків залежно від ролі співробітника і призначення політик безпеки, типу заборони на копіювання даних між корпоративною та персональної частинами пристрою.

Продукт «Horizone Mobile Virtualization» від VMWare – це гібридне рішення для мобільної віртуалізації. Користувач запускає додаток і вводить пароль, отримуючи доступ до корпоративної складової пристрою. Надалі він може перемикатися між встановленими профілями. Особливість віртуальної машини, полягає в тому що корпоративна і персональна частини повністю розділені: копіювати з однієї в іншу не можна, а тому передати конфіденційні дані у зовнішній світ без дозволу IT-департаменту неможливо [13].

Компанія Red Bend Software пропонує ПЗ «vLogix Mobile», яке забезпечує мобільну віртуалізацію на компонентному рівні, продукт максимально інтегрований в пристрій. Перемикання між корпоративною та персональної сутністю здійснюється через екран блокування і систему

сповіщень, що на практиці виявляється зручніше і безпечніше, ніж просто перейти між додатками.

Переваги BYOD для бізнесу істотно переважають недоліки. Для усунення недоліків можна, використовуючи певні технології, створити рішення, що дозволяють чітко визначати, з якого пристрою користувач заходить в корпоративну мережу. Є спеціальні параметри, що дозволяють зрозуміти, що це за пристрій – наприклад, гаджет Blackberry, ноутбук з Windows, планшет з Android або, з iOS. Можна вирахувати, що, наприклад, в ідентифікаторі пристрою в Mac-адресі перша частина – це завжди ідентифікатор виробника пристрою. Браузери, посилаючи запити, інформують систему про те, що це за браузер і на якій операційній системі він працює. Наприклад, Safari для iOS чітко себе ідентифікує. І це – лише частина технологій, що дозволяють обчислювати, за допомогою якого пристрою користувач ввійшов в мережу. Тому з BYOD-технологіями можливо не тільки розподіляти співробітників і гостей за категоріями на рівні «логін/пароль», але і вводити більш складну ієрархію політик доступу до корпоративних ресурсів з урахуванням, ще й типу пристрою, з якого користувач входить в мережу. Наприклад, якщо це співробітник IT -підрозділу, що має максимальний рівень доступу до ресурсів мережі, то йому можна заборонити отримувати ті чи інші дані з використанням власного пристрою, навіть незважаючи на те, що його логін і пароль дозволяють це робити [14].

Рішення MDM дозволяють визначати статус безпеки пристрою. В момент, коли реєструється спроба підключитися до Wi–Fi, рішення може перевірити, чи встановлений на пристрої спеціальний агент, що надає інформацію про те, яка на пристрої операційна система, чи встановлений антивірус, або чи оновлена його база сигнатур і т.д. Якщо ж спеціалізований агент не виявляється, його можна запропонувати скачати. Після скачування система знову визначає статус безпеки, і якщо статус недостатній, то пристрій переводиться в карантин. У карантині можна, наприклад, оновити бази даних антивірусам з мережі Інтернет і повторно спробувати увійти в корпоративну

мережу. Якщо після оновлення, статус безпеки стане відповідати нормі, то система авторизує користувача в мережі. Все це знижує навантаження на IT-службу.

Також можливо визначати місце, звідки користувач заходить в мережу: з офісу компанії або віддалено через VPN, наприклад, ввійшовши, в будь-яке кафе, де є публічна мережа Wi-Fi, співробітник може як і раніше отримувати доступ до інформації через VPN. Але при цьому існує небезпека того, що пристрій можуть вкрасти. Така проблема вирішувана. Можна ввести політики, які при віддаленому доступі дозволяють увійти в корпоративну мережу, але блокують самі «чутливі» зони (наприклад, записи про фінанси компанії) [15].

Існують також системи Mobile Device Management (MDM), які можна інтегрувати в рішення BYOD. З їх допомогою, крім усього вищесказаного, можна додатково убезпечити мережу, глибше «вникати» в операційну систему і для підвищення безпеки вводити додаткове програмне забезпечення. Наприклад, можна змусити вводити PIN-код, який самі користувачі ставлять рідко, або шифрувати дані на пристрої. Якщо пристрій вкрали і користувач про це повідомив, то при наступному виході пристрою «в ефір» можна дистанційно видалити з нього дані [16].

Також в рішення можна додавати компоненти, що дозволяють контролювати, що співробітник або гість робить в мережі. Наприклад, можна заборонити доступ до ігрових ресурсів з корпоративної мережі співробітникам, але дозволити це гостям, або дозволити доступ до персональних сторінок соціальних мереж, але при цьому заборонити, наприклад, викладати фотографії або слухати музику, ввести заборону на доступ до сайтів, які заражені вірусами або поширюють шкідливе ПЗ, або ввести контроль рівня пошуку при використанні будь-яких пошукових машин, що при максимально високому рівні контролю.

Всі згадані функції при вдумливому проектуванні рішення надають можливість формувати потужну ієрархію політик роздільного доступу до корпоративних ресурсів та контролю за обміном трафіком із зовнішнім світом з

урахуванням маси факторів, що впливають на безпеку компанії. При цьому багато з цих можливостей безпосередньо знижують рівень проблем, які доводиться вирішувати IT-службі, що, в свою чергу, істотно знижує вартість придбання та підтримки подібного гнучкого інформаційного середовища [17].

Такі рішення вводять компанії, які зацікавлені у перевагах, забезпечуваних масовим застосуванням персональних мобільних пристроїв і спеціалізованих додатків, і які при цьому розумно і превентивно підходять до питань управління і забезпечення безпеки в такому середовищі. Частіше це навіть не компанії IT-сфери. Наприклад, у Сполучених Штатах BYOD застосовується в багатьох індустріальних вертикалях, включаючи освіту, охорону здоров'я і державний сектор (урядом США прийнята ціла програма з впровадження BYOD в держструктурах) [18].

1.4 Висновок

В Україні поки що більш виражений одиничний інтерес до BYOD. Найбільш розвинені компанії вже розробляють для себе такі рішення. Ймовірно, в перспективі ми побачимо перші прес-релізи на цю тему, тим більше, що опитування, проведені деякими дослідницькими компаніями, вже зараз демонструють досить високий рівень розуміння необхідності впровадження BYOD-рішень з боку вищого керівництва компаній.

У нашому регіоні ми поки бачимо стримане ставлення до використання концепції BYOD тому, що не так ще багато додатків є українською мовою. Але це неминуче буде змінюватися, і найближчим часом ситуація, з точки зору реальної потреби в BYOD-рішеннях, поліпшиться. Компанії які почнуть використовувати BYOD, почнуть пропонувати їх бізнесу в різних вертикалях і будуть багато в чому визначати і рухати цей ринок. Те ж саме відноситься до операторів і провайдерів. При бажанні і певній рішучості вони також зможуть знайти величезний бізнес-потенціал у частині неопрацьованою ніші пропозиції Wi-Fi інфраструктури як сервісу. Тим більше, що це легко ув'язується і з розвантаженням трафіку даних з мобільних мереж в мережі Wi-Fi і супутнім розвантаженням мобільних мереж. Керовані послуги, рішення для операторів

зв'язку і провайдерів послуг являють собою окремий широкий напрям, який в нашому регіоні практично не розроблений [19].

В першому розділі дипломної роботи було розглянуто сутність технології BYOD, розглянуто та проаналізовано існуючі методи її впровадження на підприємстві, виділені ті методи які існують на українському ринку, та проведена порівняльна характеристика мобільних операційних систем, що використовуються в Україні. Згідно з метою дипломної роботи магістра, в спеціальній частині необхідне вирішення наступних задач:

– аналіз ефективності наведених рішень;

– вибір функціонального профілю захищеності ІзОД від НСД;

– дослідження реалізації послуг сформованого функціонально профілю захищеності обраним рішенням;

– надання рекомендацій щодо реалізації послуг профілю, вимоги яких не виконуються.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Впровадження технології BYOD

Активне розповсюдження стратегії Bring Your Own Device (BYOD, Використання персональних пристроїв в робочих цілях) істотно прискорює темпи розвитку бізнес-процесів, і це значить, що багато компаній поставлені перед необхідністю шукати баланс між мобільністю співробітників і інформаційною безпекою бізнесу, вирішуючи ряд нових завдань, пов'язаних з ефективністю управління персональними пристроями та забезпеченням безпеки їх застосування.

Виникають завдання з приводу:

– забезпечення безпеки персональних пристроїв, дієвої і ефективної реалізації і підтримки програмних рішень в умовах великої кількості різних технологій, операційних систем та інших факторів, властивих для персональних пристроїв;

– ефективного відстежування цих пристроїв, враховуючи їх часту заміну і доступну ціну;

– відстежування використання співробітниками корпоративних ресурсів і даних;

– впевненості, що особисті дані співробітників захищені так само добре, як важливі корпоративні дані;

– впевненості, що співробітники не використовують персональні пристрої для відправлення/зберігання конфіденційної інформації в загальнодоступних хмарних сховищах;

– впевненості, що звільнені співробітники зберігають персональну інформацію, але не залишають компанію з конфіденційними корпоративними даними, збереженими на персональних пристроях;

– впевненості, що програми забезпечення безпеки для BYOD не суперечать правам на недоторканність особистих даних співробітників, при цьому захищається право компанії на контроль і захист корпоративної

інформації, а також виконуються вимоги введених політик, ПЗ щодо захисту різних видів даних.

Для подолання цих труднощів ринку було запропоновано деякі «BYOD-стратегії», але внаслідок помилкового маркетингу, генерованого конкуруючими виробниками, багато BYOD-стратегій, що подаються ринку як найбільш ефективні, такими не стали.

