МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 004.12:681.3

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____ к.т.н. Г.В. Шуклін
«____» _____ 2022 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: «ДОСЛІДЖЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ ПРИ ВЗАЄМОДІЇ З МОБІЛЬНИМИ КОРИСТУВАЧАМИ»

студент групи СЗД-41 Захарченко Кирило Ігорович _____
(підпис)

Науковий керівник: к.т.н., доцент Пепа Юрій Володимирович _____
(підпис)

Нормоконтроль: Гребенніков Асаді Болдхоядович _____
(підпис)

КИЇВ – 2022

ЗАТВЕРДЖУЮ
Завідуючий кафедрою СІКЗ
к.т.н., доцент
_____ Шуклін Г.В
“____”_____2022 р.

ЗАВДАННЯ
на атестаційну роботу
ЗАХАРЧЕНКУ КИРИЛУ ІГОРОВИЧУ

1. **Тема роботи:** Дослідження захисту інформації в корпоративній мережі при взаємодії з мобільними користувачами, керівник Пепа Юрій Володимирович, доцент, затверджена наказом вищого навчального закладу від 27 лютого 2022 року №__.

2. **Строк подання** студентом роботи 20 травня 2022 р.

3. **Вихідні дані до роботи**: розглянути основні напрямки для захисту інформації мобільних користувачів в корпоративній мережі та які види атак можуть здійснювати зловмисники для отримання даних підприємства.

4. **Зміст пояснювальної записки (перелік питань, які потрібно розробити):**

4.1. Аналіз загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв.

4.2. Захист корпоративної інформації на мобільних пристроях.

4.3. Політика компаній щодо захисту корпоративних даних.

5. Перелік графічного матеріалу:

5.1. Презентація на слайдах.

6. Дата видачі завдання 16 лютого 2022 року.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «16» лютого 2022 р.

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів	Примітка
1.	Уточнення постановки завдання	16.03.22 р.	Виконано
2.	Аналіз літератури	23.03.22 р.	Виконано
3.	Обґрунтування вибору рішення	26.03.22 р.	Виконано
4.	Збір даних	30.03.22 р.	Виконано
5.	Аналіз загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв	06.04.22 р.	Виконано
6.	Захист корпоративної інформації на мобільних пристроях	20.04.22 р.	Виконано
7.	Політика компаній щодо захисту корпоративних даних	04.05.22 р.	Виконано
8.	Оформлення та друк пояснювальної записки	18.05.22 р.	Виконано
9.	Оформлення презентацій	25.05.22 р.	Виконано
10.	Отримання рецензій	01.06.22 р.	Виконано
11.	Захист в ДЕК	16.06.22 р.	Виконано

Студент: СЗД-41 Захарченко К.І. _____
(підпис)

Науковий керівник: к.т.н., доц. Пепа Ю.В. _____
(підпис)

Нормоконтроль: Гребенніков А.Б. _____
(підпис)

РЕФЕРАТ

Дана атестаційна робота присвячена дослідженню методів атак, використовуючи мобільні пристрої працівників корпоративної мережі та розробки рекомендацій для захисту проти даного типу атак. Робота складається зі вступу, списку умовних позначень, 4 розділів, що містять 13 рисунків, висновків та списку використаних джерел, що містить 13 найменувань. Загальний обсяг сторінок 41, а також список використаних джерел.

Об'єктом дослідження в роботі є методи захисту від кібератак з використанням мобільних пристроїв використовуючи доступні інструменти для захисту.

Метою роботи – дослідження вразливостей корпоративних мереж при використанні мобільних пристроїв працівниками та розробка рекомендацій щодо покращення захисту корпорацій. Огляд існуючих загроз і вразливостей операційних платформ, мобільних пристроїв і вибір механізмів захисту інформаційних ресурсів, що зберігаються на мобільних пристроях.

Як результат, у роботі наведені вказівки та рекомендації щодо захисту інформації мобільних користувачів.

Галузь застосування: Матеріали роботи можуть бути використані при створенні рекомендацій та плануванні захисту даних корпоративної мережі при взаємодії з мобільними користувачами.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЗБИТКИ ВІД КІБЕРЗЛОЧИНІВ, ЗАХИСТ МЕРЕЖ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ, ЗАХИСТ МОБІЛЬНИХ ПРИСТРОЇВ, МОБІЛЬНИЙ ПРИСТРІЙ, ЗАГРОЗИ ПЕРСОНАЛЬНИМ ДАНИМ, ВИТІК ІНФОРМАЦІЇ, ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

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

DPL (Data Leak Prevention) – технології запобігання витоку конфіденційної інформації з інформаційної системи назовні, а також технічні пристрої (програмні або програмно-апаратні) для такого запобігання витокам.

