Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувачка кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

випускної кваліфікаційної роботи
бакалавра
(назва освітнього рівня)

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

спеціальність 125 «Кібербезпека»
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Методи і засоби захисту локальної мережі підприємства за концепцією BYOD»

Виконавець: студент IV курсу, групи КБ-41

_____ **Руслан ЛЕСНЯНСЬКИЙ**
(підпис) (прізвище ім'я)

	Прізвище, ініціали	**Підпис**
Керівник	Яніна ШЕСТАК	

Нормоконтроль	Юрій ЩЕБЛАНІН	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувачка кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 «Кібербезпека»
(код і назва спеціальності)
освітньої програми Кібербезпека
(назва освітньої програми)

студенту **КБ-41** **Леснянському Руслану Романовичу**
(група) (прізвище ім'я по-батькові)
Тема дипломної роботи Методи і засоби захисту локальної мережі підприємства за концепцією BYOD

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Правила використання мобільних пристроїв і сервісів, персональні пристрої, програми автентифікації та авторизації.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися функціональністю MDM-систем та її критеріями вибору, розглянути проблеми впровадження BYOD та етапи впровадження цієї технології, розробити рекомендації впровадження концепції BYOD.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розробка рекомендацій та політики безпеки мережі підприємства за концепцією BYOD.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ Яніна ШЕСТАК
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Руслан ЛЕСНЯНСЬКИЙ
(підпис) (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2022 – 27.01.2022	*виконано*
2	Аналіз літератури	28.01.2021 – 11.02.2022	*виконано*
3	Цілі впровадження концепції BYOD	12.02.2022 - 24.02.2022	*виконано*
4	Функціональність MDM-систем	25.02.2022 - 24.03.2022	*виконано*
5	Критерії вибору мобільної платформи	25.03.2022 – 07.04.2022	*виконано*
6	Впровадження технології BYOD	08.04.2022 – 20.04.2022	*виконано*
7	Кроки на шляху впровадження BYOD	21.04.2022 – 05.05.2022	*виконано*
8	Проблеми впровадження BYOD	06.05.2022 – 20.05.2022	*виконано*
9	Політики впровадження BYOD	21.05.2022 – 01.06.2022	*виконано*
10	Оформлення пояснювальної записки	02.06.2022 – 06.06.2022	*виконано*
11	Підготовка до захисту	07.06.2022 – 13.06.2022	*виконано*

Завдання видав _____ Яніна ШЕСТАК
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Руслан ЛЕСНЯНСЬКИЙ
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Методи і засоби захисту локальної мережі підприємства за концепцією BYOD» складається зі вступу, основної частини, що містить 3 розділи, висновку і списку використаних джерел. Загальний обсяг роботи – 62 сторінки. Пояснювальна записка містить 1 рисунок, 2 таблиці, 23 джрела.

Методи дослідження дипломної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння.

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

Предмет дослідження: методи забезпечення захисту інформації з обмеженим доступом.

Практичне значення роботи полягає у розробці рекомендацій та політики безпеки мережі підприємства за концепцією BYOD.

Результати здійснених у дипломній роботі досліджень можуть бути використані спеціалістами із захисту інформації та при подальшому проведенні науково-дослідницьких робіт.

Ключові слова: концепція BYOD, MDM-рішення, Політика Безпеки, Операційні Системи.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА 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

ВСТУП

Актуальність даної роботи полягає в тому, що у ній розглядається концепція BYOD яка дозволяє використовувати для особистих та робочих цілей єдиний пристрій – свій власний. На сьогоднішній в кожної людини є достатньо потужний смартфон чи планшет який може використовуватись для роботи і це дає змогу не носити із собою два різні смартфони. Також дана робота вміщує рекомендації щодо впровадження концепції BYOD, яка дозволяє розробити політику безпеки що максимально захистить корпоративну мережу.

Термін BYOD означає «bring your own device» або «Принеси свій власний пристрій». Це дає можливість працівникам або студентам носити та використовувати свої пристрої в офіційних установах. Оскільки зараз майже кожен має принаймні один універсальний смартфон чи ноутбук із надійним набором програм і використовує їх протягом дня тому обійти тенденцію BYOD у сучасному світі майже неможливо. Виходячи з цього, багато компаній дозволяють співробітникам працювати будь-яким зручним способом, включаючи персональні мобільні пристрої. Вперше ця практика була використана в IT у 2009 році, коли Intel помітила зростаючу тенденцію співробітників брати з собою на роботу власні ноутбуки, планшети та смартфони, щоб використовувати їх у корпоративній мережі. Замість заборони, керівники підтримали цю практику, і побачили перспективу заощадити гроші та підвищити лояльність співробітників.

Згодом, з масовим поширенням смартфонів і планшетів, практика поступово перемістилася на інші сфери життя, в тому числі і на освіту.

Тому **метою роботи** є розробка рекомендацій щодо впровадження технології «Bring Your Own Device» у локальну мережу підприємства.

Для досягнення поставленої мети необхідно вирішити такі *завдання***:**

- Розглянути функціональність MDM-систем та критерії вибору мобільної платформи;
- Дослідити проблеми впровадження BYOD;

- Розглянути кроки на шляху впровадження BYOD.

Об’єктом дослідження в даній роботі є інформаційно-телекомунікаційні системи ІТ компаній, які використовують технологію «Bring Your Own Device».

Предмет дослідження в даній роботі є методи забезпечення захисту інформації з обмеженим доступом.

Методи дослідження дипломної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння;

РОЗДІЛ 1
ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність проблеми впровадження концепції BYOD

В компаніях працівники все більше використовують мобільні пристрої для роботи, проте, організації, які дозволили співробітникам використовувати мобільні пристрої повинні вміти керувати ними. При використанні мобільного пристрою в мережі компанії працівники можуть навмисно або ненавмисно розкрити конфіденційну інформацію чим зробити сильні фінансові збитки для компанії або ж користувач може неефективного використовувати цей пристрій[1].

Мобільна віртуалізація — це підхід до керування мобільними пристроями, при якому дві віртуальні платформи встановлюються на одному бездротовому пристрої. Платформа - це просто базова комп'ютерна система, на якій можуть працювати прикладні програми.

Мобільна віртуалізація відноситься до поділу мобільного обладнання на різні логічні компоненти та пристрої. Взагалі віртуалізація передбачає поділ апаратних машин на логічні частини для розподілу потужності обробки, пам’яті тощо.

Перший тип мобільної віртуалізації який впроваджується за участю виробника має вищий рівень безпеки. Він може отримати доступ до bluetooth та інших мережевих підключень, адаптується до нового програмного забезпечення і з точки зору інтеграції більш сумісний із пристроями. Цей метод передбачає співпрацю з виробниками обладнання і це в свою чергу збільшує цикл розробки - за рахунок великого обсягу дозволів. Другий тип віртуалізації дозволяє розгортання на багатьох платформах без схвалення виробника обладнання або оператора. Цей метод поступається першому за наступними ознаками: нижчий рівень безпеки та робота пристрою повільніша це вимагає більш потужного обладнання.

Спільна риса цих двох типів віртуалізації полягає в тому, щоб створити розподіл між корпоративними та споживчими програмами та даними тобто поділити на пристрій на приватну і корпоративну частини.

Корпоративна частина шифрується, щоб зовнішні додатки та служби не могли взаємодіяти з конфіденційними даними та корпоративним ПЗ. Приватна частина відокремлена від корпоративної, і не заважає користувачу повноцінно використовувати пристрій як зазвичай: переглядати новини, сидіти в соціальних мережах, спілкуватись, фотографувати, завантажувати програми, користуватися особистими електронними листами - без введення додаткових паролів. IT-департамент має можливість видалити корпоративні дані з пристрою, якщо його вкрадено, втрачено або пароль для захищеної частини введено неправильно певну кількість разів.

Найпоширеніший спосіб реалізації технології: за допомогою Virtual Private Network (VPN), рекомендовано розробниками засобів керування мобільними пристроями рішення класу Mobile Device Management (MDM) для безпечної роботи з ними.

Під час використання мобільного пристрою найпростішим способом захистити дані компанії є системи захищеного віддаленого підключення через приватну віртуальну мережу (VPN), це дозволяє відмовитися від зберігання корпоративних даних на пристроях співробітників і підтримувати доступ до ресурсів компанії через захищене з'єднання і термінальну сесію. Багато компаній мають встановлені шлюзи доступу до корпоративної мережі тому таке рішення буде вигідне. Через такі шлюзи можна обробляти інформацію з мобільних пристроїв чи комп'ютерів на платформах традиційних операційних систем. Щоб підключитись і отримати доступ до ресурсів компанії через свій пристрій потрібно лише інсталювати відповідну клієнтську частину для своєї ОС (iOS, Android, Windows Phone тощо), включити VPN та пройти авторизацію[2].

Інше питання — законність встановлення VPN-клієнта на ОС iOS. У деяких випадках доводиться обходити захист операційної системи. Користувач не має можливість отримати повний контроль над цією операційною системою і може встановлювали лише програмне забезпечення що доступне в Apple Store. У той же час далеко не всі компанії можуть пройти процес включення їх клієнта до репозиторію програм Apple, тому для встановлення проксі-сервера на iOS потрібно

обійти захист смартфону що в свою чергу позбавляє власника гарантії яку надає виробник. Міжнародні розробники інструментів безпеки на основі VPN, такі як Check Point або Stonesoft, заключили договір з Apple що дозволяє встановлювати їхнє ПЗ стандартними методами, але такі рішення не мають сертифікатів і не реалізують необхідні деяким користувачам алгоритми шифрування. Тому на сьогоднішній день на ринку немає клієнта VPN який зміг би задовольнити потреби абсолютно всіх користувачів.

Можливим рішенням цієї проблеми є використання технологія SSL-VPN, яка дозволяє шифрувати дані за допомогою протоколу HTTPS водночас не встановлюючи жодних спеціальний клієнтів. В такому разі необхідні перевірки виконується спеціальним сценарієм JavaScript, він може просканувати пристрій на наявність шкідливих ПЗ і видалити конфіденційну інформацію в кінці сеансу з його пам’яті. Клієнти цих виробників в теорії мають працювати на мобільних пристроях але ефективність їх впровадження не перевірена.

Розробники платформ управління IT запропонували окремий клас програмних продуктів – системи Mobile Device Management, (MDM) які централізовано керують корпоративними пристроями. Ці продукти дозволяють IT-департаменту автоматизувати, контролювати та захищати адміністративні політики на ноутбуках, смартфонах, планшетах чи будь-якому іншому пристрої, підключеному до мережі організації. Зараз на ринку приблизно 60 компаній постачальників рішень MDM з яких лише 20 мають рішення яке найбільш повно реалізує функціонал управління життєвим циклом мобільного пристрою.

Три групи на які можна розподілити постачальників рішень MDM систем (табл. 1.1):

-розробники засобів захисту (Symantec, McAfee, Sophos, Trend Micro);

-розробники засобів які управляють IT-системами (LANDesk, SAP, IBM, Amtel, Good Technology);

-компанії які продають рішення MDM (MobileIron, AirWatch, Fiberlink і Zenprise).

Таблиця 1.1

Постачальники 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

На сьогоднішній день є два типи продуктів MDM. Перший тип це «не повномасштабна реалізація», такий тип передбачає встановлення додатку на пристрій щоб підключитись до системи MDM та підтримку зв’язку з корпоративним сервером управління і контролю користуванням. Користувач використовує потрібний йому функціонал, а програма виконує тільки частину функцій MDM, які пов'язані з дотриманням політики безпеки. Такі додатки не

виконують управління життєвим циклом інших додатків і даних. До цього варіанту відносяться продукти компаній AirWatch, BoxTone Fiberlink, MobileIron і Zenprise.

Другий тип це «повномасштабна реалізація» який передбачає встановлення спеціального ПЗ який надає підключення до корпоративних ресурсів[3].

1.2 Аналіз технології BYOD

Принцип BYOD (Bring Your Own Device), який передбачає використання персональних мобільних пристроях, щоб дати співробітникам можливість використовувати будь-яку програму на своєму пристрої та хмарний сервіс. BYOD пропонує найкраще співвідношення роботи та особистого життя, поширення інновацій та зростання продуктивності праці. Але багато експертів стурбовані щодо BYOD так як такий підхід створює нові проблеми в інформаційній безпеці і при відсутності належної політики, яка регулює використання принесених мобільних телефонів чи інших пристроїв на робочому місці наслідки використання BYOD є серйозними, оскільки це ставить користувачів і компанію під загрозу порушення цілісності даних та кібератак. Тому є думки що негативні фактори переважають позитивні.