2.2 Проблеми впровадження BYOD

Найбільш поширені помилкові твердження пов'язані з масовим сприйняттям завдань управління ініціативами BYOD:

– рішення класу Mobile Device Management (MDM) повноцінно забезпечують безпеку корпоративних даних;

– важливі корпоративні дані можуть безпечно зберігатися в пам'яті персональних пристроїв;

– важливі корпоративні дані можуть безпечно створюватися безпосередньо на персональних пристроях;

– додатки, засновані на концепції BYOD, повинні мати доступ до важливих корпоративних даних;

– рішення класу Mobile Device Management (MDM) рівноцінні рішенням класу Data Leak Prevention (DLP).

Рішення, придатні для досягнення ефективності та безпеки застосування стратегії BYOD в організаціях.

Системи класу Mobile Device Management (MDM) дозволяють віддалено (централізовано) управляти мобільними пристроями, будь то пристрої, надані співробітникам компанією або власні пристрої співробітників (як «your own» частину в абревіатурі BYOD). Управління мобільними пристроями зазвичай включає в себе такі функції, як віддалене оновлення політик безпеки (без підключення до корпоративної мережі), поширення додатків і даних, а також управління конфігурацією для забезпечення всіх пристроїв необхідними ресурсами.

Перераховані вище функції необхідні будь-якій BYOD-програмі, але при цьому не є «панацеєю» безпеки BYOD-пристроїв, не гарантують ні збереження даних на пристроях, ні виконання вимог регуляторів.

MDM-системи встановлюють на КПК, смартфони, планшети та інші пристрої агентське програмне забезпечення, що працює на рівні додатків ("app") і що дозволяє реалізувати віддалене управління з централізованої консолі MDM-системи. Це означає, що системи MDM-принципово обмежені можливостями, наданими API операційної системи виробника персонального пристрою (якщо такий API надається взагалі), і зокрема – на рівні контрольованих комунікацій для контролю або хоча б моніторингу переміщення даних з кінцевого пристрою.

Деякі MDM рішення мають здатність самознищення всього програмного забезпечення і даних з мобільного пристрою у випадку зловмисного неавторизованого видалення з нього MDM-додатка. Проте до того моменту, поки на BYOD–пристроях не з'являться повністю незалежні операційні середовища (бізнес, персональна, середовище виробника і т.п.), сегментовані на фізичному рівні і забезпечені низькорівневими інтерфейсами для доступу СЗІ незалежних виробників, обмеженість можливостей MDM рішень з контролю вихідних потоків даних на мобільних пристроях залишиться принциповою проблемою, обговорення якої MDM-компанії уникають, а для імітації вирішення проблеми використовують «додатки» типу вищезазначених.

Для подальшого пояснення розглянемо основні можливості щодо забезпечення безпеки в BYOD, в яких зазвичай досягають успіху MDM-рішення:

– надійність парольного захисту;

– кероване видалення даних з пристрою у випадку втрати або крадіжки;

– шифрування вбудованої пам'яті і карт зберігання даних, або віртуальна «контейнеризація» даних додатків.

Всі ці функції є перевагами MDM-рішень. Проте ж сучасні MDM-системи здатні реалізувати принаймні одну функцію (що дозволяє забезпечити

віддалене стирання даних на пристрої) лише за умови, що пристрій з'явиться в мережі. Можна вважати, що дані в безпеці (тобто спрацюють функції шифрування і парольного захисту), тільки якщо пристрій втрачено так, що ніхто не знайде, або фізично знищено без можливості відновлення даних, або дісталося некваліфікованій в таких питаннях особі, залишається видавати бажане за дійсне.

Слід також мати на увазі, що існують спеціальні технічні рішення, що забезпечують відновлення даних з пристроїв і здатні «зламати» паролі на пристроях під управлінням iOS, Android, BlackBerry пристроях, а також зашифровані різними способами дані, особливо за наявності «захищених» резервних копій.

Також, MDM-системи абсолютно не враховують сценарій інсайдерської загрози, коли виток даних відбуваються випадково або навмисно з пристроїв незадоволених або звільнених співробітників.

Як наслідок, для осіб, які вирішили за допомогою BYOD-пристроїв заволодіти корпоративними даними, системи MDM всього лише створюють незначні перешкоди.

Розглядаючи безпеку зберігання і створення даних на BYOD-пристроях, потрібно пам’ятати, що завдання забезпечення безпеки корпоративних даних на персональних пристроях стоїть не тільки у зв'язку з комерційною необхідністю захисту корпоративних напрацювань, відомостей, персональних даних співробітників, але і в силу вимог різних законодавчих і нормативних актів [20]. Таким чином, методи створення, зберігання і обробки даних мають першорядне значення. На перший погляд, MDM-системи вирішують цю проблему в ситуаціях, коли співробітники вважають за краще зберігати корпоративні дані на власних пристроях.

У реальності вже сама практика зберігання даних на BYOD-пристроях породжує ризик витоку даних, незалежно від наявності на пристрої додатка MDM-системи.

Як згадувалося раніше, MDM-підхід шифрування даних у поєднанні з функцією віддаленого знищення даних забезпечує вельми низький рівень захисту. Більше того, з точки зору реальної безпеки даних цього рівня недостатньо – оскільки, потрапивши в руки кваліфікованого зловмисника, дані обмеженого доступу можуть бути попросту відправлені по мережевих каналах або вкрадені з пристрою іншим способом. Всі можливі способи переміщення або передачі корпоративних даних на/з BYOD, в тому числі через канал локальної синхронізації даних при підключенні до робочих станцій (за протоколами ITunes, ActiveSync, MTP та ін.), повинні контролюватися або хоча б блокуватися, або відображатися в тіньових копіях.

Розглянемо наступний сценарій: компанія дозволяє співробітникам підключати особисті мобільні пристрої до корпоративних ноутбуків, настільних ПК і серверів. Після підключення ці пристрої можуть легко передавати персональні дані або корпоративну інформацію компанії у величезних кількостях з надвисокими швидкостями. Така передача даних відбувається всередині периметра і, будучи невидимою для корпоративного брандмауера, відбувається абсолютно безперешкодно, без контролю і обмежень.

Далі співробітник бере пристрій із собою за межі офісу. Якщо цей пристрій загубиться або його вкрадуть, всі дані, передані на пристрій раніше в офісі, можуть бути отримані новим користувачем пристрою, будь воно зашифровано чи ні.

Персональні пристрої в даний час застосовуються набагато ширше, ніж тільки як засіб комунікацій. Прагнучі підвищити свою продуктивність, співробітники також створюють новий контент і на особистих пристроях. Як наслідок, виникає дилема «продуктивність проти безпеки» – зростання продуктивності співробітників є благом, але викликають певну стурбованість безпекою та цілісністю даних.

Розглянута проблема багато в чому повторює проблеми зберігання корпоративних даних на BYOD-пристроях, але слід звернути увагу і на іншу задачу – резервне копіювання корпоративних даних. Якщо нові документи і

дані створюються на персональному пристрої, організація змушена покладатися на свідомість співробітника, сподіваючись, що він самостійно подбає про створення резервних копій або своєчасно проведе синхронізації пристрою з робочим комп'ютером в офісі для забезпечення резервного копіювання належним чином на корпоративному рівні. Проблема, коли стратегія використання особистих пристроїв для підвищення продуктивності співробітників покладається на розумність і свідомість співробітників, але не на реальну техніку безпеки, продовжує існувати.

Тобто якщо до створення резервної копії пристрій загубиться, його вкрадуть, або дані на ньому будуть знищені (наприклад, віддалено MDM-системою) – можна вважати що нових напрацювань ніколи і не було.

Існує безліч різних додатків, у тому числі для мобільних платформ, здатних вирішувати різні завдання користувачів. Однак, якщо мобільний пристрій дозволяє співробітнику ефективно виконувати свої обов'язки і бізнес–функції, використання мобільних пристроїв для доступу та роботи з корпоративними даними не є кращим рішенням.

Якщо організація не є розробником програми для мобільного пристрою, швидше за все вона не може достовірно знати, як саме такий додаток працює з даними на пристрої, і не можете контролювати процес обробки даних додатком. Найчастіше, коли користувачі завантажують і встановлюють сторонні додатки на свої пристрої або використовують додаток вперше, вони повинні погодитися з тим, що додаток отримає доступ до даних на пристрої. Такий доступ зазвичай надається користувачами не замислюючись, більше того, як правило, вони навіть не читають умови ліцензійної угоди.

Для мобільних пристроїв, що працюють під управлінням операційних систем Android від Google або iOS від Apple, є й інші проблеми, що розширюють профіль загроз:

– користувачі мобільних пристроїв Android/iOS мають тенденцію встановлювати більше додатків третіх сторін, ніж ті, які користуються комп'ютерами на базі Windows. Чим більше додатків використовується на

мобільному пристрої, тим вище ймовірність, що принаймні один з встановлених додатків виявиться шкідливим, або буде мати істотні уразливості в системі безпеки;

– виток даних може бути зловмисно ініційований самими користувачами, який навмисно копіює корпоративну інформацію обмеженого доступу з своїх ПК на флеш-носії та інші компактні носії даних.

У той час, як деякі розробники MDM-рішень реалізують контроль мобільних додатків, дозволяючи користувачеві завантажувати і встановлювати тільки санкціоновані до застосування, продукти більшості лідерів галузі, MDM переходять до використання моделі віртуального секціонування додатків. Однак, і цей підхід буде залишатися, по суті, на півзаходом – до того часу, поки апаратні платформи мобільних пристроїв і програмні інтерфейси не еволюціонують в достатній мірі.