MDM (Mobile Device Management) – клас прикладних програмних пакетів управління парком мобільних пристроїв організації.

EMM (Enterprise Mobility Management) – процес управління мобільністю IT-середовища підприємства, що відрізняється високим рівнем безпеки, надійності, потужності.

VPN (Virtual Private Network) – узагальнена назва технологій, що дозволяють забезпечити одне або кілька мережевих з'єднань поверх іншої мережі, наприклад Інтернет.

IMEI (International Mobile Equipment Identity) – серійний номер мобільного пристрою (п'ятнадцятизначне число, тобто 14 цифр коду плюс 15-та контрольна цифра), який встановлюється заводом-виробником та є унікальним для кожного мобільного телефону.

SDK (Software Development Kit) – набір із засобів розробки, утиліт і документації, який дозволяє програмістам створювати прикладні програми за визначеною технологією або для певної платформи (програмної або програмно-апаратної).

WSUS (Windows Server Update Services) – сервіс оновлень для операційних систем і продуктів Microsoft.

SQL (Structured Query Language) – декларативна мова програмування для взаємодії користувача з базами даних, що застосовується для формування запитів, оновлення і керування реляційними БД, створення схеми бази даних та її модифікації, системи контролю за доступом до бази даних.

USMT (USER STATE MIGRATION TOOL) – легка міграція профілів і даних Windows.

WDS (Wireless Distribution System) – технологія, що дозволяє розширити зону покриття бездротової мережі шляхом об'єднання декількох точок доступу Wi-Fi в єдину мережу без необхідності встановлення дротового з'єднання між ними (що є обов'язковим у традиційній схемі побудови мережі).

IIS (Internet Information Services) – це набір серверів для декількох служб Інтернету від компанії Майкрософт. IIS поширюється з операційними системами родини Windows NT.

SLA (Service Level Agreement) – угода між постачальником послуг і користувачем про рівень послуг. Містить кількісні та якісні характеристики наданих послуг, такі як їх доступність, підтримка користувачів, час виправлення несправності та інше.

ВСТУП

Сучасні мобільні пристрої стали невід'ємною частиною нашого життя, але окрім зручності та багатьох технічних можливостей, вони несуть за собою все більшу небезпеку. Для інформації, яка в них зберігається та передається. Швидкість передачі даних у мережах 4G, яка може досягати до 1 Гбіт/с (в 6 разів більше у порівнянні з найшвидшими мережами 3G), а в мережах 5G швидкість передачі даних може досягати до 5 Гбіт/с (в 80 разів більше ніж заявлена максимально можлива швидкість в мережах 3G-операторів України). З використанням високошвидкісних мобільних мереж нового покоління, загрози інформаційної безпеки для державних та приватних установ збільшуються, адже для зловмисників відкриваються більші технічні можливості, оскільки працівники все частіше використовують мобільні пристрої для віддаленої роботи, а не тільки для спілкування.

Сьогодні Bring Your Own Device (BYOD) – це далеко не новий термін в IT-індустрії, але він дуже стрімко привернув до себе увагу на фоні пандемії COVID-19 і швидкого переходу бізнесу в «домашній» режим. Деякі організації вже були підготовлені до непередбачуваного майбутнього – пандемії, заздалегідь прийнявши рішення про дозвіл працювати співробітникам з дому, хоч завжди, якщо вони цього тільки забажають. Це є яскравий приклад того, коли принцип BYOD став частиною щоденної рутини компаній, у даному випадку необхідністю для виживання бізнесу у такий складний час. І як показує практика, кількість користувачів даного підходу з кожним роком лише зростатиме.

Також, під час війни, зі сторони країни агресора значно збільшилась кількість кібератак усіх характерів та кількість дезінформації задля залякування населення України. Прикладом є фіктивний лист про капітуляцію від імені президента.

Тому, наразі базове розуміння правил поведінки, та можливих ризиків є абсолютно необхідне не тільки для захисту персональної інформації, своїх статків, але й також свого, та життя рідних. Зважаючи на територіально-політичну ситуацію у країні та світі, потрібно розуміти що моніторингові системи на підприємстві, навчання персоналу та тренінги з обізнаності у захисті даних є необхідністю задля уникнення витоку інформації, та підтримки контролю потоку інформації на підприємстві, або у персональному житті.