Щоб перевірити обґрунтованість цих побоювань звернем увагу на дослідження, проведене Cisco IBSG Consulting, воно показало, що впровадження BYOD вже принесло компаніям величезні переваги, і в майбутньому їх буде ще більше. Багато що залежить від практичного втілення принципів BYOD. Сьогодні переважна більшість (89%) організацій дозволяють співробітникам приносити на роботу персональні пристрої. В результаті організації починають усвідомлювати, що успішне впровадження BYOD вимагає безпечного доступу, простих методів аутентифікації та чітких правил використання мобільних пристроїв і сервісів але це лише початок. Більш широкий стратегічний підхід до BYOD принесе більше переваг компаніям за рахунок зниження операційних витрат, підвищення продуктивності та економії критичного ресурсного - часу.

Детальний аналіз фінансових аспектів впровадження BYOD у Бразилії, Китаї, Німеччини, Індії, Великобританії та США показує, що в усіх цих країнах компанії вже отримують значні переваги від BYOD. Дослідники не тільки оцінили ефективність та зрілість існуючих підходів до впровадження BYOD, але й намагалися визначити корисність повного використання переваг цього принципу. Виявляється зараз досить мало компаній наблизилися до повної реалізації концепції. На сьогоднішній день організації використовують лише одну п’яту (21%) усіх можливостей BYOD[4].

1.3 Цілі впровадження концепції BYOD

Майже для кожної галузі використання мобільного пристрою під час роботи є звичним явищем. Адже, не використовувати пристрій для роботи здавалося б майже дивним. Проте для багатьох організацій мобільні пристрої на робочому місці ставлять складне питання: хто надає пристрій? Відповідь проста — BYOD

Тенденція BYOD полягає в тому, що компанії дозволяють співробітникам брати з собою на роботу свої власні пристрої, щоб використовувати їх у робочих цілях. BYOD протилежна тенденції «Here’s Your Own Device» (HYOD), яка історично була більш поширеною в компаніях – програма, де компанія надає співробітникам мобільні пристрої. Arlington Heavy Hauling вирішила дати своїм водіям планшети, щоб вони могли заповнювати документи в дорозі, що дозволило швидко та легко надсилати дані назад до офісу.

Технологія BYOD дозволяє зробити процес праці більш продуктивними, дозволяючи співробітникам власні пристрої які вони собі вибирають. Деякі можуть віддати перевагу пристрої з операційною системою Android. Інші можуть віддати перевагу пристрої, що працює на платформі iOS (Apple). І навіть можливо, що деякі віддають перевагу ОС Windows Mobile (хоча таких мало). Незалежно від того, чому вони віддають перевагу, можна впевнено сказати, що їм буде зручніше користуватися власним пристроєм, ніж той, який їм дасть компанія.

За допомогою власних пристроїв працівники зазвичай можуть виконувати роботу більш високої якості з більшою швидкістю, що підвищує продуктивність в цілому. Але чому це так? Одна з причин полягає в тому, що перехід між операційними системами або навіть інтерфейсами пристроїв може бути незручною зміною, і користувачам часто потрібно багато часу, щоб повністю налаштуватися. Інша причина полягає в тому, що співробітники просто краще знайомі з опціями і функціями власного пристрою. Також BYOD може допомогти зменшити фінансові витрати на закупку різних пристроїв та вирішить питання їх знеціненння. Давайте подивимося правді в очі – навіть якщо ви придбали найновішу модель пристрою цього року, новіші з'являться протягом кількох місяців. У реальному світі ваша компанія буде постійно намагатися отримати новітні пристрої з найновішими та найкращими функціями. Залишивши пристрої на розсуд співробітників, ваша компанія може заощадити значну суму грошей. Завдяки заохоченням постачальників, які зазвичай пропонують споживачам мобільних пристроїв новинки, більшість людей можуть користуватись найновішими пристроями. Компаніям же догнати таку тенденцію буде важче. Ці нові пристрої будуть мати нові функції та кращі операційні системи, що означає більшу продуктивність і кращі вбудовані протоколи безпеки. Звичайно, організації також прагнуть забезпечити достатню безпеку в своїх мережах, тоді як окремі особи хочуть забезпечити їхню особисту конфіденційність. Люди носять із собою свої пристрої в будь-який час доби, де б вони не були. Для вас це означає, що у вас є співробітник, який завжди підключений до роботи, якщо виникне така потреба. Це не означає, що вони працюватимуть весь час, але це означає, що вони матимуть підвищену швидкість реагування, якщо черговий дзвонить у неробочий час.

У сучасному бізнес-ландшафті хмарні програми стають синонімом успіху. Близько 90% організацій використовують хмару, а 50% використовують хмарні сервіси як найкраще рішення. Політика BYOD йде рука об руку з цими хмарними сервісами. Більшість передових програм підтримують мобільні пристрої, а це означає, що ваші співробітники матимуть доступ до своїх передових робочих інструментів у будь-який момент. Використовуючи BYOD, ви полегшуєте перехід

до рішень майбутнього. Іншою важливою ціллю BYOD є гнучкість для всіх. Деякі компанії не враховують, що навіть із обладнанням компанії у співробітників все одно будуть власні пристрої. По суті, ви просто подвоюєте кількість пристроїв, які вони повинні носити з собою в будь-який момент часу. Але з BYOD компанії не доведеться турбуватися про це. Будь-яку необхідну роботу можна виконати з будь-якого місця та на одному пристрої, безпечно та зручно. Співробітникам не доведеться турбуватися про суворі правила поводження з майном компанії. BYOD надає співробітникам і компанії більшу гнучкість для роботи будь-яким найбільш ефективним способом[5].

Висновки за розділом 1

Майже для кожної галузі використання мобільного пристрою під час роботи є звичним явищем. Не використовувати його для роботи здавалося б майже дивним. Поки в Україні інтерес до концепції BYOD одиночний і лише передові компанії розробляють такі рішення для себе. Можливо в майбутньому темпи популярності цієї концепції виростуть так як проведені опитування продемонстрували розуміння необхідності і високий рівень бажання впровадження BYOD-рішень з боку керівництва компаній.

Так як на сьогодні більшість додатків є не українською мовою тому ми не бачимо стрімкого зростання популярності концепції BYOD в нашому регіоні. Звичайно з часом це виправиться і ситуація неминуче буде мінятись в кращу сторону, потреби в рішеннях-BYOD зростуть. Як тільки компанії стануть активно впроваджувати концепцію BYOD, вони почнуть їх пропонувати бізнесу і ринок стрімко почне розвиватись.

В першому розділі дипломної роботи було розглянуто актуальність проблеми захисту локальної мережі підприємства за концепцією BYOD, розглянули проблеми VPN мереж для ОС IOS, розглянули постачальників рішень MDM і її мінімальний набір функцій, була проаналізована сама технологія BYOD та визначено цілі впровадження цієї технології.

РОЗДІЛ 2
ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ BYOD ЗА ДОПОМОГОЮ MDM-СИСТЕМ

2.1 Функціональність MDM-систем

Mobile Device Management — це будь-яке програмне забезпечення, яке дозволяє IT-департаментам автоматизувати, контролювати та захищати адміністративні політики на ноутбуках, смартфонах, планшетах чи будь-якому іншому пристрої, підключеному до мережі організації. Співробітники все більше звикають використовувати пристрій, операційну систему та програму на свій вибір. Через різноманітність мобільних пристроїв IT-відділи стикаються з унікальним набором проблем під час розгортання та підключення внутрішнього вмісту та ресурсів. Як правило, MDM розгортає сукупність корпоративних рекомендацій і сертифікатів, конфігурацій на пристрої, додатків, серверного програмного забезпечення та обладнання для керування пристроями кінцевих користувачів.

Мета MDM — максимізувати підтримку пристроїв, організаційну функціональність та безпеку, забезпечуючи певну гнучкість користувача, наприклад для використання технології BYOD.

Сегментація дозволяє IT-відділам безперешкодно встановлювати параметри безпеки та відповідність вимогам для певних користувачів, груп або географічних місць в організації. Щоб зменшити витрати, підвищити ефективність роботи та пом’якшити ризики, включаючи порушення даних та безпеки, організації повинні впровадити надійну систему MDM. Увага до MDM посилилася, оскільки використання мобільних пристроїв значно збільшилась.

Багато факторів підвищили важливість керування мобільними пристроями для C-suite. До них належать:

- масове розгортання мобільних додатків вимагає інструментів для захисту активів і керування ними;

- зростаюче занепокоєння через порушення безпеки, пов’язані з використанням мобільних пристроїв співробітниками;

- стандартизація практик і процесів керування мобільними пристроями.

Оскільки тепер співробітники виконують багато, якщо не більшість своїх обов’язків на портативних пристроях, організаціям потрібна корпоративна мобільність. MDM полегшує можливості віддаленої роботи, використовуючи хмару для роботи з даними. Тому мобільні пристрої співробітників стали об’єктами зловмисного програмного забезпечення, хакерів через велику кількість даних, які зберігаються та передаються на кожному пристрої. Організації визнають свою відповідальність за безпеку та захист цих даних від втрати, надаючи своїм співробітникам доступ до основних ресурсів. У рамках цієї відповідальності MDM забезпечує критичні оновлення та виправлення необхідних програм і мікропрограми не лише для функціональності, але й для безпеки. MDM підтримує роботу та продуктивність співробітників за допомогою резервного копіювання даних у режимі реального часу.

Пристроями керують у відповідності з цими функціями адміністратори, які працюють на серверній платформі MDM, що дозволяє віддалено керувати функціями пристрою. Додаток або програмне забезпечення встановлені на пристрої щоб ввести у функціональність MDM та інтегруватись із серверними службами корпоративної мережі, такими як:

- доступ до інформації;

- передача даних;

- спільний доступ до журналу пристрою;

- інші можливості за потреби.

Розповсюдження власних смартфонів і зростаюча тенденція BYOD, що підживлюються триваючою пандемією, роблять надзвичайно важливою стратегію MDM. Перегляньте деякі з останніх статистичних даних BYOD та корпоративної мобільності згідно з нещодавнім дослідницьким звітом:

- 67% усіх співробітників використовують пристрої BYOD в офісі;

- BYOD дозволяє користувачам витрачати еквівалентно дві додаткові години щодня на виконання службових обов’язків;

- 87% роботодавців дуже залежать від того, що працівники мають віддалений доступ до бізнес-інформації та програм на їхніх пристроях;

- 69% тих, хто приймає рішення, підтримують тенденції BYOD;

- 59% компаній вже прийняли стратегії BYOD;

- очікується, що індустрія BYOD досягне близько 367 мільярдів доларів до 2022 року.

MDM часто є компонентом рішень з керування корпоративною мобільністю (EMM), що включає сукупний набір інструментів для захисту мобільних додатків, пристроїв, наданих компанією та BYOD, вмісту, даних і доступу та керування ними. Компоненти в рамках рішення EMM можуть мати функції, що перекриваються (Рисунок 1.1). Наприклад, рішення MDM може також пропонувати функції для керування додатками та даними, щоб доповнити те, що може широко пропонуватися лише рішеннями для керування мобільними додатками.