Деякі розробники систем управління мобільними пристроями (MDM) стверджують, що їх рішення забезпечують повноцінний захист від витоків даних в силу наявності функцій шифрування і знищення даних на пристрої. Але чи справді ці функції, саме те, що вимагають як внутрішні нормативні акти компаній, так вимоги регуляторів, спрямовані на забезпечення безпеки конфіденційних і важливих даних?

Розглядати MDM-системи як DLP-системи в рамках загальноприйнятої концепції безпеки некоректно, оскільки існують досить чіткі і акцентовані на безпеці даних визначення терміна Data Leak Prevention, встановлені галузевими аналітиками [21].

Виходячи із загальноприйнятого визначення, DLP-рішення має бути здатне аналізувати дані в станах «Передані дані» (data-in-motion), «Використовувані дані» (data-in-use), та/або «Збережені дані» (data-at-rest) по їх вмісту. Зазначені види аналізу даних, що мають вирішальне значення для виконання завдань контролю, моніторингу та забезпечення цілісності даних, просто відсутні в сучасних MDM-системах.

Крім того, для використання MDM-системи залишається актуальною проблема з недостатністю захисту від випадкових або навмисних витоків даних.

Слід також врахувати, що при тому, що MDM-системи мають довірений доступ до пристрою і збережених на ньому даних, вони не здатні забезпечити фільтрацію вихідних комунікацій або змінних носіїв, що підлягають ні по вмісту, ні по контексту користувача, даних або використовуваного каналу.

2.3 Комплексна стратегія вирішення проблемі безпеки при використання BYOD

Що стосується безпеки BYOD, будь-яка система управління мобільними пристроями (MDM) буде ефективна тільки в якості компонента в ширшій, комплексної стратегії забезпечення безпеки даних на мобільних пристроях. MDM–системи слід застосовувати для вирішення завдань загального управління і контролю мобільних пристроїв, шифрування даних.

Найбільш ефективним рішенням безпеки даних для пристроїв BYOD є надання доступу до інформаційних активів компанії через віддалене підключення BYOD-пристроїв через термінальні сесії до віртуальних Windows-середовищ, які в свою чергу захищені функціонуючої на хості DLP-системою, що забезпечує запобігання неконтрольованих витоків даних з хоста. Такий підхід називається Virtual Data Leak Prevention (vDLP).

Продуктивність користувачів і безпека

Підвищення продуктивності мобільних користувачів є основним обґрунтуванням для санкціонування компанією доступу до корпоративних даних з мобільних пристроїв. Високошвидкісне підключення до мережі і доступ до інформаційних активів компанії через віртуальні середовища не тільки вирішує проблему продуктивності мобільних співробітників в стратегії BYOD, але й істотно знижує ризики витоку даних. При цьому звичайні робочі місця, розміщені в офісі компаній, також повинні бути захищені від несанкціонованого використання змінних носіїв і USB-пристроїв, що

дозволяють непомітно для служб інформаційної безпеки скачувати корпоративні дані.

Технологія Virtual DLP пропонує контрольоване надання віддаленого доступу до корпоративних даних на відміну від локального зберігання даних на BYOD-пристроях в підході MDM.

При використанні віртуальних робочих середовищ співробітники отримують доступ до даних тільки після авторизації облікового запису в домені Active Directory (AD) чи іншому каталозі LDAP. Доступ надається через захищений VPN-тунель, який використовує у свою чергу строгу автентифікацію користувача та/або пристрою.

Таким чином забезпечується виконання трьох ключових умов безпеки:

– безпечна обробка даних – співробітники не використовують програми для локальної обробки даних на пристрої BYOD при підключенні до корпоративного порталу по безпечної сесії, або можливість використання даних блокується на контекстному рівні. Таким чином гарантується, що корпоративні дані компанії не будуть поширені далі контрольованого пристрою;

– безпечне зберігання даних – корпоративні дані що захищаються можуть бути доступні тільки у віртуальному середовищі, і в разі редагування або іншої зміни зберігаються тільки на сервері або можуть бути роздруковані на принтерах в корпоративній мережі – при цьому не допускається або контролюється локальне збереження даних у вбудованій пам'яті BYOD-пристроїв, що підключаються знімних накопичувачах, друк на принтерах поза корпоративної мережі. Оскільки корпоративні дані компанії існують тільки на серверах організації, а не на персональних пристроях, можливо забезпечити належний контроль і резервне копіювання на стороні організації;

– моніторинг даних – для кожної сесії співробітника Virtual DLP-рішення, яке функціонує в віртуальному середовищі Windows, забезпечує фільтрацію вмісту файлів і даних, що проходять через комунікаційні канали (електронна пошта, веб-сайти, клієнти миттєвих повідомлень т.д.), опубліковані додатки, канал друку, переслані диски і мережеві файлові ресурси, а також

знімні носії, доступ до яких дозволено програмним забезпеченням віртуального хостингу.

Мобільні співробітники потребують високої продуктивності, з чого випливає потреба співробітників у швидкій адаптації до моделі віртуалізації, підтримці різних видів віртуальних середовищ і виключення будь-яких непередбачених запитів на розширення функціональності віртуального середовища.

Це означає, що перелік розміщених у віртуальному середовищі додатків повинен включати в себе ті, які можуть якісно замінити додатки, які зазвичай використовуються для роботи з даними або для комунікацій в «локальному» режимі:

– браузер для роботи в Internet;
– Outlook або інший клієнт електронної пошти;
– дозволена в організації клієнти миттєвих повідомлень;
– Microsoft Office або інший продукт для роботи з документами різних типів;
– інші додатки, що використовуються в організації і необхідні для виконання посадових обов'язків.

Важливо відзначити, що при використанні сценаріїв віртуалізації робочого середовища також вирішується завдання забезпечення захисту даних завдяки тому, що корпоративні дані зберігаються тільки на серверах організації, які в свою чергу забезпечені належним захистом і регулярним резервним копіюванням. Таким чином, більша частина створюваного на мобільних пристроях контенту може бути гарантовано збережена для організації незалежно від того, на якому виді BYOD-пристрої були створені або змінені документи і дані.

При використанні рішення Virtual DLP всі програми, що працюють з корпоративними даними, запускаються всередині віртуальної Windows-сесії, тобто по суті існують тільки на «домашньому» сервері організації. При такому підході співробітники можуть вільно використовувати опубліковані на сервері

віртуалізації програми, необхідні їм для роботи, при цьому служба інформаційної безпеки зберігає повний контроль над робочими даними, оскільки збереження відбувається не на пристрої BYOD, а на сервері.

MDM-системи відіграють значну роль у забезпеченні безпеки стратегії BYOD, але слід знову чітко позначити, що при цьому вони не виконують завдання запобігання витоків даних.

Для створення повноцінного та ефективного вирішення щодо запобігання витоків даних з мобільних пристроїв MDM-системи повинні працювати спільно з резидентними DLP-системами.

Спеціалізовані DLP-рішення можуть допомогти організації, що вирішує питання швидкої інтеграції персональних мобільних пристроїв в технічні бізнес-процеси, в задачах виявлення критично важливих для бізнесу даних, визначення правил роботи, зберігання і передачі даних за межі компанії (або всередині компанії).

Персональних мобільних пристроїв, що проникають всередину корпоративного мережевого периметра, стає все більше – це смартфони, планшети, флеш-носії, цифрові камери, і навіть MP3-плеєри. Активний розвиток мережевих сервісів і додатків, широке поширення і загальнодоступність «хмарних» сховищ і соціальних мереж також істотно підвищує ризики неконтрольованих витоків даних. Для вирішення цієї проблеми і призначені спеціалізовані резидентні DLP-системи.

Ефективний захист від витоків даних передбачає контроль на різних рівнях і різними методами (як заснованими на контексті даних, так і на аналізі вмісту файлів і даних) в поєднанні з вибірковістю застосування технологій контролю для найширшого спектра потенційних каналів витоку даних.

Чимала частина каналів витоку безпосередньо пов'язана з підключенням різних пристроїв через порт USB, з чого випливає обов'язковість використання контекстних методів контролю та фільтрації підключення через USB пристрїв скрізь, де це підключення може призвести до обміну даними між пристроєм і робочою станцією. Фахівці з інформаційної безпеки повинні визначати права

доступу для користувачів і груп відповідно до їх функціональних обов'язків, щоб досягти балансу між продуктивністю використання персональних пристроїв для роботи і зниженням ризиків витоків.

2.4 Побудова профілю захищеності

Розглянемо найбільш популярне на теперішній час рішення впровадження концепції BYOD на підприємстві, з допомогою систем класу MDM (управління мобільними пристроями), що існує на українському ринку, та відобразимо виконання вибраних нами послуг стандартного функціональному профілю захищеності 3.КЦД.1 в комп'ютерній системі, що входить до складу автоматизованої системи класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації (таблиця 2.5):

3.КЦД.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Відповідно до нормативного документу системи технічного захисту інформації 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» детальніше розглянемо кожну з послуг функціонального профілю захищеності, оцінімо існуючий стан захищеності інформації з обмеженим доступом, відобразимо способи за допомогою яких послуги даного профілю реалізуються в системі.