1 ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ КОРИСТУВАЧІВ СУЧАСНИХ МОБІЛЬНИХ ПРИСТРОЇВ ТА ЗАСОБИ ЇХ ЗАХИСТУ

1.1 Статистика

Кожен третій житель України (33%) має смартфон з сенсорним екраном, а серед людей у віці 18-50 років – половина (50%). Порівняно з 2015 роком простежується зростання частки таких людей - з 26% до 33% у випадку загального населення і з 41% до 50% у випадку осіб до 50 років. Якщо серед молоді 65% користуються смартфонами [Додатки (Рис. 1)], то серед осіб літнього віку – 5%. Типовий користувач смартфонів - це молода особа не старше 40 років з вищою освітою, яка проживає у середніх і великих містах України. Більшість (66%) користуються операційною системою Android, а 69% користувачів смартфонів мають досвід встановлення додатків. Найбільш популярними є соціальні мережі (73%), ігри (61%), навігація (51%), месенджери (49%).

Нажаль неуважні, або недосвідчені користувачі мобільних пристроїв встановлюють і зловмисне програмне забезпечення, яке може нанести особисту шкоду, чи принести збитки організації, в якій вони працюють. Зловмисник може отримати доступ до соціальних мереж, особистої та корпоративної пошти, даних платіжних карток, списку контактів, вимагати гроші заблокувавши мобільний пристрій, чи використовувати його для мережевих атак. Враховуючи швидкість передачі даних, його можливості збільшуються в рази.

1.2 Важливість надійного паролю

Небезпеку для інформації несуть і відкриті Wi-Fi мережі, атак кожен має змогу до них підключитись та виконувати необхідні зловмисні дії. Також небезпечними можна вважати і умовно захищені мережі в публічних місцях чи організаціях, до яких можна підключитись прочитавши пароль з чеку чи дізнавшись його у працівника. Дані проблеми захисту інформації в бездротових

мережах є актуальними та поширеними. Ненадійні паролі стають причиною хакерських атак. Після того як зловмисник підключиться до мережі, після проникнення він отримує доступ абсолютно до всіх підключених пристроїв. Крім того, якщо ненадійний або стандартний пароль використовується для панелі налаштувань, то всі пристрої також піддаються ризику хакерської атаки. 30% користувачів використовують в якості пароля слово з топ – 10 000 паролів. Збільшення словника до 10 000 000 дасть приріст всього до 33% всіх паролів. Третина всіх паролів, що використовуються, зламуються шляхом банального перебору варіантів зі словника. Список найбільш часто використовуваних паролів зазнав незначних змін за минулі кілька років. Знання користувачів в області інформаційної безпеки дуже обмежені, значне їх число не збирається приділяти час захисту своїх даних: майже 17% облікових записів були захищені паролем «123456» [Додаток (Рис. 2)].

При цьому паролі розподілені наступним чином:

- 0.5% користувачів використовують в якості пароля *password;*
- 0.4% користувачів використовують в якості пароля password або 123456;
- 0.9% користувачів використовують в якості пароля password, 123456 або 12345678;
- 1.6% користувачів використовують в якості пароля слово з топ 10 паролів;
- 4.4% користувачів використовують в якості пароля слово з топ 100 паролів;
- 9.7% користувачів використовують в якості пароля слово з топ 500 паролів;
- 13.2% користувачів використовують в якості пароля слово з топ 1000 паролів;
- 30% користувачів використовують в якості пароля слово з топ 10 000 паролів.

Застосування таких паролів як «1q2w3e4r» і «123qwe» показує, що деякі користувачі намагаються використовувати непередбачувані поєднання символів для створення захищених паролів, проте їх зусилля як мінімум недостатні. Програми для злому паролів, засновані на словниках, в першу чергу аналізують

такі поширені варіації. У кращому випадку, це збільшить час злому на кілька секунд.

При умові підбору в 10 000 паролів за секунду, якщо за приклад словника паролів взяти перелік можливих мобільних телефонів, при форматі + 380 YY XXX XX XX (YY код регіону або мобільного оператора, де є 16 кодів оператора, або 48 кодів регіонів ті операторів України, XXX XX XX номер телефону), то:

- для перебору мобільних номерів потрібно 4 години 26 хвилин;

- для кодів регіонів та операторів України потрібно вже 13 годин 20 хвилин.