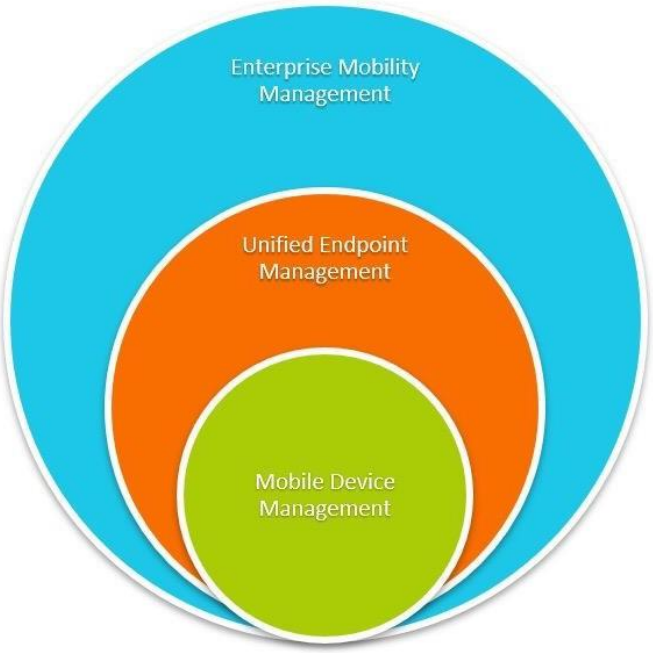

Рисунок 2.1 – Компоненти в рамках рішення EMM

MDM приділено багато уваги в останні роки, оскільки корпоративні IT-постачальники виходять на ринок зі своїми власними рішеннями для керування пристроями. Такі фрази, як керування мобільними пристроями, керування мобільністю підприємства та уніфіковане керування кінцевими точками (UEM), зазвичай використовуються для продажу загальних функцій, що перекриваються. Отже, перш ніж ми розглянемо ключові можливості рішення MDM, давайте розмежуємо терміни MDM від EMM та UEM:

Mobile device management (MDM) зосереджено на управлінні смартфонами та мобільними пристроями, які підключаються до корпоративної мережі.

Enterprise mobility management (EMM) є надкомплектом MDM і включає багато компонентів, таких як керування додатками, керування мобільним вмістом, керування безпекою мобільних пристроїв, керування витратами на мобільних пристроях, а також керування ідентифікацією та доступом тощо.

Unified endpoint management (UEM) об’єднує керування всіма кінцевими пристроями, включаючи смартфони, пристрої Інтернету речей, датчики, носії та інші кінцеві точки. Єдина централізована платформа об'єднує управління всіма пристроями, що підключаються до мережі.

Зазвичай MDM-рішення складається з двох частин: контрольного центру та клієнтського програмного забезпечення. Клієнтське програмне забезпечення може включати засоби шифрування, які дають змогу забезпечити конфіденційність робочих даних незалежно від особистої інформації користувача, а також ряд інструментів, призначених для віддаленого моніторингу та управління пристроєм[6].

MDM-системи можуть володіти вбудованим антивірусним рішенням, також можуть бути частиною мультиплатформної системи інформаційної безпеки. Рішення щодо управління мобільними пристроями існують для більшості популярних мобільних платформ (Android, iOS, Windows Phone, Blackberry, Symbian). Однак набір доступних функцій може відрізнятися залежно від операційної системи. Це зумовлено відмінностями в ідеології платформ і, як наслідок, у різному рівні доступу до даних для розробників MDM-рішень.

Ключові елементи MDM рішень:

- керування активами, яке включає підтримку кількох платформ для компаній, щоб застосовувати спеціальні організаційні політики до корпоративної мобільності та використання BYOD в корпоративній мережі. Управління активами може відстежувати та контролювати використання пристроїв, а також застосовувати політику компанії на всіх зареєстрованих пристроях, кількох платформах та версіях операційної системи;

- керування конфігураціями, яке може ідентифікувати, контролювати та керувати параметрами апаратного та програмного забезпечення на основі географічних регіонів, профілів користувачів та ідентифікаційних даних;

- керування ризиками, аудит і звітність, які відстежують активність пристрою та повідомляють про аномальну поведінку, щоб обмежити такі проблеми, як несанкціонований доступ до корпоративних мереж або передача даних;

- оновлення та розповсюдження програмного забезпечення, що дозволяє віддалено керувати програмами, оновленнями програмного забезпечення та ОС, а також ліцензіями на кількох пристроях;

- керування профілями, що дозволяє керувати політиками та налаштуваннями для певних груп кінцевих користувачів на основі конкретних профілів;

- керування ідентифікацією та доступом, яке гарантує, що пристрій, дані, мережеве з’єднання та послуги надаються відповідним авторизованим користувачам;

- керування додатками, які мають доступ до налаштувань. А також блокування або дозвіл різних додатків та функцій ПЗ;

- корпоративні магазини додатків, які підтримують бібліотеку програм і служб, призначених для корпоративного використання, які доступні авторизованим кінцевим користувачам;

- оптимізація пропускної здатності, яка керує використанням пропускної здатності на рівні пристрою та програми;

- безпека даних, яка забезпечує доступ до даних, їх передачу та використання відповідно до організаційної політики. Наприклад, у разі викрадення або втрати пристрою дані, збережені на пристрої, можуть бути видалені;

- керування вмістом, яке синхронізує та захищає бізнес-інформацію на кількох пристроях;

- технічна підтримка, яка включає виділену віддалену технологічну підтримку, може надаватися віддалено.

На додаток до впровадження рішень безпеки MDM, організації можуть покращити безпеку своїх мобільних пристроїв, дотримуючись цих найкращих практик:

- створити спеціальний магазин додатків. Коли співробітники завантажують програми з загальнодоступних сайтів, вони можуть отримати зловмисне програмне забезпечення на додаток до програми. Роботодавці можуть усунути цю загрозу, створивши спеціальний магазин додатків із лише «чистими» додатками, які перевіряє ІТ-відділ, запобігаючи завантаженню з інших сайтів;

- розробити політику безпеки для пристроїв. Варто розробити політику для пристроїв, що належать співробітникам, що включає вимоги до надійних паролів і шифрування;

- надавати ПЗ для віртуальної приватної мережі (VPN) на пристрої, яким потрібен доступ до конфіденційних даних;

- обмежити доступ до загальнодоступних мереж Wi-Fi;

- підвищити обізнаність співробітників. Неуважність співробітників часто є причиною злому даних, тому освіта співробітників є важливою для підвищення безпеки.

Хоча мобільні пристрої й надалі залишатимуться об’єктом кібератак, ІТ-організації можуть значно знизити свій ризик, впроваджуючи захист мобільних пристроїв за допомогою передових методів безпеки та сучасного програмного забезпечення безпеки. Поєднання виявлення мобільних загроз і керування мобільними пристроями забезпечує максимальний захист даних і програм, надаючи співробітникам переваги мобільних пристроїв.

Переваги використання MDM величезні. Найбільшою перевагою є економія часу за рахунок автоматизації повторюваних завдань. Наприклад, вручну налаштувати параметри Wi-Fi на 100 пристроях і попросити співробітників встановити певні програми є громіздкими завданнями. Ці завдання можна повністю автоматизувати за допомогою MDM.

Також іншими перевагами є:

- підвищена продуктивність і ефективність, навіть на персональних пристроях. Коли персональний мобільний пристрій керується сервером MDM, можна запобігти використанню неважливих програм у робочий час. Це не дозволить співробітникам отримати доступ до соціальних мереж та інших програм, поки вони працюють. Коли співробітники не відволікаються на сповіщення соціальних мереж та інші сповіщення в додатку, вони приділять роботу повну увагу і будуть більш продуктивними;

- дотримання правил відповідності. Деякі норми (наприклад, HIPAA, PCI-DSS і GDPR) вимагають суворих заходів захисту даних. Рішення MDM можуть автоматизувати цей захист на всіх пристроях, підключених до сервера MDM;

- дистанційне управління. Пристрої, підключені до сервера MDM, можна оновлювати, виправляти й керувати ними віддалено, не перериваючи роботу користувача.

2.2 Критерії вибору мобільної платформи

При виборі мобільної платформи за допомогою якої співробітники будуть взаємодіяти із ресурсами компанії спершу потрібно виділити основні вимоги і функції які має мати платформа:

- безпека інформації що зберігається на пристроях. Дані на пристроях які знаходяться за межами офісу повинні бути в зашифрованому вигляді і передаватись по захищеним протоколу. Так як з великим ростом кількості смартфонів зростає кількість шкідливого ПЗ яке може порушити цілісність інформації. Тому ІТ-

департаменту повинна бути доступні дані щодо конфіденційної інформації яка знаходиться на пристрої співробітника і можливість нею керувати;

- безпечний обмін даними. Працівники повинні мати можливість безпечної комунікації із партнерами чи клієнтами;

- безпечне середовище для додатків. Інколи коли співробітник не має доступу до інтернету але йому потрібно використовувати певну інформацію її потрібно зберегти на власному пристрої для цього потрібне спеціальне захищене середовище яке відповідає вимогам безпеки. Також це середовище повинно керуватися адміністратором підприємства який може перевести дані в режим «тільки для читання» або повністю видалити з пристрою;

- робота з великими файлами. Так як сьогодні часто передають відео великих розмірів або високої якості мобільні платформи повинні відповідати цій вимозі;

- прозорість управління. Для різних відділів і робочих груп адміністратору який керує мобільною платформою потрібно запроваджувати різні ПБ і призначати різні права доступу. Контролюючи роботу мобільних співробітників, можна відстежувати зміни вмісту файлів, публікацій та інших факторів;

- відповідність рівня безпеки світовим стандартам.

Якщо вибирати мобільну платформу для конкретного підприємства то слід врахувати наступні питання:

- визначити цілі впровадження і основні вимоги які повинна мати система;

- визначити ОС які буде підтримувати система;

- перевірка готовності співробітників до використання мобільної платформи.

У сучасному світі існує величезна різноманітність мобільних пристроїв. Мобільна операційна система — це операційна система для мобільних телефонів, планшетів, розумних годинників чи інших мобільних пристроїв, вона поєднює в собі функції операційної системи персонального комп'ютера з функціями, корисними для мобільного використання. Мобільна ОС посідає чудове місце в належному функціонуванні будь-якого мобільного пристрою. Подібно до ПК, які мають безліч різних типів операційних систем, смартфони можуть працювати з різними операційними системами або різними версіями.

Розробники операційних систем мобільних пристроїв наближають їх можливості і функції до таких же якими володіють ПК. Проте ОС для мобільних пристроїв мають свої переваги та недоліки. Їхні основні особливості наступні (табл. 1.2).

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

Нижче описано три популярні рішення для керування мобільними пристроями (MDM) кожне з яких має свої особливості і організацію технології. Вибір платформи буде залежати від розмірів підприємства і цілей які потрібно виконати.

Cisco Meraki охоплює управління ноутбуками та настільними комп'ютерами, а також смартфонами та планшетами. Ця консоль керування цією системою дуже приваблива і містить карту, що показує розташування всіх керованих пристроїв вашої компанії. Однак він не може керувати офісним обладнанням з підтримкою Інтернету речей або Wi-Fi, наприклад принтерами. Він буде взаємодіяти з пристроями під керуванням Windows, Mac OS, Windows Phone, iOS, Android, Chrome OS і Samsung Knox .

В основі MDM лежить безпечний канал зв'язку, який шифрується AES за допомогою 256-бітового ключа. Зв'язок додатка захищений VPN, який застосовується для кожної програми.

Конфігурацію можна змінювати залежно від типу пристрою, профілю користувача або моделі власності. Ці групи пристроїв можна налаштувати масово, але завжди є можливість індивідуальної конфігурації. Користувачі зі своїми власними пристроями можуть зареєструватися для включення в мережу . Метод доставки програм і файлів даних називається Backpack. Центральний адміністратор створює пакет файлів, а потім надсилає дозволи доступу групам, окремим особам або всій мережі. Ці пакети будуть доступні на пристроях, які належать користувачам, після того, як вони будуть зареєстровані та включені в групу користувачів.

Усі права на втрачені або вкрадені мобільні телефони можуть бути анульовані, а також їх можна заблокувати або стерти віддалено. Meraki автоматично відстежує використання мобільного тарифного плану , тому надмірну активність можна визначити за реальними звітами, а вкрадені пристрої можуть бути негайно відключені від телефонів і служб передачі даних.

BlackBerry Unified Endpoint Management — це рішення для керування кінцевими точками, розроблене для моніторингу пристроїв Інтернету речей (IoT). За допомогою одного централізованого інтерфейсу користувача ви можете

переглядати огляд пристроїв, користувачів і програм , які використовуються у вашій мережі. Інструмент підтримує операційні системи, включаючи Windows 10, Mac OS, iOS, Android і Chrome OS .