Таблиця 2.1 – Функціональний профіль захищеності інформації

Критерій	Послуга безпеки	Рівень послуги безпеки
Конфіденційність	Базова довірча конфіденційність	КД-2
	Повторне використання об'єктів	КО-1
	Мінімальна конфіденційність при обміні	КВ-1
Цілісність	Мінімальна довірча цілісність	ЦД-1
	Обмежений відкат	ЦО-1
	Мінімальна цілісність при обміні	ЦВ-1
Доступність	Квоти	ДР-1
	Ручне відновлення	ДВ-1
Спостережність	Захищений журнал	НР-2

	Однонаправлений достовірний канал	НИ-2
	КЗЗ з гарантованою цілісністю	НК-1
	Одиночна ідентифікація і автентифікація	НО-2
	Розподіл обов'язків адміністраторів	НЦ-2
	Самотестування при старті	НТ-2
	Автентифікація вузла	НВ-1

Для підвищення рівня захищеності інформації вирішено підняти рівень послуги НР-2 «Захищений журнал» до рівня НР-3 «Сигналізація про небезпеку», тому що адміністратор безпеки повинен мати можливість відстежувати зміни ПЗ мобільного пристрою, що стосується захищеності ІзОД. А також до профілю захищеності включити послугу КК-1 «Виявлення прихованих каналів», тому що існує потенційна небезпека появи прихованого каналу передачі даних (ІзОД) між корпоративним і персональним профілями користувача ІКС.

2.5 Оцінка існуючого стану захищеності ОІД

Перевіримо стан захищеності АС, спираючись на методику, запропоновану у документах та вимоги до функціональних послуг безпеки [22].

КД-2. Базова довірча конфіденційність

Послуга довірча конфіденційність дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Під об’єктами що належать домену користувача мається на увазі ті об’єкти власником яких є користувач (створені користувачем).

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.

КО-1. Повторне використання об'єктів

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

КК-1. Виявлення прихованих каналів

Повинен бути виконаний аналіз прихованих каналів

Всі приховані канали, які існують в апаратному і програмному забезпеченні, а також в програмах ПЗП, повинні бути документовані

Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або

вимірів

Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність

КВ-1. Мінімальна 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.

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.

ЦД-1. 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.

ЦО-1. Обмежений відкат

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану забезпечується відкат.

Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

ЦВ-1. Мінімальна 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.

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.

ДР-1. Квоти

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів.

Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу.

Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

ДВ-1. Ручне відновлення

Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування.

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС.

Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

НР-3. Сигналізація про небезпеку

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ран жируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються.

КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки.

Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації

НИ-2. Одиночна ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС.

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.

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

НК-1. Однонаправлений достовірний канал

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ран жируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

Однонаправлений достовірний канал дозволяє користувачу безпосередньо взаємодіяти з КЗЗ.

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ.

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

НО-1. Виділення адміністратора

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування.

Виділення адміністратора дозволить зменшити потенційні збитки від навмисних або помилкових дій користувача.

Політика розподілу обов’язків, що реалізується КЗЗ, повинна виділяти ролі адміністратора і звичайного користувача і призначені їм функції.

Послуга реалізована на рівні НО-2. Серед переліку ролей ОЕ існує декілька ролей, що користувачів що виконують адміністративні операції (адміністратор мережі, адміністратор серверу, адміністратор бази даних).

НЦ-2. КЗЗ з гарантованою цілісністю

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами. Послуга характеризує міну здатність КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об’єктами.

Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ.

В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

НТ-2. Самотестування при старті

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ран жируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС.

Політика самотестування, що реалізується КЗЗ, повинна містити властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

Послуга не реалізована оскільки відсутня політика самотестування, яка описувала б властивості ОС та реалізована ні процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

НВ-1: Автентифікація вузла

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію.

Ця послуга дає можливість забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем [22].

НР-3. Сигналізація про небезпеку

Реєстрація дозволяє контролювати небезпечні для КС дії КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки КС. КЗЗ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій

Таблиця 2.2 – Реалізація послуг безпеки

Критерій	Рівень послуги безпеки	Чим реалізується
Конфіденційність	КД-2	Active Directory ОС Windows
	КО-1	Не реалізується
	КВ-1	Служби криптографії ОС Windows
	КК-1	Не реалізується
Цілісність	ЦД-1	Служби криптографії та Active Directory ОС Windows
	ЦО-1	Створення точки відновлення ОС Windows
	ЦВ-1	Служби криптографії ОС Windows
Доступність	ДР-1	Active Directory ОС Windows

	ДВ-1	Windows Task Manager ОС Windows
Спостережність	НР-2	Служба журналів подій ОС Windows
	НИ-2	Протокол Kerberos v5 ОС Windows
	НК-1	Не реалізується

Продовження таблиці 2.2

Критерій	Рівень послуги безпеки	Чим реалізується
	НО-2	Створення облікових записів ОС Windows з різними повноваженнями
	НЦ-2	Не реалізується
	НТ-2	Процедура POST ОС Windows
	НВ-1	Служби криптографії ОС Windows

1 Active Directory ОС Windows – («Активний каталог», AD) – LDAP-сумісна реалізація служби каталогів корпорації Microsoft для операційних систем сімейства Windows NT. Active Directory дозволяє адміністраторам використовувати групові політики для забезпечення однаковості налаштування користувальницького робочого середовища, розгортати програмне забезпечення на безлічі комп'ютерів через групові політики або за допомогою System Center Configuration Manager (раніше Microsoft Systems Management Server), встановлювати оновлення операційної системи, прикладного та серверного програмного забезпечення на всіх комп'ютерах в мережі, використовуючи Службу поновлення Windows Server. Active Directory зберігає дані і налаштування середовища в централізованій базі даних. Мережі Active Directory можуть бути різного розміру: від декількох десятків до декількох мільйонів об'єктів.

2 Служби криптографії ОС Windows – представлені трьома службами управління: службою баз даних каталога, яка перевіряє цифрові підписи файлів Windows; службою захищеного кореня, яка додає і видаляє сертифікати довіреної кореня центру сертифікації з цього комп'ютера; і службою ключів, яка дозволяє подавати заявки на сертифікати з цього комп'ютера. Якщо ця служба зупинена, всі ці служби управління не працюватимуть. Ця служба перевіряє підписи файлів Windows. Однак, все одно можливо отримувати вікно з попередженням про непідписаний драйвер. Ця служба необхідна для оновлення Windows в ручному та автоматичному режимах, а також для інсталяції Service Pack'ов і DirectX 9.0. Windows Media Player і деякі .NET додатки можуть вимагати цю службу для функціонування деяких функцій. Служба займає близько 1.9 Мб в оперативній пам'яті.

Назва служби: CryptSvc

Назва процесу: svchost.exe

Windows XP Home: Автоматично

Windows XP Pro: Автоматично

Рекомендоване значення: Автоматично

Вхід від імені: Локальна система

3 Створення точки відновлення ОС Windows – образ системи – це точна копія диска. Образ системи включає диски, необхідні для запуску Windows.

Він також містить файли, програми та налаштування системи Windows, а також ваші файли, програми та налаштування. Образ системи можна використати, щоб відновити вміст комп’ютера, якщо жорсткий диск чи комп’ютер вийде з ладу. Відновлення комп’ютера з образу системи – це повне відновлення; не можна вибрати окремі елементи для відновлення, і всі поточні файли, програми та настройки системи замінюються вмістом образу системи.

Цей тип резервного копіювання містить особисті файли, рекомендується періодично створювати резервні копії файлів за допомогою архівації Windows, щоб у разі потреби можна було відновити окремі файли та папки. Під час налаштування архівації Windows можливо вибирати елементи, резервну копію

яких потрібно створити, разом з образом системи, або ви можете вибрати елементи, резервну копію яких потрібно створити, а також вказати, чи слід включати образ системи.

Якщо комп’ютер має кілька дисків або розділів, можна створити образ системи, який міститиме їх усі, виконавши дії, наведені в розділі Резервне копіювання файлів, програм і налаштування системи.

4 Диспетчер задач ОС Windows – утиліта для виведення на екран списку запущених процесів і споживаних ними ресурсів (зокрема статус, процесорний час і споживана оперативна пам'ять). Також є можливість деякої маніпуляції процесами.

5 Служба журналів подій ОС Windows – (Event Log) в Microsoft Windows стандартний спосіб для додатків і операційної системи запису і централізованого зберігання інформації про важливі програмні і апаратні події. Служба журналів подій зберігає події від різних джерел в єдиному журналі подій, програма перегляду подій дозволяє користувачеві спостерігати за журналом подій, програмний інтерфейс (API) дозволяє додаткам записувати в журнал інформацію і переглядати існуючі записи.

6 Протокол Kerberos v5 ОС Windows – орієнтований в основному на клієнт-серверну архітектуру, запропоновує механізм взаємної автентіфікації двох співрозмовніків (хостів) перед встановленням зв'язку між ними в умовах незахіщеного каналу. Kerberos – це також пакет вільного програмного забезпечення, розроблений в Массачусетському технологічному інституті, що реалізовує цей протокол. Повідомлення протоколу Kerberos захищені проти прослуховування мережі та повторних атак (англ. «replay attack»).

Kerberos базується на симетричних алгоритмах шіфрування та для своєї роботи потребує довірену третю сторону. Деякі модіфікації протоколу можуть використовувати елементи асиметричного шифрування.

7 Створення облікових записів ОС Windows – запис, що містить відомості, які користувач повідомляє про себе деякій комп'ютерній системі.

8 Процедура POST ОС Windows – (англ. Power-On Self-Test) – самотестування після ввімкнення. Перевірка апаратного забезпечення комп'ютера, виконувана при його включенні. Виконується програмами, що входять в BIOS материнської плати.

Функції, аналогічні POST комп'ютера, характерні для багатьох сучасних електронних пристроїв.

Вибір між проходженням повного або скороченого набору тестів при включенні комп'ютера можна задати в програмі налаштувань базової системи введення-виведення.

У більшості персональних комп'ютерів у разі успішного проходження POST системний динамік видає один короткий звуковий сигнал, у разі збою – різні послідовності звукових сигналів. Крім того, BIOS генерує код поточного стану завантаження (і, в разі збою, відповідно помилки), який можна дізнатися за допомогою комбінації світлодіодів або семисегментних індикаторів (на деяких материнських платах), а також на POST Card, яка вставляється в слот розширення на материнській платі (або вже вбудована в неї) і відображає код помилки на своєму індикаторі. POST-карта, що дозволяє діагностувати неполадки на стадії запуску комп'ютера.

Зіставити конкретний звуковий код, текстове повідомлення на моніторі або код POST з причиною збою під час завантаження комп'ютера можна по документації виробника BIOS, материнської плати або додаткової плати контролера пристрою.

2.6 Рішення для реалізації невиконаних умов профілю

Реалізація невиконаних умов профілю розглядається в таблиці 2.3

Рівень послуги безпеки	**Чим реалізується**
КО-1	ПЗ Ccleaner v 4.13
КК-1	VM, App, DLP, MDM
НР-3	Криптографічний сервер «Славутич», MDM, AES-256
НК-1	VPN, MDM

НЦ-2	Криптографічний сервер «Славутич»

Таблиця 2.3 – Реалізація послуг безпеки

Безпека BYOD = MDM + App + VPN + VM + DLP

1 ПЗ Ccleaner v 4.13 – CCleaner (раніше – Crap Cleaner) – це безкоштовна утиліта з закритим вихідним кодом, яка надає користувачам потужний і простий у використанні інструмент для очищення і оптимізації 32-бітних і 64-розрядних операційних систем Microsoft Windows. Утиліта була створена британської приватною фірмою Piriform Limited і написана на мові C++.

2 VM – віртуальна реалізація Windows-системи, що надає користувачам робоче середовище, в якому можуть бути опубліковані і доступні необхідні для роботи програми і дані, частково реалізуємо послугу виявлення прихованого канала КК-1.

3 App – додаток для віддаленого підключення мобільного пристрою через мережу Інтернет до віртуального хостингу додатків організації (додатки з сайта Держспецзв'язку), з допомогою яких реалізуємо послугу виявлення прихованих каналів, повторне використання об'єктів (ПЗ для очистки оперативної пам'яті).

4 DLP – система запобігання витоків даних, інтегрована у віртуальне робоче середовище Windows, що забезпечує контроль доступних в цьому віртуальному середовищі каналів передачі даних (електронна пошта, веб-сайти, програми швидкого обміну повідомленнями, канали друку, переслані у віртуальне середовище локальні USB–пристрої) для запобігання витоків даних з BYOD–пристроїв.

5 MDM – система рішення Mobile Device Management це програмне забезпечення, завдяки якому можна забезпечити, контроль і підтримку мобільних пристроїв, що використовуються співробітниками компаній для роботи в корпоративних системах. MDM-рішення дозволяють бізнесу захистити корпоративну інформацію від сторонніх осіб, оскільки правила безпеки прописані для всіх пристроїв, що підключаються до IT-систем

компанії. Для контролю локальних додатків на пристроях, віддаленого знищення даних.

6 Криптографічний сервер «Славутич»

Криптографічний сервер «СЛАВУТИЧ» призначений для:

– захисту TCP/IP з’єднань «клієнтів» з «серверами» за допомогою шифрування запитів "клієнтів" та "відповідей" серверів;

– перевірки цілісності даних за рахунок перевірки хеш-коду;

– автентифікації криптографічних серверів «СЛАВУТИЧ».

За допомогою криптографічного сервера «СЛАВУТИЧ» можливо забезпечити захист загальнодоступних серверів від сторонніх користувачів, які не мають доступу до сервера, гарантувати «клієнтам» та «серверам» конфіденційність передачі даних та їх цілісність. Криптографічний сервер «СЛАВУТИЧ» являє собою програмний засіб, який дозволяє виконувати функції ідентифікації, контролю цілісності, автентифікації та приховування змісту даних, які передаються між «клієнтами» та «серверами» в загальнодоступних мережах.

До складу криптографічного сервера «СЛАВУТИЧ» входять: програмний засіб криптографічного сервера, технічно-експлуатаційна, регламентуюча та інша документація.

7 VPN (Hamachi) – захищене криптографічним протоколом SSL підключення до віртуальної приватної мережі організації (Virtual Private Network), що використовується опублікованими додатками, в тому числі для додаткової автентифікації користувачів. З допомогою чого реалізуємо шифрування даних, що передаються, та організуємо конфіденційність даних при обміні.

2.7 Кроки на шляху впровадження BYOD

Співробітники організацій хочуть і будуть використовувати свої власні пристрої на робочому місці. Більше того, вони вже їх використовують і роблять це далеко не перший день.

Найбільші побоювання у IT-керівників викликають питання безпеки, зокрема доступ до конфіденційної інформації і можливість її витоку за межі організації. У співробітників десятиліттями був і є доступ до конфіденційної інформації, а наявність компакт-дисків, USB, пересилання електронною поштою, камер на мобільних телефонах, копіювальних апаратів, ручок та паперу робили можливим виток інформації.

У квітні 2017 року компанія iPass випустила звіт Global Mobile Workforce Report з результатами опитування більш ніж 5300 співробітників в 1100 організаціях по всьому світу. Дослідження показало, що всього 27% працівників з планшетними комп'ютерами отримали їх від компанії, в якій працюють. Решта 73% використовують для роботи власні планшети. 94% мають смартфони, причому господарі як смартфонів, так і планшетів застосовують їх не лише для читання електронної пошти, а й для інших завдань [23].

Має сенс дослідити значення BYOD для управління IT-сервісами. Ряд ключових областей IT Service Management (управління IT-послугами, ITSM) відіграють певну роль при застосуванні підходу BYOD. Його слід сприймати як будь-який інший сервіс, проте він має свої відмінні особливості.

Сервісна стратегія

Необхідно ретельно обміркувати наслідки прийняття стратегії BYOD, що стосуються юридичних, фінансових, кадрових питань та необхідності відповідати вимогам, зазначеним в угоді про рівень обслуговування. Підхід «визначати, аналізувати, стверджувати і надавати», використовуваний при управлінні портфелем сервісів, слід застосовувати до сервісу BYOD, як і до всіх інших сервісів.

Необхідно визначити реальний попит на сервіс BYOD всередині організації, а також зрозуміти фінансові наслідки прийняття підходу BYOD.

Стратегія BYOD зробить вплив на корпоративні політики та процедури щодо використання особистих пристроїв, причому ці політики будуть

відрізнятися в різних країнах внаслідок відмінностей у законах про захист конфіденційних даних, оподаткування, робочих практиках і т. д.

Управління фінансами

Необхідно вивчити фінансові аспекти підходу BYOD, такі як витрати, повернення інвестицій (ROI) і отримана цінність (ROV). Одночасно з

скороченням закупівлі апаратного забезпечення та економії на його підтримці можливе також збільшення витрат на системи безпеки, адміністрування та інвестиції в інфраструктуру.

З боку організації можливе надання різних пільгових умов, пов'язаних з обладнанням, наприклад безвідсоткові кредити для співробітників на купівлю нових комп'ютерів, регулярні виплати і т. д., а також оплата додатків, придбаних для вирішення завдань, пов'язаних з роботою. Всі ці додаткові витрати необхідно зіставити з економією на закупівлю обладнання та оплати підтримки при використанні підходу BYOD, а також з отриманою цінністю від участі, задоволеності, продуктивності та збереження лояльності співробітників.

2.8 Політики впровадження BYOD

Застосування стратегії BYOD буде ключовим чином впливати на створення корпоративних політик і процедур. Ці політики повинні включати в себе як мінімум наступне [24]:

– термінологію для пояснення співробітникам відповідальності, яка на них накладається, коли вони отримують безперервний доступ до устаткування, використовуваного для вирішення робочих завдань;

– мінімальні вимоги до апаратного забезпечення і ОС;

– інформацію про те, хто, скільки і на що (апаратне забезпечення, ПО, підтримка) повинен витратити матеріальних коштів;

– інформацію про те, що буде, а що не буде підтримуватися силами IT–підрозділу;

– політики віддаленого доступу і політики безпеки;

– рівні допустимого доступу до даних;

– способи безпечного зберігання даних компанії;

– необхідні дії у разі, якщо пристрій вкрадено;
– необхідні дії у разі звільнення співробітника;
– фінансові зобов'язання компанії та співробітника;
– видалення даних з жорсткого диска пристрою.

На додаток до перерахованих рекомендацій потрібно, щоб політики процесу управління інформаційною безпекою ясно описували дії, які необхідно здійснювати, якщо мобільний пристрій буде загублено або якщо співробітник вирішить покинути компанію. Наприклад, організація в даній ситуації може залишити за собою право стерти з мобільного пристрою корпоративні дані або взагалі всі дані.

В рамках процесів управління доступом та управління інформаційною безпекою можуть бути згенеровано одноразові коди доступу з обмеженим часом дії. Варто також заздалегідь визначити, дотримання яких процедур очікується від співробітника при використанні особистого мобільного пристрою. Наприклад, можна зажадати наявності встановленого антивірусного захисту певного рівня на будь-якому мобільному пристрої, який використовується співробітником в робочих цілях.