Ключові риси:

- керує політикою пристрою;
- підтримує iOS, Android, Chrome OS, Windows і Mac OS;
- активувати використання за допомогою QR-коду (лише для iOS і Android);
- доступно локально та в хмарі;

Керувати політиками за допомогою BlackBerry Unified Endpoint Management дуже легко. Ви можете керувати політиками, користувачами, групами та програмами з консолі. Завдання, які ви можете виконувати, включаючи призначення програм обліковим записам користувачів, розповсюдження програм у контейнери та налаштування рідних програм.

Підключення нових користувачів також неймовірно ефективне, з можливістю активації нових пристроїв за допомогою QR-коду для користувачів iOS та Android . Групи також можуть бути пов’язані з AD для автоматичного залучення нових користувачів . Існує також можливість відокремити робочі дії від особистих із кількома типами активації, наприклад «Робота та особисті пристрої» та «Лише робота».

SimplySecure — це хмарний MDM, який може працювати з мобільними пристроями iOS та Android і портативними сховищами. Загальна послуга називається SimplySecure Management System і може охоплювати настільні комп’ютери, ноутбуки, мобільні пристрої та USB-накопичувачі в цих різних цінових категоріях. Просто сплачуйте за кожен пристрій, яким ви хочете керувати. Проте оплата послуги здійснюється щорічно, а не за місяць. Якщо вам потрібна щомісячна ціна, вам потрібно знайти торговельного посередника Simply Secure і купити послугу там.

Доступ до інформаційної панелі послуги здійснюється через веб-браузер. Налаштуйте свої мобільні пристрої віддалено та масово, застосовуючи різні

політики до груп пристроїв. Загублені пристрої можна стерти віддалено, а пристрої, які демонструють підозрілу активність, можна помістити на карантин .

Служба включає відстеження розташування пристрою, і ви можете застосувати захист паролем, щоб додати додатковий рівень безпеки на випадок, якщо вони будуть втрачені. Ви можете змінити ці паролі віддалено, щоб створити миттєвий замок у разі несправності.

Усі комунікації в мережі вашої компанії захищені шифруванням. Хоча цей захист не поширюється на прямий доступ до програм через хмару, ви можете маршрутизувати доступ через сервер компанії, щоб застосувати рівень безпеки до програм і доступу до даних. Шифрування також можна застосувати до даних, що зберігаються на пристрої.

Це легкий варіант для малого бізнесу, а доставка через хмару означає , що вам не потрібно запускати велику мережу або наймати системного адміністратора, щоб скористатися цією послугою . Можливість включати пам’ять USB до покриття є унікальною та застосовує шифрування, яке можете розшифрувати лише ви та ваші співробітники. Це чудове рішення проблеми втрати конфіденційних даних разом із втраченим пристроєм пам’яті USB.

Переваги впровадження BYOD для бізнесу:

- підвищує продуктивність співробітників;
- зменшує операційні витрати;
- доступ до нових пристроїв і технологій;
- підвищує довіру між роботодавцем і працівником;
- зменшує тиск на команди підтримки;
- допомагає залучити найкращі таланти, спрощуючи віддалену роботу[7].

MDM системи допомагають слідкувати за статусом безпеки сматфону. Коли пристрій підключиться до Wi–Fi мережі, система може перевірити, чи встановлений на пристрої спеціальний агент, який передає інформацію про ОС яка стоїть на пристрої, наявність антивірусу, оновлення його баз сигнатур і т.д. Якщо такого агента не знайдено, його можна запропонувати скачати. Після інсталяції система знову визначає статус безпеки, і вирішує чи авторизувати користувача в мережі чи

перевести пристрій в карантин в разі коли рівень безпеки недостатній. У карантині можна спробувати оновити ПЗ або скачати антивірус з мережі Інтернет і знову спробувати увійти в корпоративну мережу.

Існують MDM системи, за допомогою яких можна убезпечити мережу додатково ввівши ПЗ. Наприклад щоб встановити обов'язковий PIN-код або шифрувати дані на пристрої.

Також існують компоненти які можна інтегрувати в рішення які дозволяють контролювати активність співробітника в мережі інтернет. Це дає змогу наприклад обмежити доступ до ігрових ресурсів з корпоративної мережі співробітникам але дозволити доступ гостям або ж заборонити відвідувати сайти які заражені шкідливим ПО або поширюють його.

Враховуючи багато факторів, які впливають на безпеку компанії, ретельне проектування усіх цих функцій у рішенні дає можливість сформувати потужну ієрархію політик для індивідуального доступу до ресурсів компанії та контролю обміну трафіком із зовнішнім світом. У той же час багато з цих можливостей безпосередньо знижують рівень проблем, які повинні вирішувати IT-служби, значно знижуючи витрати на придбання та підтримку схожого гнучкого інформаційного середовища[8].

Такі рішення впроваджуються компаніями, зацікавленими в перевагах широкого використання персональних мобільних пристроїв і спеціалізованих додатків, і є логічним і превентивним підходом до управління та безпеки в таких середовищах. Зазвичай це навіть не IT-компанії. У Сполучених Штатах, наприклад, BYOD використовується в багатьох вертикалях, включаючи освіту, охорону здоров'я та державний сектор.

2.3 Впровадження технології BYOD

Bring Your Own Device, більш відомий як BYOD, — це підхід до обчислень кінцевих користувачів, який передбачає підтримку і заохочення кінцевих

користувачів організації, які отримують доступ до ключових керованих IT-ресурсів на своїх особистих пристроях.

Концепція BYOD була вперше представлена в 2009 році, але вона не стала популярною до 2010 року. Кількість персональних пристроїв почала стрімко зростати тоді на робочому місці та в IT-відділі стало використовуватись все більше смартфонів і планшетів, які використовують співробітники без надання великої підтримки[9].

У відповідь деякі компанії почали блокувати персональні пристрої на своїх мережевих і поштових серверах. Коли iOS 4 вийшов у 2010 році, були випущені перші API для роботи з мобільними пристроями. Тоді компанії почали розуміти, що не можуть ігнорувати BYOD.

Таким чином, перші програми BYOD були розроблені в 2011 році з офіційною підтримкою, запровадженою на робочому місці. Керівники компаній стали відчувати себе комфортніше, вводячи текст на сенсорних клавіатурах, і ринок корпоративної мобільності також почав швидко змінюватися.

Незважаючи на те, що концепція BYOD повинна була зосередитися на безпеці пристроїв, перші реальні занепокоєння щодо витоку даних і безпеки не виникли до 2012 року. Люди почали проявляти підвищену стурбованість про свою конфіденційність. Компанії почали зосереджуватися на чіткому донесенні політики BYOD до зацікавлених користувачів, одночасно працюючи над розумінням наслідків безпеки та конфіденційності. Це викликало збільшення попиту на рішення з керування мобільними пристроями (MDM).

BYOD змінив спосіб надання компаніям доступу до комп’ютерних мереж. Традиційно IT-відділ будував закриті мережі, доступ до яких можуть мати лише комп’ютери, якими володіє компанія. Проте, за допомогою BYOD співробітники змогли підключити власні смартфони, планшети та комп’ютери до більш відкритих мереж.

Для руху BYOD є плюсом шалена популярність смартфонів і планшетів разом з нижчою вартістю портативних комп’ютерів. Люди, які раніше залежали від

організацій, які видають їм обладнання для роботи, тепер можуть легко володіти особистими пристроями, які можуть виконувати ту саму роботу.

Простіше кажучи, BYOD – це спосіб для IT-відділу організації надати кінцевим користувачам доступ до ключових ресурсів. Це може включати IT-послуги, такі як:

- ліцензійні програмні додатки;
- хмарні платформи даних/сховищ;
- підключення до мережі;
- корпоративні комунікаційні системи;
- додатки, розроблені власними силами;
- послуги ідентифікації та SSO.

BYOD є основною темою в обчислювальних системах для кінцевих користувачів та IT вже близько десяти років, після популярності та постійно знижуваної вартості персональних пристроїв, а також зростання вимог до мобільності споживачів; спочатку ноутбуки, а потім мобільні та планшетні пристрої[10].

Це концепція, яка охоплює галузі та все більш поширена в сучасних корпоративних, державних, медичних та освітніх організаціях. Переваги впровадження політики BYOD у вашій компанії має ряд переваг[11]. До них належать:

- підвищення продуктивності співробітників. Одне дослідження показало підвищення продуктивності на 16% протягом 40-годинного робочого тижня;
- підвищення ефективності співробітників. Оскільки працівникам зручніше користуватися власними пристроями, вони можуть виконувати роботу швидше та ефективніше;
- підвищує комфорт співробітників. Працівники задоволені своєю роботою і з більшою ймовірністю залишаться в компанії завдяки гнучкому режиму роботи;
- загалом економить гроші IT-відділу (і компанії). IT не потрібно витрачати гроші на обладнання, програмне забезпечення, обслуговування пристроїв або

ліцензування, але все одно може скористатися перевагами оновлених технологій, інтегрованих у робоче місце.

Хоча BYOD має деякі переваги, є й недоліки, які слід враховувати. До них належать:

- відсутність повністю захищеної мережі. Немає закритої внутрішньої мережі яка обмежується лише комп’ютерами, що належать компанії;

- доступ до незахищеного Wi-Fi. Працівники, безсумнівно, використовуватимуть свої пристрої без вихідних. Таким чином, вони, ймовірно, отримають доступ до незахищеного Wi-Fi-з'єднання в магазинах, аеропортах, кав'ярнях і, можливо, власних будинках. Незахищені мережі можуть полегшити хакерам доступ до даних компанії;

- можливе збільшення витрат IT-відділу. Якщо IT-відділ вирішить, що вони наддадуть підтримку персональним пристроям, це може призвести до дещо збільшення витрат;

- відсутність безпеки на персональних пристроях. Співробітники можуть не мати належного антивірусного програмного забезпечення або брандмауера, встановленого на своїх пристроях;

- можливі порушення даних. Ваша компанія піддається підвищеному ризику порушенню даних у результаті втрати або крадіжки персональних пристроїв. Співробітники, які залишають компанію, також можуть поставити вас під загрозу порушення даних.

IT-відділ організації має вирішити, чи і як вони забезпечуватимуть персональні пристрої та визначити відповідні рівні доступу. Щоб захистити своїх співробітників і вашу компанію, дуже важливо мати чітко визначену політику безпеки BYOD. Ця політика має інформувати та навчати працівників, як використовувати свої пристрої на роботі, не завдаючи шкоди конфіденційним даним.

Політика BYOD має відповідати найкращим практикам. Вона повинна включати:

- типи дозволених пристроїв – Microsoft, Apple тощо;

- чітку політику безпеки та володіння даними для всіх пристроїв, які входять у приміщення;

- чіткі вимоги до паролів. Пристрої повинні мати надійні паролі, щоб захистити конфіденційність і запобігти злому даних;

- чи буде надаватися IT-підтримка для пристроїв співробітників і який рівень підтримки буде запропоновано. Також вказано має бути як співробітники можуть отримати ці IT-послуги;

- адекватна програма BYOD не лише реалізує MDM для керування пристроями, які мають доступ до мережі. Вона також реалізує контроль доступу до мережі або NAC. Це полегшує контроль доступу до корпоративних мереж і ресурсів. Дозвіл будь-якому пристрою підключатися до мережі компанії без контролю чи перевірки є небезпечним;

- чітке визначення кому належать які програми та дані. Це допоможе коли співробітник буде залишати компанію;

- перелік програм, які будуть дозволені, а які заборонені. Деякі програми, хоча й підходять для особистого використання, становлять ризик для даних компанії;

- правила відвідування веб-сайтів, не пов’язаних з роботою. Ці веб-сайти можуть включати соціальні мережі та розважальні сторінки. Деякі компанії блокують сайти у своїй мережі з метою безпеки та підвищення продуктивності співробітників;

- стратегія звільнення співробітника. Цей процес, включатиме відключення робочої електронної пошти та інших форм доступу та стирання робочих даних із особистих пристроїв;

- кроки, які повинні зробити співробітники, якщо вони отримають нові пристрої під час роботи. Якщо працівник оновить свій персональний комп’ютер або смартфон, що йому потрібно зробити?

- план відшкодування будь-яких витрат, пов’язаних із пристроєм. Наприклад, деякі компанії можуть платити за тарифний план мобільного передавання даних або частину вашого інтернет-з’єднання, якщо ви часто працюєте вдома.

Мобільна безпека та політика BYOD привертають набагато більше уваги з боку корпоративних IT компаній через зростаюче занепокоєння щодо використання смартфонів. Як результат, IT компанії продумано налаштовують існуючу корпоративну політику, щоб пристосуватися до мінливого ландшафту загроз і технологій. Загалом, політика мобільної безпеки та політики BYOD повинні включати такі документи:

- політика прийнятного використання мобільних пристроїв;
- політики BYOD, CYOD, COPE (корпоративна власність, особиста активність) і COBO (корпоративна власність, лише бізнес);
- політика безпеки мобільних пристроїв;
- приклад шаблонів політики мобільної безпеки та BYOD.

Правильні рішення безпеки можуть звести до мінімуму ризик BYOD і забезпечити безперебійну роботу вашої політики. Є кілька елементів, які повинні бути враховані ефективним рішенням безпеки BYOD. Ідеальним рішенням є рішення, яке охоплює декілька або всі ці елементи та сприяє комплексній стратегії безпеки мобільних пристроїв. Нижче наведено короткий опис різних заходів безпеки, які можна використовувати як частину комплексної програми безпеки BYOD[12].

Шифрування даних, що зберігаються та передаються

Оскільки використання BYOD виводить дані за межі контролю багатьох інших заходів безпеки підприємства, важливо, щоб організації шифрували конфіденційні дані в стані спокою та передавання. Шифрування гарантує, що вміст конфіденційних файлів буде захищено навіть у найгіршому випадку, наприклад, пристрій вкрадено або перехоплено трафік через незахищену мережу. Обов’язкове використання надійних паролів забезпечує певний захист, але шифрування краще. Як зазначається в цій статті Інституту InfoSec: «Щоб забезпечити захист, організаціям необхідно впровадити шифрування протягом усього життєвого циклу даних (в передачі та в стані спокою). А щоб запобігти несанкціонованому доступу та підтримувати шифрування у разі порушення безпеки, IT-відділ відповідної організації повинен взяти під контроль ключі шифрування».

Контроль встановлення додатку

Існують деякі елементи керування, доступні для певних пристроїв та операційних систем, які IT-спеціалісти можуть використовувати для контролю над програмами, встановленими на пристрої співробітника. Наприклад, пристрої Apple iOS можна налаштувати на заборону доступу до App Store, а для пристроїв Android компанії можуть використовувати Android Enterprise для керованого порталу Google Play, який містить лише схвалені програми (серед багатьох інших корисних функцій для BYOD). Однак обмеження можливості співробітника завантажувати або встановлювати програми на власні пристрої для особистого використання не є практичним рішенням для більшості компаній. Ці методи подібні до заходів, які вживаються з метою батьківського контролю, тому природно, працівники можуть відчувати, що це посягає на їх особисту свободу. Більшість співробітників сподіваються, що вони зможуть використовувати свої персональні пристрої на свій розсуд, коли вони не працюють, ведуть бізнес або не підключені до захищеної мережі компанії, що робить інші рішення більш практичними для безпеки BYOD. Варто зазначити, що Android Enterprise пропонує контейнерне середовище для розділення робочих і особистих додатків і даних, що дозволяє компаніям краще контролювати пристрої, які використовуються в робочих цілях, не обмежуючи особисте використання свого пристрою співробітниками. Нижче ми обговоримо контейнеризацію більш детально.

Керування мобільними пристроями

Рішення для керування мобільними пристроями (MDM) пропонують баланс між повним контролем для роботодавців і повною свободою для співробітників, пропонуючи можливість розгортати, захищати та інтегрувати пристрої в мережу, а потім централізовано відстежувати й керувати цими пристроями. Сфера MDM все ще знаходить свою основу і не позбавлена частки проблем. Наприклад, деякі підприємства можуть скористатися перевагами більш розширених функцій, доступних у MDM, створюючи менш ідеальний користувальницький досвід, який є занадто обмежуючим і змушує співробітників протистояти корпоративній програмі BYOD.

Контейнеризація

Контейнеризація все частіше пропонується в поєднанні з (або в парі з) рішеннями MDM. Контейнеризація — це метод, за допомогою якого частина пристрою може бути по суті відокремлена від решти програм і вмісту на пристрої у власний захищений міхур, захищений окремим паролем і регулюється окремим набором політик. Це дозволяє співробітникам насолоджуватися повним, безперешкодним використанням своїх пристроїв у вільний час, не створюючи ризиків для безпеки мережі компанії. Коли користувач увійшов у контейнерну зону, персональні програми та інші функції, не керовані контейнером, недоступні. Контейнеризація — це привабливе рішення, яке не обмежує можливості співробітників використовувати свої персональні пристрої на свій розсуд, усуваючи при цьому можливість використання або доступу співробітників до програм, які не відповідають порогу безпеки компанії під час роботи. Контейнеризація обмежує корпоративну відповідальність, не впливаючи на особисте використання, але, з іншого боку, вона не захищає персональні дані співробітників на пристроях, які втрачені або вкрадені та повинні бути стерті. Це проблема, яку легко подолати за допомогою належного резервного копіювання особистих даних.

Чорний список

Чорний список – це термін, який описує процес блокування або заборони певних програм, які, як визначено, становлять ризик для безпеки підприємства. Занесення в чорний список також є методом, який деякі компанії використовують для обмеження доступу співробітників до програм, які можуть заважати продуктивності, наприклад ігор або додатків для соціальних мереж. Служби обміну файлами – це ще одна категорія програм, які часто потрапляють у чорні списки, оскільки компанії побоюються, що співробітники можуть навмисно чи ненавмисно поділитися конфіденційною інформацією з неавторизованими третіми сторонами. Хоча цей метод може бути ефективним шляхом обмеження доступу до програм, які не відповідають критеріям безпеки вашої компанії, чорний список не часто використовується для BYOD, оскільки цей процес означає контроль доступу до програм на персональних пристроях співробітників як під час роботи, так і в

неробочий час. Звичайно, це створює проблему для деяких співробітників, які наприклад люблять грати в ігри, коли вони не на роботі.

Внесення до білого списку

Додавання в білий список є просто протилежністю чорного списку. Замість того, щоб блокувати доступ до списку конкретних програм, білий список дозволяє отримати доступ лише до списку схвалених програм. Цей процес часто вважається більш ефективним просто через величезну кількість існуючих додатків і веб-сайтів. Чекати, доки працівник завантажить програму та використає її для передачі даних, щоб визначити, що це загрожує безпеці, іноді занадто довго.

Додавання в білий список обходить цю проблему, просто забороняючи доступ до будь-чого, якщо воно не було попередньо схвалено IT як безпечне. Звичайно, як і внесення в чорний список, це може створити проблеми для BYOD, блокуючи доступ співробітників до програм, які вони хочуть використовувати, коли вони не на роботі.

Інші заходи безпеки BYOD

Існує ряд інших заходів безпеки, які іноді використовуються як частина комплексної програми безпеки BYOD. Наприклад, антивірусне програмне забезпечення, встановлене на окремих пристроях, часто є основним компонентом таких програм безпеки. Компанії можуть придбати корпоративну ліцензію та встановлювати програмне забезпечення на пристроях BYOD або просто вимагати від співробітників встановлення власних і перевіряти з IT-відділом, що їхні пристрої захищені. Оскільки зловмисне ПЗ націлено на мобільні пристрої, ризик того, що така шкідлива програма вплине на мережу компанії через особистий пристрій співробітника, дуже реальний.

Моніторинг – це ще один компонент, який іноді використовується як частина програми безпеки BYOD, хоча думки змішані. IT-спеціалісти могли б впровадити системи, які відстежують місцезнаходження пристроїв співробітників по GPS або інтернет-трафік на окремих пристроях. Хоча ці системи моніторингу можуть виявитися корисними для виявлення незвичайної активності або визначення місцезнаходження загубленого пристрою, багато хто вважає, що ці рішення заходять

занадто далеко в конфіденційність співробітників. Суть полягає в тому, що безпека BYOD, як і безпека підприємства, вимагає багатогранного підходу, який усуває потенційні ризики, зводячи до мінімуму вторгнення в конфіденційність і зручність використання, коли справа доходить до особистого використання. Контекстно-залежні рішення безпеки, які забезпечують контроль над доступом користувачів, додатками, мережевим підключенням і пристроями, на додаток до можливостей шифрування, поєднують ключові елементи, необхідні для забезпечення безпеки підприємства в ландшафті BYOD. Підприємства, які використовують ці рішення, користуються перевагами BYOD і пожинають плоди, такі як продуктивність і задоволення співробітників завдяки кращому балансу між роботою та особистим життям, одночасно ефективно пом'якшуючи ризики безпеки, які колись переслідували компанії, які впроваджували BYOD[13].

2.4 Проблеми впровадження BYOD

Використання мобільних пристроїв сьогоднішніми працівниками настільки ж поширене, як і самі смартфони. Межі розмиваються, оскільки співробітники переходять зі свого Instagram на файлообмінник компанії на своїх особистих пристроях. Недавнє опитування, проведене Samsung на замовлення компанії Oxford Economics, показало, що майже 80% роботодавців вважають, що їхні працівники не можуть виконувати свою роботу без власних мобільних пристроїв. Компанії покладаються на них, щоб зв'язатися з працівниками під час і після звичайного робочого дня. Співробітники покладаються на них, щоб залишатися на зв'язку зі своєю електронною поштою та іншими важливими бізнес-додатками[14].

Розвиток технології та очікувані витрати на забезпечення їх робочої сили захищеними пристроями зробили BYOD привабливою пропозицією для роботодавців. Працівникам подобається, що їм потрібно відстежувати лише один пристрій пристрою та зручність керування своїми особистими та робочими речами в одному місці[15].

У контрольному звіті інтелектуального управління інформацією за 2019 рік респонденти вказали, що:

- понад 60% співробітників використовують персональні програми для обміну файлами та/або персональні пристрої для доступу та обміну інформацією компанії;

- більше половини компаній (52%) відмовляють або забороняють використання персональних пристроїв.

Отже, яке рішення? У кількох дослідженнях було показано, що дозволивши співробітникам приносити свої власні пристрої це підвищило моральний дух та продуктивність працівників. Хоча в практиці BYOD є плюси і мінуси не всі компанії хочуть впроваджувати політику, яка є популярною та економічно ефективною. Причиною тому є найбільш помітні ризики.

Ризики BYOD стають більш очевидними, якщо врахувати вплив великої кількості різних точок входу в системи компанії. Якщо співробітники не завантажують критичні виправлення безпеки або не використовують захищені мережі для передачі критичних файлів вони наражають компанію на небезпеку. Щоб зрозуміти наскільки компанія готова протистояти різним небезпекам потрібно проаналізувати основні ризики. Сім основних ризиків BYOD:

- Можливості для крадіжки даних.

Політика BYOD дозволяє легко підтримувати контакт зі своїми співробітниками. Але що, якщо вони в аеропорту і відправлять файл через незахищену мережу Wi-Fi? Подумайте про ризики розкриття цієї інформації хакерами, які шукають доступ до критичних систем компанії, що особливо поширене в аеропортах. Хакери знайдуть можливість викрасти дані, і практика BYOD може стати для них чудовим середовищем для цього.

- Проникнення шкідливих програм.

Ваші співробітники використовують свої пристрої для завантаження різного роду інформації і можуть бути необережними щодо відокремлення та захисту цінних даних компанії від усього іншого. Що станеться, якщо вони ненавмисно завантажать мобільну гру з прихованим шкідливим програмним забезпеченням або

вірусами? Вони можуть передати його прямо в мережу вашої компанії під час наступного входу.

- Потенційні юридичні проблеми.

Репутація організації може бути серйозно пошкоджена, якщо порушення безпеки через пристрій співробітника призведе до витоку важливої інформації про ваших клієнтів або ділових партнерів. Це означає, можливо, розглядати судові позови різних сторін. Тоді вашій компанії потрібно буде викласти капітал, намагаючись захистити себе від юридичних проблем. Не кажучи вже про можливі юридичні санкції з боку місцевих, державних або федеральних органів влади, якщо вони визнають, що ваш бізнес не вжив достатньо запобіжних заходів для забезпечення безпеки пристрою.

- Втрата або крадіжка пристрою.