Компанія може встановити додаткові вимоги до персональних пристроїв співробітників, зокрема, можуть бути задані обмеження на тривалість гарантійного періоду, який надається постачальником або виробником пристрою.

Контрольний список, що стосується безпеки в рамках стратегії BYOD, який включає наступні рекомендації:

– використовувати для BYOD-пристроїв ті ж налаштування, що і для зовнішніх пристроїв, що підключаються до мережі;
– дозволити підключення BYOD-пристроїв тільки після їх «чистки» IT–адміністраторами;
– розглянути можливість використання окремої закритої віртуальної машини для робочих цілей;

– заборонити зберігання корпоративних даних на пристроях і надати доступ до захищеного хмарному сервісу, як альтернативу;

– заборонити використання пристроїв, які зазнали модифікацію ПЗ;

– вимагати застосування шифрування;

– блокувати конфіденційні документи залежно від типу пристрою або тимчасових обмежень.

Проектна документація сервісу

Проектна документація сервісу повинна бути розроблена з особливим акцентом на питання безпеки, що стосуються сервісу, на пов'язані з ним технологічні стандарти, динаміку сервісу, вимоги до підтримки і вимоги до

рівня обслуговування. У цю документацію повинні входити як мінімум:

– вимоги (бізнес-вимоги, як і де сервіс повинен використовуватися, контактні дані);

– проект сервісу (функціональні вимоги; вимоги до рівня обслуговування, вимоги до операційного управління, проектні вимоги сервісу, очікувані результати, в тому числі фінансові);

– оцінка готовності організації;

– план життєвого циклу (загальна програма сервісу, план перетворення сервісів (включаючи всі вимоги до тестування), операційний план прийому з критеріями прийому).

Вимоги до проектування сервісів повинні включати сервісну модель, що описує структуру сервісу, тобто як всі компоненти пов'язані і яким чином вони взаємодіють один з одним. Саме тут слід врахувати, які пристрої можуть підтримувати ті чи інші бізнес -сервіси. Наприклад, смартфон або планшет може бути використаний для доступу до деяких бізнес-сервісів, але не до всіх. Динаміку розвитку сервісу необхідно фіксувати, вона може стати частиною системи управління конфігураціями.

Управління каталогом сервісів

Сервіс BYOD необхідно включити в каталог сервісів, який повинен відображати як мінімум наступні його характеристики:

– що включає в себе сервіс;

– стандартні для сервісів деталі та опції;

– будь-які винятки, що стосуються сервісу;

– хто має право на отримання цього сервіс;

– рівні авторизації та узгодження, необхідні для отримання можливості користуватися сервісами;

– зобов'язання, що накладаються на користувача, включаючи посилання на відповідні політики;

– витрати (наприклад, на підтримку), які може нести співробітник;

– можливі компенсації, такі як посібник на використання власного пристрою і закупівлю додатків для вирішення робочих завдань;

– час надання сервісу і час роботи служби підтримки;

– контактні дані для отримання більш докладної інформації по сервісу (включаючи можливість скарг та пропозицій).

Управління рівнем обслуговування

Організації доведеться розглядати цільові рівні обслуговування для різних пристроїв, використання яких допускає концепція BYOD, причому слід враховувати такі параметри, як можливість підключення до корпоративної мережі і постійна технічна підтримка. Обов'язки як співробітника, так і організації повинні бути визначені в угоді про рівень обслуговування (Service Level Agreement, SLA). Скажімо, первинна підтримка з питань підключення може надаватися тільки при прийнятті умов надання сервісу, що включають забезпечення заданого рівня безпеки на пристрої і трирічну гарантію на пристрій від виробника. Якщо компанія не надає додаткової підтримки для особистого пристрої співробітника, крім первинного підключення, це повинно бути чітко вказано.

Угода про рівень обслуговування повинна ясно відображати політику BYOD, рівні та умови підтримки, ціни і т. д., використовуючи як посилання на відповідну інформацію, так і безпосередньо текст угоди.

Управління релізами і розгортанням

Рекомендується використовувати поетапний підхід до розгортання сервісу, щоб протестувати, перевірити і оцінити результати допуску кожного конкретного типу пристроїв до мережі організації.

З появою доступу необхідно провести тестування з метою реєстрації можливості або неможливості використання кожного типу пристрою для отримання всіх видів сервісів, до яких дозволено підключення.

Тестування повинне включати якомога більше сценаріїв з безпеки, щоб гарантувати, що головному «неспокою», принесеному сервісом, приділено достатньо уваги.

Управління змінами

Якщо адаптація співробітників проходить в рамках процесу управління змінами, слід створити запит на зміну, який відповідатиме за прийняття кожним співробітником політики BYOD. Це має забезпечити перевірку того факту, що співробітник прочитав і підписався під політикою BYOD до того, як йому буде надано доступ до IT -ресурсів.

Все це також повинно застосовуватися до співробітників, які переходять на використання пристроїв за принципом BYOD. Конфігураційні одиниці, пов'язані з співробітниками, повинні відображати факт використання ними сервісу BYOD.

Управління сервісними активами і конфігураціями

Якщо співробітники організації враховуються як конфігураційні одиниці, слід додати їм атрибут, який вказує, чи використовують вони обчислювальні

потужності організації (і якщо так, то що саме) або ж працюють зі своїми особистими пристроями. Це дозволить будувати звітність і відслідковувати по ній зміну з часом частки співробітників, що користуються сервісом BYOD. Аналіз даної тенденції дозволяє прогнозувати кількість співробітників, які будуть використовувати сервіс BYOD в майбутньому, і тому дає уявлення про те, як багато обчислювальної техніки знадобиться організації надалі. Це дає матеріал для управління запасними обчислювальними ресурсами у разі збою в особистому пристрої співробітника.

Слід також перевірити поточні ліцензії на ПЗ, щоб забезпечити організації можливість надання співробітникам доступу до будь-якого ліцензованого ПЗ, яке їм необхідно при використанні персональних комп'ютерів в мережі підприємства.

Управління попитом

Необхідно проводити дослідження для визначення і передбачення масштабу використання пристроїв за принципом BYOD в компанії.

Вплив може надати і ступінь мобільності працівників: більш мобільним співробітникам може бути зручніше використовувати пристрої за принципом BYOD, ніж мати стаціонарне робоче місце. Ще одним важливим фактором є рівень комп'ютерної грамотності співробітників організації.

При плануванні та втіленні в життя підходу BYOD необхідно враховувати всі ці фактори, щоб оцінити рівень потужності обчислювальних пристроїв, які організації потрібно буде забезпечити як для нормальної операційної діяльності, так і для надання запасних пристроїв у разі виникнення збоїв у роботі пристроїв співробітників. У політиці BYOD має бути зазначено, що у разі неможливості виконання співробітником покладених на нього обов'язків за допомогою свого особистого пристрої йому буде надано необхідний пристрій з власності організації доти, поки співробітник не зможе користуватися своїм пристроєм знову.Також необхідно встановити баланс між бажанням персоналу використовувати свої особисті пристрої за принципом BYOD і складністю для служби підтримки в супроводі великої кількості різних і незнайомих пристроїв.

Підтримка користувачів і служба Service Desk

Повинно бути досягнуто ясне взаєморозуміння між службою Service Desk і співробітниками компанії в питанні про те, що саме підтримується при використанні особистих пристроїв за принципом BYOD. Все це повинно бути визначено в політиці.

Ряд контрольних прийомів, серед них [25]:

– підтримка BYOD-пристроїв з обмеженням за часом на кожен пристрій (наприклад, не більше 30 хвилин);

– підтримка, при якій співробітники сервісної служби вживають розумні спроби для вирішення інциденту, розуміючи водночас, що збої, пов'язані з BYOD-пристроями, є особистими проблемами власника пристрою;

– обмеження підтримки з технічних областям, коли за деякими технологіями підтримка здійснюється, а по деяким ні;

– наявність набору запасних пристроїв, з яких співробітник може тимчасово взяти замінити зламаний пристрій;

– підтримка силами спільноти, тобто з можливістю обміну між співробітниками інформацією та досвідом за допомогою поштових розсилок, корпоративних соціальних мереж;

– надання підтримки за контрактами, укладеними зі сторонніми сервісними організаціями;

– повний аутсорсинг служби підтримки;

– навчання та проведення тренінгів для співробітників з метою познайомити їх з найбільш часто виникаючими неполадками і способами боротьби з ними, а також політиками BYOD і накладеної на співробітників відповідальністю.

Головне, щоб кордони були чітко визначені і всіма зрозумілі. Потрібно визначити, на якому рівні підтримки надаватиметься технічний супровід для особистих пристроїв співробітників, а також сформулювати мінімальні вимоги

до пристрою для дозволу підключення до корпоративної мережі.

Служба Service Desk і співробітники, що забезпечують підтримку користувачів, повинні чітко уявляти, що підтримується силами IT, що підтримується силами сторонніх компаній і які обов'язки накладаються на співробітників, що використовують сервіс BYOD.

Співробітники повинні розуміти, який рівень доступу до їх персональних

пристроїв і даних, що зберігаються на них, вимагає організація. Це має бути визначено за участю відділу кадрів і включено в політику. Наприклад, чи може компанія, використовуючи недоліки програмного коду, стежити за діями

співробітниками? Якщо пристрій було втрачено або була виявлена вразливість в системі безпеки, чи може організація стерти всі дані з пристрою або з стертих даних будуть виключені персональні дані співробітника?

У Service Desk і співробітників, що займаються підтримкою користувачів, повинні бути необхідні знання та інструменти.