Співробітник, який втратив пристрій або його вкрали, може перерости від великої незручності до катастрофи для всієї вашої компанії, якщо він не дотримується рекомендованих протоколів безпеки компанії. Що робити, якщо у нього не було надійного пароля для входу в системи компанії? Чи полегшив він пошук паролів, зберігаючи їх десь на своєму пристрої?

Навіть якщо працівник зробив усе правильно, хакери тепер мають доступ до більш складних технологій. Хтось із достатньою рішучістю та вмінням може зламати надійний пароль або ідентифікатор відбитка великого пальця.

- Погане керування мобільними пристроями.

Співробітники можуть залишити вашу компанію з будь-якої причини. Як ви можете бути впевнені, що колишні співробітники більше не матимуть мобільного доступу до корпоративних програм? Наскільки легко їм із доступом до свого пристрою було б повернутися до програми чи системи? Чи зможете ви відстежити пристрій як джерело порушення безпеки?

- Відсутність навчання співробітників.

Багато порушень безпеки виникають через помилки співробітників. Вони можуть не повністю розуміти вимоги компанії, коли мова заходить про захист свого пристрою. Чи вимагаєте ви, щоб ваші працівники відвідували практичні інструктажі

чи просто підписували документ, в якому зазначено, що вони розуміють політику компанії? Неналежна підготовка може призвести до того, що співробітники будуть робити помилки, що призведе до компрометації безпеки систем вашої компанії.

- Тіньові IT.

Тіньові IT – це використання систем інформаційних технологій, пристроїв, програмного забезпечення, додатків і послуг без явного схвалення IT-відділу. Останніми роками він зріс у геометричній прогресії з використанням хмарних додатків і сервісів.

Хоча тіньові IT можуть підвищити продуктивність співробітників і стимулювати інновації, вони також можуть створити серйозні ризики для безпеки вашої організації через витік даних, потенційні порушення відповідності тощо.

Не варто відмовлятись у компанії від концепції BYOD через ряд ризиків так як плюси використання цієї технології виправдовують себе. Дотримання політики безпеки та рекомендацій щодо користування мобільними пристроями допоможе запобігти використанню пристроїв співробітників для здійснення кібератак на вашу компанію[16].

Висновки за розділом 2

Компанія потребує ефективної політики при впровадженні технології BYOD адже на сьогоднішній день багато співробітників звикли працювати на портативних пристроях і часто підключаються до корпоративних ресурсів компанії поза межами захищеної мережі офісу. Також при використанні цієї технології слід врахувати що пристрій може загубитись чи його викрадуть і це потребує визначених кроків.

Використання MDM систем дозволяє управляти, відстежувати та захищати дані на пристроях але не запобігає витоку даних з цих пристроїв тому для комлексного захисту потрібно використовувати поєднання з іншими методами контролю даних.

Також потрібно організувати спеціальне захищене середовище на якому співробітники зможуть зберігати конфіденційні дані у випадках коли буде потрібно

з ними працювати а доступу до мережі Internet буде з різних причин, наприклад води будуть в літаку чи в місцевості де низька швидкість інтернету або він взагалі відсутній.

У другому розділі дипломної роботи було розглянуто можливості та функції MDM-систем та критерії вибору цих систем. Також було розглянуто впровадження концепції BYOD та проблеми її впровадження.

РОЗДІЛ 3
РЕКОМЕНДАЦІЇ ВПРОВАДЖЕННЯ КОНЦЕПЦІЇ BYOD

3.1 Комплексна стратегія вирішення проблеми безпеки при використанні BYOD

Коли справа доходить до безпеки BYOD, будь-яка система керування мобільними пристроями (MDM) може бути ефективною лише як один із компонентів ширшої, комплексної стратегії безпеки мобільних даних. Систему MDM слід використовувати для вирішення загального управління та контролю мобільних пристроїв, шифрування даних тощо.

Одним із найкращих рішень щодо захисту даних у концепції BYOD є дистанційне підключення до ресурсів організації. В такому випадку пристрій використовує корпоративні дані без локального зберігання їх на внутрішні пам’яті, в рамках термінальних сесій з підключенням до серверів компанії, які захищені DLP-системою, що функціонує на віддаленому сервері або у віртуальних Windows-середовищах. Таке рішення називається Virtual DLP[17].

На відміну від локального зберігання даних на BYOD-пристроях в системах MDM, технологія Virtual DLP дозволяє організувати контрольований віддалений доступ до ресурсів компанії. Працівникам надають підключення до даних тільки після авторизації облікового запису в домені AD чи іншому каталозі LDAP. Створюється VPN-тунель, який забезпечує надійне та захищене з’єднання і автентифікацію користувача та/або пристрою. В такому підході забезпечується три ключові умови безпеки:

– безпечна обробка даних – співробітники не працюють з програми для локальної обробки даних на пристрої BYOD. Це гарантує, що корпоративні дані компанії не будуть поширені далі контрольованого пристрою;

– безпечне зберігання даних. Корпоративні дані організації зберігаються тільки на серверах компанії, а не на персональних пристроях тому можливо

забезпечити належний контроль і резервне копіювання на стороні організації. При цьому локальне збереження даних у вбудованій пам'яті BYOD-пристроїв, що підключаються не допускається або контролюється компанією;

– моніторинг даних. Моніторинг доступу до всіх конфіденційних файлів і запис детальних даних про використання, таких як користувач, відділ, файл, до якого зверталися, тип файлу та час відповіді операції.

Для того щоб працівники могли продуктивно працювати потрібно забезпечити швидку адаптацію до моделі віртуалізації, підтримку віртуального середовища і широкий функціонал робочого середовища. Це означає обов’язкову наявність додатків у віртуальному середовищі які можуть якісно використовуються для роботи з даними або для комунікацій:

– браузер для виходу в Internet;

– клієнт електронної пошти;

– клієнти обміну повідомленнями;

– програми для роботи з документами різних типів (Microsoft Office або інший);

– інші додатки, що необхідні для виконання посадових обов'язків[18].

Завдяки рішенням vDLP усі програми, які обробляють корпоративні дані, працюють у віртуальному сеансі Windows, тобто на сервері організації. Завдяки такому підходу служби ІБ зберігають повний контроль над робочими даними, оскільки сховище знаходиться не на пристрої BYOD, а на їхньому сервері, а співробітники можуть вільно використовувати програми, опубліковані на віртуалізованих серверах.

Щоб розробити повноцінне та ефективне вирішення щодо запобігання витоків даних з смартфонів MDM-системи повинні впроваджуватись разом з резидентними DLP-системами. Так як MDM-системи не виконують запобігання витоків даних але відіграють значну роль у забезпеченні безпеки стратегії BYOD.

Спеціалізовані рішення DLP можуть допомогти організаціям вирішити проблему швидкої інтеграції персональних мобільних пристроїв у технічні бізнес-процеси, включаючи виявлення критично важливих бізнес-даних, визначення

правил роботи, а також зберігання та передачу даних за межі компанії (або всередині компанії).

Канали витоку інформації існують у будь-якому інформаційному просторі. Персональних мобільних пристроїв, що можуть стати причиною втрати інформації стає все більше – це смартфони, планшети, флеш-носії, цифрові камери, і навіть MP3-плеєри. Канал витоку в найзагальнішому розумінні розуміється як неконтрольований спосіб передачі інформації. В результаті зловмисник може отримати несанкціонований доступ до потрібних йому конфіденційних даних компанії. Для вирішення цієї проблеми і призначені спеціалізовані резидентні DLP-системи.

Компанії, які працюють з конфіденційною інформацією будь-якого типу, потребують власної комплексної системи безпеки, яка є перешкодою для зловмисника на всіх рівнях обробки даних. На технічному рівні системи DLP можуть запобігти витоку, автоматично виявляючи спробу несанкціонованої передачі інформації за межі захищеного середовища.

Скрізь де USB підключення може призвести до обміну даними обов’язковим є використання методів контролю та фільтрації підключення, тому що це може призвести до витоку даних. Найбільша частина таких втрат даних пов’язана з підключенням пристроїв через USB порт. Фахівці з ІБ повинні визначати права доступу і політики безпеки для користувачів і груп відповідно до їх функціональних обов'язків[19].

Безпека BYOD

1 ПЗ CCleaner v 4.13 – це безкоштовний, потужний і простий у використанні додаток для очищення і оптимізації 32-бітних і 64-розрядних ОС Microsoft Windows.

2 VM – віртуалізація Windows-системи, що дозволяє користувачам працювати у віртуальному робочому середовищі.

3 App – додаток для віддаленого підключення пристрою через мережу Інтернет до віртуального хостингу додатків організації.

4 DLP – система запобігання витоків даних, інтегрована у віртуальне робоче середовище Windows.

5 MDM – це ПЗ, яке дозволяє IT-департаментам автоматизувати, контролювати та захищати адміністративні політики на ноутбуках, смартфонах, планшетах чи будь-якому іншому пристрої, підключеному до мережі організації. Мета MDM — максимізувати підтримку пристроїв, організаційну функціональність та безпеку, забезпечуючи певну гнучкість користувача, наприклад для використання концепції BYOD.

6 Криптографічний сервер «Славутич». Виконує такі функції:

– захист TCP/IP з’єднань за допомогою шифрування запитів "клієнтів" та відповідей серверів;

– контроль цілісності даних за рахунок перевірки хеш-коду;

– автентифікація інших криптографічних серверів.

7 VPN (TorGuard) – Потужна служба VPN TorGuard пропонує необмежену швидкість та пропускну здатність для вашого бізнесу на більш ніж 3 000 серверах у 50 країнах світу. Ви можете пристосувати ваш пакет відповідно до розміру вашого бізнесу, з опціями для 8 з'єднань та зашифрованих електронних поштових облікових записів. Користувацькі облікові записи включають виділений сервер, до 30 виділених IP-адрес та 24/7 доступ до адміністратора VPN[20].

3.2 Кроки на шляху впровадження BYOD

Політика BYOD дає співробітникам більшу гнучкість у використанні смартфонів, які їм надають перевагу, на роботі. Концепція BYOD це зростаюча тенденція, яку IT компанії мають ввести у свої офіси. Тим не менш, багато IT-менеджерів продовжують нервувати щодо створення стратегій і відмовляються від контролю над мобільними пристроями. Нижче наведено план з 9-ти пунктів, який допоможе вирішити проблеми відповідальності, безпеки та досвіду співробітників[21].

1. Вирішіть, чи підходить BYOD для вашої організації

Приділіть деякий час, щоб спочатку обміркувати плюси та мінуси використання власної політики щодо пристроїв. Якщо у вас є ризики вище

середнього (наприклад, національна оборонна промисловість), BYOD може бути не найкращим кроком для вас. Завдяки добре розробленій політиці BYOD економить гроші компанії та надає співробітникам більшу гнучкість.

2. Встановіть політику безпеки

Тепер, коли ваші співробітники можуть отримувати конфіденційну інформацію з дому, ваша політика має вирішувати можливі підводні камені. Це включає встановлення суворих вимог до паролю, щоб — якщо пристрій потрапив у чужі руки — ви могли бути впевнені, що ваші дані в безпеці.

Крім паролів, у вашому плані впровадження BYOD має бути зазначено:

- мінімальний необхідний контроль безпеки для пристроїв;

- де саме будуть зберігатися дані (включаючи те, що зберігається локально);

- тайм-аут неактивності;

- чи вимагаєте від співробітників завантажити програму безпеки для мобільних пристроїв;

- ваша політика віддаленого стирання.

Залежно від вашої галузі, вам може знадобитися створити додаткові обмеження на основі вимог відповідності.

3. Створіть посібник із прийнятного використання

Якщо у вас ще немає «Політики прийнятного використання», вам слід створити її разом із політикою BYOD. Ця політика допоможе вашим співробітникам не відволікати вас, убезпечивши вашу мережу від вірусів і шкідливих програм.

Створюючи посібник із прийнятного використання, окресліть, до яких програм працівникам дозволено доступ зі своїх особистих пристроїв, а до яких обмежено. Ви також повинні звернути увагу:

- які веб-сайти заборонені, коли пристрій підключено до мережі компанії;

- до яких типів корпоративних даних працівники можуть отримати доступ зі своїх пристроїв;

- які дисциплінарні заходи ви будете застосовувати, якщо хтось порушить політику.

Зауважте одну річ: не блокуйте такі веб-сайти, як Facebook або YouTube. Блокування цих сайтів може здатися надмірним контролем, особливо з особистих пристроїв ваших співробітників. Вам потрібен прийнятний посібник із використання, який не є занадто суворим і показує, що ви довіряєте своїй команді.

4. Визначте сферу застосування прийнятних пристроїв

Створіть список пристроїв, які ви дозволите використовувати співробітникам для роботи. Наприклад, ви можете вказати смартфони Android або певні моделі iPhone. Додаток Mobile Forms від Device Magic є кросплатформним, але вам потрібно буде визначити, які інші програми використовуватимуться, якщо ви розглядаєте змішане середовище. Щоб створити свій список, врахуйте кілька факторів. По-перше, якими пристроями вже володіють співробітники? По-друге, які пристрої ви можете ефективно контролювати за допомогою ваших систем керування BYOD?

5. Установіть програмне забезпечення для керування мобільними пристроями

Програмне забезпечення для керування мобільними пристроями (MDM) дозволяє налаштовувати, керувати та контролювати всі персональні пристрої за допомогою однієї програми. Ваша IT-команда може потім авторизувати налаштування безпеки та конфігурації програмного забезпечення на будь-якому пристрої, підключеному до вашої мережі.

За допомогою програмного забезпечення MDM ваша IT-команда може створювати автоматичне резервне копіювання інтелектуальної власності вашої компанії за допомогою хмари, сканувати на наявність вразливостей у вашій системі, блокувати мобільні пристрої, які можуть бути загрозами, забезпечувати оновлення програм для захисту від шкідливих програм, віддалено оновлювати та виправляти проблеми тощо. дотримуватись політики безпеки.

6. Використовуйте двофакторну аутентифікацію для програм компанії

Двофакторна аутентифікація не дозволяє хакерам видавати себе за користувачів і отримати доступ до облікових записів компанії. Вона забезпечує безпеку вашої секретної інформації, змушуючи кожного, хто входить у програму, пройти додатковий крок, наприклад, надати відповіді на таємні запитання або

використовувати код, який було надано в електронному листі чи текстовому повідомленні.

7. Захистіть дані компанії та персональні дані на пристроях співробітників

Звичайно вам потрібно захистити власні дані в політиці BYOD, але також корисно захистити персональні дані ваших співробітників. Ваші співробітники заслуговують на певний рівень конфіденційності.

Ваше програмне забезпечення та процеси MDM ніколи не повинні взаємодіяти, копіювати чи зберігати особисту інформацію, програми та інші дані вашого співробітника, наприклад інформацію про місцезнаходження.

8. Спростіть процес реєстрації

Процес реєстрації для вашої програми BYOD має бути простим. Не просіть співробітників заповнювати паперову форму або проходити кілька раундів затвердження. Ваші співробітники повинні мати можливість зареєструватися через систему IT-квиток, щоб відстежувати всі запити та їх прогрес. Після реєстрації їм не потрібно завантажувати занадто багато різних додатків — однієї або лише кількох має вистачити, щоб отримати доступ до потрібної інформації без зайвої роботи.

9. Проводьте навчання для своїх співробітників (регулярно)

Проводьте регулярні навчальні семінари, щоб ваші співробітники були в курсі політики BYOD та потенційних ризиків недотримання правил. Ви також можете створити докладний посібник або дозволити співробітникам запланувати індивідуальне навчання з кимось із IT-відділу. Таким чином, співробітники не тільки дізнаються, як найкраще використовувати свої пристрої, а й розуміють потенційні ризики та те, як компанія планує уникнути таких проблем.

3.3 Політики впровадження BYOD

Цей документ містить вказівки щодо використання особистих смартфонів та/або планшетів співробітниками (користувачами) [Назва компанії] для доступу до мережевих ресурсів [Назва компанії]. Доступ і використання мережевих служб

надається за умови, що кожен користувач читає, підписує, поважає та дотримується політики [Назва компанії] щодо використання цих пристроїв і послуг[22].

1. Призначення цього BYOD

[Назва компанії] надає своїм співробітникам привілей використовувати власні смартфони та планшети на свій вибір на роботі для їхньої зручності. Ця Політика BYOD призначена для захисту конфіденційності, безпеки та цілісності даних і технологічної інфраструктури [Назва компанії] від ризиків, які можуть виникнути, коли співробітники використовують свої особисті пристрої в бізнес-цілях. Співробітники [Назва компанії] повинні погодитися з положеннями та умовами, викладеними в цій політиці, щоб мати можливість підключати свої пристрої до мережі компанії.

2. Пристрої BOYD

Наступні пристрої дозволені для використання співробітниками BYOD та підключення до мережі [НАЗВА КОМПАНІЇ]:

- Android Смартфони та планшети;
- смартфони Blackberry з та Playbook;
- IOS iPhone та iPads;
- [СПИСОК ВСІХ ІНШИХ ДОЗВОЛЕНИХ ПРИСТРОЇВ].

Перш ніж отримати будь-який доступ до мережі компанії, пристрої повинні бути представлені IT-відділу для належного забезпечення роботи та налаштування стандартних програм, таких як браузери, офісне програмне забезпечення та засоби безпеки.

3. Конфіденційність

[НАЗВА КОМПАНІЇ] буде поважати конфіденційність вашого особистого пристрою та запитуватиме доступ до пристрою лише у технічних спеціалістів для впровадження заходів безпеки, як зазначено нижче, або для відповіді на законні запити на виявлення, які виникають у ході адміністративного, цивільного чи кримінального провадження (застосовується лише якщо користувач завантажує державну електронну пошту/додатки/документи на свій особистий пристрій).

4. Прийнятне використання

а) Компанія визначає прийнятне комерційне використання як діяльність, яка прямо чи опосередковано підтримує бізнес [Назва компанії].

б) Компанія визначає прийнятне особисте обмежене використання часу компанії (особисте спілкування або відпочинок) таке як…[Вказати].

в) Співробітники можуть використовувати свої пристрої BYOD для прийнятного ділового та особистого використання [Назва компанії], як зазначено в політиці використання комп’ютерів [Назва компанії].

г) Співробітники можуть використовувати свій мобільний пристрій для доступу до таких ресурсів компанії: [Електронна пошта / Календар / Контакти / Документи / Вказати].

д) Наступні програми дозволені для завантаження, встановлення та використання на пристроях BYOD [Вказати програми].

5. Обмеження

а) Співробітникам заборонено доступ до певних веб-сайтів у робочий час/під час підключення до корпоративна мережа на розсуд компанії. Такі веб-сайти включають, але не обмежуються до: [ВКАЗАТИ].

б) Співробітники не можуть використовувати свої пристрої BYOD в робочий час в особистих цілях, які не дозволені для використання комп'ютерів [НАЗВА КОМПАНІЇ], як зазначено в Політиці використання комп'ютерів [НАЗВА КОМПАНІЇ]. Наприклад, пристрої BYOD не можуть використовуватися для доступу порнографічних або образливих матеріалів, зберігання або передачі закритої інформації [НАЗВА КОМПАНІЇ], вчинення переслідувань, заняття підприємницькою діяльністю, яка суперечить їхнім інтересам, обов’язкам щодо [НАЗВА КОМПАНІЇ] тощо.

в) Наведені нижче програми заборонені для завантаження, встановлення та використання на пристроях BYOD. [ВКАЗАТИ]

г) [НАЗВА КОМПАНІЇ] має політику нульової терпимості до текстових повідомлень або електронної пошти за кермом, і дозволено розмовляти лише без рук під час водіння.

6. Чутливі дані

Користувач не буде завантажувати або передавати конфіденційні бізнес-дані на свої персональні пристрої. Конфіденційні бізнес-дані визначаються як документи або дані, втрата, неправильне використання або несанкціонований доступ яких може негативно вплинути на конфіденційність або добробут особи (особисту інформацію), результат звинувачення/скарги/справи, конфіденційну інформацію або фінансові операції компанії.

7. Обов'язки

Після того, як працівники зрозуміли наслідки та погодилися з політикою, вони мають певні обов’язки, коли справа доходить до їхніх пристроїв. Вони не повинні дозволяти зручності та доцільності переважати політику і повинні використовувати лише схвалені пристрої та програмне забезпечення перевірені ІТ-відділом. Про всі втрачені або вкрадені пристрої необхідно негайно повідомити до ІТ-відділу (та оператора мобільного зв’язку) у межах 24 години. Працівник може нести відповідальність за заміну персонального пристрою, як зазначено в політиці, але він все одно матиме конфіденційну інформацію, яка може бути скомпрометована. Навіть під час ремонту працівники повинні використовувати авторизовані ремонтні центри, щоб гарантувати, що конфіденційна інформація не буде порушена під час ремонту.

Нарешті, співробітники повинні знати про вектори кібератак, включаючи зловмисне ПЗ та соціальну інженерію. Телефони та пристрої, що діють за політикою BYOD, не можна нікому позичати друзям, родичам або будь-кому іншому.

Політика BYOD може працювати, але внесок співробітників є важливим для створення ефективної політики. Політика, яка надто обмежує або не забезпечує підтримку відповідних пристроїв, призведе до відсутності участі співробітників. Кожен причетний несе відповідальність за досягнення успіху політики BYOD.

Захист пристроїв і даних за межами офісу

Існують унікальні проблеми безпеки, пов’язані з роботою за межами офіційного офісу У цьому підрозділі ви дізнаєтеся найкращі методи захисту ваших пристроїв і даних за межами офісного середовища. Майте на увазі, що найкращі

методики слід використовувати з усіма пристроями (ноутбуками, телефонами, планшетами тощо).

1. Користування безкоштовним Wi-Fi. Зручність безкоштовного підключення може бути привабливою. Однак мережі з відкритим доступом (тобто ті, до яких можна отримати доступ без паролів) набагато небезпечніші, ніж безпечні з'єднання, які можна знайти на робочому місці. Безкоштовний Wi-Fi – це точка доступу для злочинців Окрім переваг безкоштовного Wi-Fi є і недолік: будь-хто може підключитися до нього в будь-який момент. Хакери можуть стежити за з'єднаннями Wi-Fi з відкритим доступом і стежити за вашою діяльністю в Інтернеті. Якщо ви не здійсните заходів безпеки, злочинці можуть побачити ваші імена користувачів, паролі, важливі електронні листи, дані кредитної картки або розповсюджувати шкідливе програмне забезпечення. Поради щодо безпеки в Wi-Fi із відкритим доступом. Використовуйте https. Ніколи не обмінюйтеся конфіденційними даними із сайтом, URL-адреса якого не починається з https. Сайти, які використовують https (замість http), забезпечують безпечні з'єднання та захищають ваші дані від шпигунів. Завжди використовуйте https, коли ви входите на сайт, вводите пароль, магазин або банк у відкритій мережі Wi-Fi. Пам'ятайте: https не гарантує, що сам сайт безпечний. Це лише гарантує, що ваше спілкування з цим сайтом є безпечним.

2. Використовуйте VPN. Якщо у вас є доступ до своєї корпоративної VPN або віртуальної приватної мережі (або іншої безпечної VPN) під час подорожі, використовуйте її для захисту своєї діяльності в Інтернеті. VPN створюють безпечні з'єднання, використовуючи шифрування та інші заходи, що дозволяють безпечно передавати дані через Інтернет

3. Обмежте свою діяльність. Якщо ви не використовуєте VPN тоді суворо обмежте свою діяльність в Інтернеті (тобто не входьте на захищені сайти та не виконуйте жодних фінансових операцій). Уникайте передачі конфіденційних даних, включаючи номери кредитних карток, під час підключення до мережі Wi-Fi з відкритим доступом.

4. Будьте особливо обережні з публічними комп'ютерами. Немає способу переконатися, що вашу інформацію не викрадають на загальнодоступному

комп’ютері. Антивірусне програмне забезпечення та брандмауери не захищають вас від хакерів у спільній мережі. Ніколи не входьте на веб-сайти та не вводьте будь-яку особисту інформацію на загальнодоступному пристрої — навіть за допомогою https. Єдине, що ви повинні робити на загальнодоступному комп’ютері, це переглядати.

5. Найкращі методи захисту даних вдома. Інформаційна безпека. Не розміщуйте конфіденційну інформацію на портативних пристроях. Набагато імовірніше, що дані будуть втрачені або вкрадені, якщо їх помістити на портативний пристрій. Якщо ваші дії ставлять під загрозу комерційну таємницю, фінансові дані компанії або інтелектуальну власність, ваш роботодавець може втратити мільйони, а ви можете втратити роботу. Конфіденційну інформацію слід залишити в офісі або отримати віддалений доступ через захищені сервери компанії.