Управління постачальниками

Організація може розглянути варіант, коли співробітникам, які працюють за принципом BYOD, технічна підтримка надається сторонньою організацією.

У звіті «Checklist for an Employee – Owned Notebook or PC Program» аналітики Gartner наводять деякі поради щодо сторонньої служби підтримки та міркування з обслуговування.[26]

Однією з головних переваг від використання співробітниками своїх персональних пристроїв є полегшення роботи служби підтримки при налаштуванні цих пристроїв або вирішенні інцидентів з нестандартними програмами.

Проте найбільш важливим є принцип, за яким співробітники мають пристрої, які підходять для виконання робочих завдань, в будь-який час. Якщо такі пристрої ламаються, то співробітник повинен звідкись отримати підтримку.

Кращою практикою в цій галузі є організація для учасників ініціативи BYOD відповідних варіантів підтримки від сторонньої організації. Таке обслуговування може здійснюватися спеціалізованими компаніями, що займаються підтримкою, або виробниками ПК. На додаток до апаратного забезпечення план з надання підтримки повинен включати в себе підтримку з питань ОС і ПЗ, так само як і з питань роботи домашньої мережі і принтерів.

Дії компанії:

– під час роботи з пілотної версії плану компанія може виплачувати всю суму (або її частину), затрачену на підтримку, у вигляді компенсації співробітникам;

– компанії можуть надавати програмні системи, завантажені з образу, що належить компанії, співробітникам «напрокат». Ця стратегія дозволяє зберегти продуктивність співробітників на період налаштування їх власних пристроїв.

Слід зазначити, що повинна бути окрема VIP–програма підтримки для ТОП–менеджерів, яким необхідно більш швидке і персоналізоване обслуговування. Щоб забезпечити адекватне фінансування, вищі керівники повинні платити за дану послугу.

При взаємодії з постачальниками слід розвивати різні варіанти підтримки в області BYOD і вибирати той варіант, який доступний організації і найбільшою мірою задовольняє її вимогам.

Управління знаннями

В умовах, коли використовується велика кількість різних пристроїв, управління знаннями має ключове значення. Як мінімум буде вимагатися підтримка з питань підключення конкретних пристроїв до мережі організації, тому база знань повинна містити відповідні інструкції.

Також база знань повинна включати деталі політики BYOD і вимоги до співробітників, мінімальні специфікації пристроїв, обов'язковий гарантійний період.

При появі нового типу пристроїв у співробітників, необхідно провести оновлення бази знань інформацією про те, як підключити цей пристрій до мережі організації.

Інструменти спільної роботи також дозволяють співробітникам отримувати доступ до знань і досвіду їх колег у випадках, коли виникають якісь складнощі. Хороші інструменти спільної роботи і повноцінна, актуальна і точна база знань можуть радикально зменшити потребу в допомозі, що надається співробітниками Service Desk з питань BYOD.

2.8 Висновок

Оскільки мобільні пристрої найчастіше використовуються за межами захищених офісних мереж, традиційні компоненти безпеки не можуть забезпечити належні контроль і моніторинг комунікацій з мобільних пристроїв. Крім того, залишається ризики фізичної втрати або крадіжки мобільних пристроїв.

Ефективна стратегія BYOD полягає не тільки в управлінні, відстеження і знищенні даних на пристроях при необхідності, але і в запобіганні витоків даних з мобільних пристроїв. При цьому слід використовувати як контекстні, так і контенті методи контролю даних.

У користувачів будуть виникати проблеми, що вони не завжди зможуть отримати достатній доступ до даних, стикатимуться з нестачею пропускної здатності каналу або відсутністю мережевого підключення поза офісом (наприклад, в літаку, в країнах третього світу), а значить, повинні мати можливість зберігати корпоративні дані локально на персональних мобільних пристроях. І цілком припустимі ситуації, коли це буде виправдано. Тим не менше, для більшості організацій приведене дане комплексне рішення захисту інформації виявиться більш компромісною, ніж реальний ризик втратити даних обмеженого доступу, і як наслідок – ризик падіння престижу і репутації компанії, зрив угод, великі штрафи або інших санкцій при порушенні вимог регуляторів.

В спеціальній частині дипломної роботи магістра проаналізовано ефективність наведених рішень впровадження технології BYOD, обрано функціональний профіль захищеності ІзОД від НСД, та проведене дослідження реалізації послуг сформованого функціонально профілю захищеності обраним рішенням. Було надано рекомендацій щодо реалізації послуг профілю, вимоги які не виконуються. Розроблене комплексне рішення впровадження BYOD. Також буди розроблені політики впровадження та застосування концепції BYOD в організації.

3. ЕКОНОМІЧНИЙ РОЗДІЛ

Bring your own device (BYOD) - це IT-політика, згідно з якою співробітникам дозволено або рекомендується використовувати особисті мобільні пристрої (телефони, планшети, ноутбуки) для доступу до корпоративних даних та систем.

Застосування технології «Bring your own device» зменшує технологічні витрати для компаній польового обслуговування - BYOD переносить витрати на працівника, заощаджуючи кошти на придбанні пристроїв, а також на щомісячній сплаті службових послуг. Навіть субсидіювання особистих мобільних пристроїв працівників коштує набагато менше, ніж покупка пристроїв, сплачених повністю за допомогою мобільної ініціативи компанії.

Метою розділу є економічне обґрунтування підвищення рівня захищеності інформаційно-телекомунікаційної системи із технологією «Bring Your Own Device». Для цього необхідно здійснити розрахунок:

– капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування;

– річного економічного ефекту;

– показників економічної ефективності застосування технології технологією «Bring Your Own Device».

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

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

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, $К_{пр}$=10000 грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, $К_{аз}$=45000 грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

Впровадження технології «Bring Your Own Device» передбачає організацію для учасників ініціативи BYOD відповідних варіантів підтримки від сторонньої організації. Таке обслуговування може здійснюватися спеціалізованими компаніями, що займаються підтримкою, або виробниками ПК. На додаток до апаратного забезпечення план з надання підтримки повинен включати в себе підтримку з питань ОС і ПЗ, так само як і з питань роботи домашньої мережі і принтерів. Вартість послуг залучення сторонніх організацій на етапі провадження технології «Bring Your Own Device» складає в середньому 10000 грн.

Також можливе придбання додаткового апаратного забезпечення (мобільних пристроїв тощо) загальною вартістю 45000 грн.

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

$$К = 10000 + 45000 = 55000 \text{ грн.}$$

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак} \text{ , грн.}$$

де $С_в$ - вартість відновлення й модернізації системи ($С_в$=0);

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ = 0 грн.).

Впровадження технології «Bring Your Own Device» передбачає використання хмарного сховища 20 співробітниками компанії, вартість якого на місяць складає в середньому 560 грн. на користувача. Отже,

$$С_в = 20*560 = 11200 \text{ грн.}$$

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

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Річний фонд амортизаційних відрахувань ($С_а$) визначається прямолінійним методом нарахування амортизації відповідно до строків їх корисного використання.

$$С_а = 45000 / 5 = 9000 \text{ грн.}$$

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

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

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

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 15000 грн. Додаткова заробітна плата – 8% від основної заробітної плати. Отже,

$$С_з = 15000*12 + 15000*12*0,08= 194400 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2016 р. складає 22%.

$$С_{єв} = 181440 *0,22 = 42768 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_p \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,2 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1,2*1920*1,64 = 3778,56 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 2% ($С_{тос}$ = 55000 *0,01=1100 грн).

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

$$С_к = 9000 + 194400 + 42768 + 3778,56 + 1100 = 251046,56 \text{ грн.}$$

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

$$С = 11200 + 251046,56 = 262246,56 \text{ грн.}$$

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 8 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 7000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 9000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 3 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 7 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 800 тис. грн. у рік;

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

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 50.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_{п} + П_{в} + V,$$

де $П_{п}$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

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

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

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

$$П_{П} = \frac{\sum Зс}{F} \cdot t_{п} = \frac{7000 \cdot 7}{176} \cdot 4 = 1113{,}64 \quad \text{грн},$$

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

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

$$П_{в} = П_{ви} + П_{пв} + П_{зч},$$

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

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

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

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

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{7000 \cdot 10}{176} \cdot 8 = 3181{,}81 \text{ грн.}$$

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

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_в = \frac{9000 \cdot 3}{176} \cdot 2 = 306{,}82 \text{ грн.}$$

$$П_в = 3181{,}81 + 306{,}82 + 26000 = 29488{,}63 \text{ грн.}$$

У разі застосування технології «Bring Your Own Device» співробітники мають пристрої, які підходять для виконання робочих завдань, в будь-який час. Якщо такі пристрої ламаються, то співробітник повинен звідкись отримати підтримку. Вартість заміни устаткування або запасних частин може складати біля 26000 грн.

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

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{800000}{2080} \cdot (4 + 2 + 8) = 5769{,}23 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

U = 29488,63 + 1113,64+ 5769,23 = 36371,47 грн.

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_1 \sum_{50} 36371{,}47 = 1818573{,}5 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (25%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

E = 1818573,5*0,25 – 262246,56= 191396,82 грн.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

$$ROSI = \frac{\text{E}}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{191396,82}{55000} = 3,5, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$\text{ROSI} > (\text{N}_{\text{деп}} - \text{N}_{\text{інф}})/100),$$

де $\text{N}_{\text{деп}}$ – річна депозитна ставка, (17 %);

$\text{N}_{\text{інф}}$ – річний рівень інфляції, (9%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$3,5 > (17 - 9)/100 = 3,5 > 0,06.$$

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{3,5} = 0,29 \quad \text{років.}$$

3.4 Висновок

Підвищення рівня захищеності інформаційно-телекомунікаційної системи із технологією «Bring Your Own Device» є економічно доцільним, оскільки коефіцієнт повернення інвестицій ROSI складає 3,5, що перевищує величину річної депозитної ставки з урахуванням інфляції. Термін окупності складає 0,29 років.

Економічний ефект від підвищення інформаційної безпеки шляхом впровадження технології «Bring Your Own Device» складе 191396,82 грн.

ВИСНОВКИ

В Україні поки що більш виражений одиничний інтерес до BYOD. Найбільш розвинені компанії вже розробляють для себе такі рішення. Ймовірно, в перспективі ми побачимо перші прес-релізи на цю тему, тим більше, що опитування, проведені деякими дослідницькими компаніями, вже зараз демонструють досить високий рівень розуміння необхідності впровадження BYOD-рішень з боку вищого керівництва компаній.

В першому розділі дипломної роботи магістра було розглянуто сутність технології BYOD, розглянуто та проаналізовано існуючі методи впровадження BYOD на підприємстві, виділені ті методи які існують на українському ринку, та проведена порівняльна характеристика мобільних операційних систем, що використовуються в Україні.

Оскільки мобільні пристрої найчастіше використовуються за межами захищених офісних мереж, традиційні компоненти безпеки не можуть забезпечити належні контроль і моніторинг комунікацій з мобільних пристроїв. Крім того, залишаються ризики фізичної втрати або крадіжки мобільних пристроїв.

Ефективна стратегія BYOD полягає не тільки в управлінні, відстеженні і знищенні даних на пристроях при необхідності, але і в запобіганні витоків даних з мобільних пристроїв.

В спеціальній частині дипломної роботи магістра було обрано функціональний профіль захищеності ІзОД від НСД, досліджена реалізації послуг сформованого функціонально профілю захищеності обраним існуючим рішенням впровадження BYOD на підприємстві та надані рекомендацій щодо реалізації послуг профілю, вимоги яких не виконуються.

ПЕРЛІК ПОСИЛАНЬ

1 Cisco: полная реализация принципа BYOD повышает производительность и сокращает расходы (Електронний ресурс) / Спосіб доступу: URL: http://www.cisco.com/web/RU/news/txt/2013/05/053013b.html – Заголовок з екрана.

2 BYOD: концепция, технологии и решения (Електронний ресурс) / Спосіб доступу: URL: http://www.skomplekt.com/solution/byod.htm – Заголовок з екрана.

3 Магический квадрант Gartner: «Лаборатория Касперского» вошла в рейтинг мировых производителей MDM-решений (Електронний ресурс) / Спосіб доступу: URL: http://www.kaspersky.ru/news?id=207734023 – Заголовок з екрана.

4 Gartner2014Report: Magic Quadrant for Enterprise Mobility Management Suites (Електронний ресурс) / Спосіб доступу: URL: https://info.mobileiron.com/ gartner-magic-quadrant-2014content.html?utm_mip=headtech-cis – Заголовок з екрана.

5 Управление мобильными устройствами (MDM) (Електронний ресурс) / Спосіб доступу: URL: http://itsave.ru/mobile-device-management/ – Заголовок з екрана.

6 Virtualization as a solution for BYOD Android smartphones (Електронний ресурс) / Спосіб доступу: URL: http://www.techrepublic.com/blog/smartphones /virtualization-as-a-solution-for-byod-android-smartphones/ – Заголовок з екрана.

7 Junos Pulse Mobile Security Suite (Електронний ресурс) / Спосіб доступу: URL: http://www.juniper.net/ru/ru/products-services/security/mobile-security/# features-benefits – Заголовок з екрана.

8 Корпоративная мобильная виртуализация — таблетка от головной боли по имени BYOD (Електронний ресурс) / Спосіб доступу: URL: http://www.computerra.ru/cio/4828– Заголовок з екрана.

9 BYOD: станет ли MDM адекватным ответом? (Електронний ресурс) / Спосіб доступу: URL: http://ko.com.ua/byod_stanet_li_mdm_adekvatnym_otvetom _103762 – Заголовок з екрана.

10 DeviceLock DLP (Електронний ресурс) / Спосіб доступу: URL: http:// http://www.devicelock.com/ru/articles/detail.html?ID=2558 – Заголовок з екрана.

11 Прежде чем разрешать BYOD, оцените риски (Електронний ресурс) / Спосіб доступу: URL: http:// http://www.osp.ru/news/articles/2013/34/13037379/ – Заголовок з екрана.

12 BYOD: новые бизнес-козыри (Електронний ресурс) / Спосіб доступу: URL: http://http://www.pcmag.ru/solutions/detail.php?ID=49221 – Заголовок з екрана.

13 Бен Фрид: «Я не верю в BYOD, когда речь идет о ноутбуках» (Електронний ресурс) / Спосіб доступу: URL: http:// http://ibusiness.ru/articles/28652 – Заголовок з екрана.

14 Bring Your Own Device с точки зрения интересов отечественного бизнеса (Електронний ресурс) / Спосіб доступу: URL: http://www.cisco.com /web/RU/news/releases/txt/2012/112912c.html – Заголовок з екрана.

15 Что такое BYOD и насколько она эффективна в организациях? (Електронний ресурс) / Спосіб доступу: URL: http://ecm-journal.ru/post/Chto-takoe-BYOD-i-naskolko-ona-ehffektivna-v-organizacijakh.aspx – Заголовок з екрана.

16 BYOD - четыре буквы, от которых ИТ-директора бегут в панике (Електронний ресурс) / Спосіб доступу: URL: http://www.osp.ru/cio/2012/ 02/13013084/ – Заголовок з екрана.

17 Глобальное исследование утечек корпоративной информации и конфиденциальных данных, 2011. Аналитический центр InfoWatch – Москва, 2012. – 30 с.

18 Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – НиТ, Санкт–Петербург, 2004. – 384 с.

19 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. – К.: ДСТС31 СБ України, 1999. – 26 с.

20 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99.–К.. ДСТСЗІ СБ України, 1999. – 16 с.

21 Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України (станом на 2 квітня 2012 року) (Електронний ресурс) / Спосіб доступу: URL: http://www.dstszi.gov.ua/dstszi/control/ uk/publish/article;jsessionid=140F77BFF5167554CD3353B12F059064?art_id=78319&cat_id=39181 – Заголовок з екрана.

22 Предотвращение утечек данных (Електронний ресурс) / Спосіб доступу: URL: http://www.sovit.net/articles/technologies/data_loss_prevention/ – Заголовок з екрана.

23 Защита от утечек данных – DLP–решения (Електронний ресурс) / Спосіб доступу: URL: http://www.protectme.ru/infosec/dlp – Заголовок з екрана.

24 Статья DLP – DataLoss / LeakPrevention – Технологии предотвращения утечек конфиденциальной информации – TADVISER (Електронний ресурс) / Спосіб доступу: URL: http://www.tadviser.ru/index.php/Статья:DLP – Заголовок з екрана.

25 Ефременко Наталья. Онтологии в DLP – системах третьего поколения. – Information Security, №4. – 2009.

26 Векторная модель текста (Електронний ресурс) / Спосіб доступу: URL: http://www.neural.ru/dictionary/Векторная модель текста – Заголовок з екрана.

27 Порівняння систем захисту від витоків (DLP) – частина 1, Безпека ПЗ, Security & Hack, статті (Електронний ресурс) / Спосіб доступу: URL:

http://easy–code.com.ua/2011/09/porivnyannya–sistem–zaxistu–vid–vitokiv–dlp–bezpeka–pz–security–hack–statti/ – Заголовок з екрана.

28 Закону України «Про інформацію».

29 Закону України «Про захист персональних даних».

30 ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення».

31 ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт»

32 НД ТЗІ 1.4-001-2000 «Типове положення про службу Захисту інформації в автоматизованій системі».

33 НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»

34 НД ТЗІ 1.1-002-99 «Загальні положення про захист інформації в комп'ютерних системах від несанкціонованого доступу».

35 НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

36 НД ТЗІ 2.5-005-99. «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

37 Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

38 В.Г. Олифер, Н.А. Олифер Компьютерные сети. Принципы, технологии, протоколы – Спб.: Питер, 2001. – 672 с.

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	1 Розділ	15	
6	А4	2 Розділ	37	
7	А4	3 Розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	4	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на дипломну роботу магістра на тему:
Підвищення рівня захищеності інформаційно-телекомунікаційної системи із технологією «Bring Your Own Device»
студента групи 125м-17-1
Чернобривеця Яна Вячеславовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерела та __ додатка.

Актуальність теми полягає в необхідності вдосконалення організації захисту інформації на підприємстві при використанні персональних пристроїв обробки інформації.

Зміст та структура дипломної роботи дозволяють розкрити поставлену тему повністю.

Студент показав добрий рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. У роботі було розглянуто актуальність концепції BYOD, сучасні підходи реалізації технології BYOD на підприємстві, функціональні можливості цих рішень.

Визначено рівень захищеності інформації відповідно функціональному профілю захищеності, який досягаються з використанням MDM-рішень та виявлені нереалізовані послуги. Запропоновано комплексне рішення впровадження BYOD.

Це підтверджує самостійність обробки даних, практичні рекомендації та висновки.

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а його автор Чернобривець Ян Вячеславович заслуговує на оцінку «_____».

Керівник дипломної роботи,
д.ф.-м.н., проф. Т.С. Кагадій

Керівник спец. част.,
ст. викл. кафедри БІТ І.І. Начовний