6. Спільний доступ до файлів. Не використовуйте несанкціоновані рішення для спільного доступу на своїх пристроях. Рішення для обміну файлами, як-от хмарні програми для зберігання даних і приватні однорангові мережі, можуть нести значні ризики для безпеки. Ніколи не встановлюйте несанкціоноване програмне забезпечення та не використовуйте неавторизовані програми на своїх корпоративних пристроях. Не вмикайте спільний доступ до файлів на своєму комп’ютері, якщо цього не порадив ваш ІТ-відділ.

7. Безпека пристрою. Не дозволяйте друзям або родині використовувати ваші корпоративні пристрої. Дозволяючи друзям використовувати ваш робочий ноутбук, щоб перевіряти електронну пошту або дозволяючи дітям грати в ігри на вашому корпоративному смартфоні, ви ставите під ризики дані на вашому пристрої. Ви несете відповідальність за безпеку своїх корпоративних пристроїв і даних, які вони зберігають.

8. Резервні копії також захищають дані. Резервні копії гарантують, що цілісність даних не буде порушена, а дані можуть бути відновлені, коли це необхідно. Дотримуйтесь політик вашої організації щодо резервного копіювання та відновлення. Поговоріть зі своїм ІТ-відділом про використання затверджених компанією методів резервного копіювання.

9. Будьте уважні до фізичної безпеки. Не залишайте сумки для ноутбуків або мобільні пристрої без нагляду в аеропортах, конференціях, зустрічах. Візьміть ці пристрої з собою, навіть якщо виходите зі столу, щоб забрати замовлення на прилавку. Відкладіть свій мобільний телефон перед тим, як зайнятися такими видами діяльності, як перевірка багажу або оплата кави.

10. Будьте уважні до підслуховування. Коли ви користуєтеся ноутбуком, планшетом або мобільним телефоном у громадських місцях, задайте собі ці два запитання: Що незнайомці можуть бачити на моєму екрані? Що чують незнайомі люди? Вживайте заходів, щоб ваші приватні розмови та спілкування залишалися конфіденційними.

11. Пам’ятайте про електронні сліди. Здавалося б, невинна онлайн-діяльність може розповісти багато про ваші звички, зокрема про те, де ви знаходитесь, а де ні. Будьте обережні, користуючись електронними реєстраціями та повідомляючи своє місцезнаходження на фотографіях та публікаціях у соціальних мережах, особливо якщо ви займаєтесь конфіденційною справою.

12. Беріть свої пристрої з собою, коли це можливо. Слідкуйте за своїми пристроями, якщо ви подорожуєте або відвідуєте громадське місце. Фізична охорона свого ноутбука – найкраща профілактика крадіжки. Не кладіть свій ноутбук або інший пристрій на землю там, де його не видно[23].

Висновки за розділом 3

Отже коли справа доходить до безпеки BYOD, будь-яка система керування мобільними пристроями (MDM) може бути ефективною лише як один із компонентів ширшої, комплексної стратегії безпеки мобільних даних. Систему MDM слід використовувати для вирішення загального управління та контролю мобільних пристроїв, шифрування даних тощо.

Одним із найкращих рішень щодо захисту даних у концепції BYOD є надання доступу до ресурсів компанії через віддалене підключення. В такому випадку пристрій використовує корпоративні дані без локального зберігання їх на внутрішні

пам’яті, в рамках термінальних сесій з підключенням до серверів компанії, які захищені DLP-системою, що функціонує на віддаленому сервері або у віртуальних Windows-середовищах.

Політика BYOD може працювати, але внесок співробітників є важливим для створення ефективної політики. Політика, яка надто обмежує або не забезпечує підтримку відповідних пристроїв, призведе до відсутності участі співробітників. Кожен причетний несе відповідальність за досягнення успіху політики BYOD.

ВИСНОВКИ

Майже для кожної галузі використання мобільного пристрою під час роботи є звичним явищем. Не використовувати його для роботи здавалося б майже дивним. Поки в Україні інтерес до концепції BYOD одиночний і лише найбільш розвинені компанії розробляють такі рішення для себе.

Компанія потребує ефективної політики при впровадженні технології BYOD адже на сьогоднішній день багато співробітників звикли працювати на портативних пристроях і часто підключаються до корпоративних ресурсів компанії поза межами захищеної мережі офісу. Також при використанні цієї технології слід врахувати що пристрій може загубитись чи його викрадуть і це потребує визначених кроків.

Також ефективна стратегія BYOD повинна забезпечити управління, відстеження, захист даних а також запобігати витокам даних.

В першому розділі дипломної роботи було розглянуто актуальність проблеми захисту локальної мережі підприємства за концепцією BYOD, розглянули проблеми VPN мереж для ОС IOS, розглянули постачальників рішень MDM і її мінімальний набір функцій, була проаналізована сама технологія BYOD та визначено цілі впровадження цієї технології.

У другому розділі дипломної роботи було розглянуто можливості та функції MDM-систем та критерії вибору цих систем. Також було розглянуто впровадження концепції BYOD та проблеми її впровадження.

У третьому розділі дипломної роботи було розроблено комплексну стратегію вирішення проблеми безпеки при використанні BYOD, кроки як потрібно реалізувати впровадження концепції BYOD та розроблено ПБ яку можна використовувати для підприємства чи організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bring Your Own Device (BYOD) - особисті пристрої в роботі: наскільки це безпечно і що чекає на ваш IT-відділ? [Електронний ресурс] / Спосіб доступу: URL: https://skomplekt.com/solution/byod.htm/.

2. Make your Everywhere Workplace possible [Електронний ресурс] / Спосіб доступу: URL: https://www.ivanti.com/?miredirect.

3. 10 найкращих програм MDM: рішення для управління мобільними пристроями в 2021 році [Електронний ресурс] / Спосіб доступу: URL: https://uk.myservername.com/10-best-mdm-software.

4. Data Loss Prevention (DLP) [Electronic resource] / Access: URL: https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/.

5. Mobile Device Management (MDM) Explained [Electronic resource] / Access: URL: https://www.bmc.com/blogs/mdm-mobile-device-management/.

6. A Complete Guide to Mobile Device Management (MDM) [Electronic resource] / Access: URL: https://www.miradore.com/blog/mdm-mobile-device-management/.

7. What is BYOD and why it's important [Electronic resource] / Access: URL: https://www.appsanywhere.com/resource-centre/byod/what-is-byod-and-why-its-important.

8. Is BYOD (Bring Your Own Device) dead? [Electronic resource] / Access: URL: https://www.netmotionsoftware.com/blog/industry-disruption/is-byod-dead.

9. What is Bring Your Own Device (BYOD)? [Electronic resource] / Access: URL: https://planergy.com/blog/what-is-byod/.

10. The Challenges of BYOD and Why IT Support is Crucial [Electronic resource] / Access: URL: https://www.htl.london/blog/byod-challenges-and-why-it-support-is-crucial?format=amp.

11. Introducing BYOD in an organisation: the risk and customer services viewpoints [Electronic resource] / Access: URL:

https://www.researchgate.net/publication/267642925_Introducing_BYOD_in_an_organisation_the_risk_and_customer_services_viewpoints.

12. Byod definition [Electronic resource] / Access: URL: https://www.yourdictionary.com/byod.

13. Reducing Risk: How to Make BYOD Safer [Electronic resource] / Access: URL: https://www.securitymagazine.com/articles/86319-reducing-risk-how-to-make-byod-safer.

14. How to Implement a BYOD Policy Your Employees Will Actually Follow [Electronic resource] / Access: URL: https://kmicro.com/how-to-implement-a-byod-policy-employees-will-follow/.

15. 10 Successful Steps to Implement a Bring Your Own Device (BYOD) Policy [Electronic resource] / Access: URL: https://www.navitend.com/blog/article/10-successful-steps-to-implement-a-byod-policy.

16. 7 Things to Include in your BYOD Policy [Electronic resource] / Access: URL: https://www.titanfile.com/blog/7-things-to-include-in-your-byod-policy/amp/.

17. Security best practices for BYOD policies [Electronic resource] / Access: URL: https://www.techadvisory.org/2021/07/security-best-practices-for-byod-policies/.

18. BYOD policy best practices [Electronic resource] / Access: URL: https://www.powerdms.com/policy-learning-center/byod-policy-best-practices.

19. The Pros and Cons of a Bring Your Own Device (BYOD) to Work Policy [Electronic resource] / Access: URL: https://www.thebalancecareers.com/bring-your-own-device-byod-job-policy-4139870.

20. What Does BYOD Mean? Bring Your Own Device Definition [Electronic resource] / Access: URL: https://www.indeed.com/career-advice/career-development/what-does-byod-mean.

21. 8 Steps for Successfully Implementing a BYOD Policy [Electronic resource] / Access: URL: https://www.devicemagic.com/blog/8-steps-successful-byod-policy/.

22. ЯК: Вступ до BYOD для IT-мереж - 2022 [Електронний ресурс] / Спосіб доступу: URL: https://uk.go-travels.com/71340-an-introduction-to-byod-for-it-networks-817819-5666581.

23. BYOD Security: Expert Tips on Policy, Mitigating Risks, & Preventing a Breach [Electronic resource] / Access: URL: https://digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing-breach.ю.

ДОДАТОК А
ПОРІВНЯННЯ НАЙКРАЩИХ ПРОГРАМ ДЛЯ УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ

Програмне забезпечення для планування проектів	Платформа	Особливості	Найкраще для	Рейтинги	Ціна
Мірадоре	Android, iOS, macOS та Windows.	Реєстрація та керування пристроями, Відстеження місцезнаходження, Управління програмами, Автоматизація, Захист пристроїв та даних, Технічна підтримка.	Безпечне, ефективне та легке управління мобільними пристроями.	5.0	План Freemium для необмежених пристроїв; 14-денна безкоштовна пробна версія, $ 2 до $ 3 / пристрій на місяць.
IBM MaaS360	Android, iOS, macOS та Windows.	Легке управління пристроями, Швидке розгортання додатків, Захищена співпраця над вмістом, Безпечне рішення MDM.	Безпечне управління мобільними пристроями.	5.0	30-денна безкоштовна пробна версія, $ 4,00 - $ 9,00 на клієнта або пристрій на місяць.
Від MobiControl	Windows, Android, iOS, macOS та Linux.	Правила дотримання / попередження, Інтерактивна програма, каталог Захищений пристрій, програми, вміст та дані, Швидке забезпечення та реєстрація.	Швидке забезпечення та зарахування.	5.0	30-денна безкоштовна пробна версія, Від 3,25 до 90 доларів США / пристрій на місяць,
Люкс 'Барамунді'	Веб-програма, Windows,	Віддалена підтримка, Діагностичні	Управління мобільними активами та	5.0	30-денна безкоштовна пробна версія,

	Macintosh.	інструменти, Безперервність бізнесу, Журнал резервного копіювання Управління IT-активами, управління аудитом Контроль доступу / дозволи управління IT Управління ліцензіями, Захист від копіювання.	аудитом.		5000 доларів безстрокової ліцензії, $ 25,90 за пристрій плюс щорічна плата за обслуговування, що варіюється від 3,50 до 5,50 доларів США.
Управління кінцевою точкою Citrux (раніше XenMobile)	Windows 10, ОС Google Chrome та Apple macOS.	Єдина консоль, управління кінцевими точками, Унікальні можливості мікро-VPN, Управління мобільними додатками, Citrix Secure Mail.	Захищена пошта та унікальні можливості мікро-VPN.	4.5	30-денна безкоштовна пробна версія, Від 3,26 до 27 доларів США / пристрій / місяць.
Jamf Pro	Усі мобільні пристрої Apple.	Інтеграція API, Розширені конфігурації, Управління програмами, Підтримка Apple TV, Менеджер школи Apple, інтеграція, Управління дотриманням вимог.	Розширена конфігурація та інтеграція з рішеннями Apple.	5.0	30-денна безкоштовна пробна версія, $ 3,33 / місяць / пристрій iOS або tvOS, $ 7,17 / місяць / Mac.