В стійких паролів ситуація зовсім інша. Для комбінації, що можуть складатись з 63 символів у паролі для Wi-Fi мережі, які обираються з множин у 88 знаків, час для їх перебору буде становити більше 19 млрд. років!

Хакерська група, яка раніше інфікувала цілу «армію» пристроїв зі сфери Інтернету речей, цілеспрямовано заразила 3,2 мільйона домашніх Wi-Fi маршрутизаторів за допомогою шкідливого програмного оновлення. Вони встановили сервер, який автоматично підключається до уразливих маршрутизаторів і відправляє інфіковане оновлення. Такий підхід надає їм постійний доступ до пристрою і можливість заблокувати обліковий запис власника, а також відповідні дії інтернет-провайдера і виробника обладнання.

Рівень розкриття кіберзлочинів в Україні становить в середньому 50%, при цьому 80% постраждалим вдається відшкодувати збитки, яких вони зазнали внаслідок дій злочинців. За даними опитування у якому взяли участь 502 експерта в області інформаційної безпеки та IT-фахівців, у найближчі три роки інформаційна безпека матиме найбільший вплив на IT-стратегію компаній.

Основною перешкодою для захисту компаній від кіберзагроз 65,1% вважають дефіцит бюджету, 47% – брак фахівців з IT-безпеки.

Основні загрози інформаційній безпеці організацій [Додаток (Рис. 3)] несуть забезпечення мобільності співробітників (51%) та інтернет речей (20%).

4,2% організацій на сьогодні захищені максимально надійно.

49,7% - фахівців оцінюють захист на три бали з можливих п’яти.

Більше половини опитаних за останній рік мали проблеми з атаками, а саме:

- зараження шкідливим ПЗ - (70,2%);
- спам, фішинг і різні види інтернет-шахрайства (52,5%);
- DOS-атаки (37,4%);
- шпигунські атаки (20%);
- програми-вимагачі (18,5%);
- спрямовані атаки хакерів (15,1%);
- ботнети (12,5%).

Більша кількість компаній виявляють проблему протягом одного дня (37,3%). Протягом години це вдається зробити в 11,5% організацій, близько тижня потрібно для 31,5% фірм. Іншим компаніям потрібно більше часу.

Збиток, нанесений в результаті кібератаки, виражається переважно в збоях системи (58,4%), втрата даних і неавторизований доступ до них також поширені: 25,2% і 14,9% відповідно. Крім того, в результаті дій зловмисників фахівці втрачали час, не могли скористатися необхідним обладнанням, втрачали доступ до зашифрованих зловмисниками даних, несли репутаційні втрати.

В свою чергу, кількість сім-карт на ринку України продовжує зменшуватись, незважаючи на продаж великої кількості смартфонів на дві сім-картки (більше 90%) можна зробити висновок, що користувачі стали більше приділяти увагу економії у використанні ресурсів мережі та більш сумлінно відноситись до можливостей своїх пристроїв.

2 ЗАХИСТ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ НА МОБІЛЬНИХ ПРИСТРОЯХ

2.1 Огляд існуючих загроз і вразливостей операційних платформ мобільних пристроїв

Постановка проблеми: За оцінкою Міжнародного союзу електрозв'язку (ITU) абоненти мобільного зв'язку в світі ростуть набагато швидше, ніж населення. Прогностична модель передбачає, що обсяг світового ринку складе 8,4 млрд. Абонентів при 99,3% заселення до 2025 року (8,2 млрд. У 2019 році, [Додаток (Рис. 4)]). Це свідчить про збільшення мобільних пристроїв, а відповідно і частоти їх застосування для потреб організацій.

До того ж повсюдне використання стратегії *Bring Your Owm Device* у всіх сферах діяльності дозволяє прискорити бізнес-процеси, практично миттєво отримувати актуальну інформацію та спростити комунікацію з колегами. При очевидній зручності використання і мобільності співробітників виникає безліч проблем і ризиків інформаційної безпеки. Що і зумовлює актуальність обраної теми.

За даними дослідження спеціалістів ESET, у 2019 році 68% виявлених вразливостей на Android пристроях були критичними, а 29% з них могли бути використані для завантаження небезпечного коду. Зокрема, увагу дослідників і користувачів привернула уразливість CVE-2019-2107, яка дозволяла зловмисникам відтворювати відео на смартфоні жертви.

Навіть IOS пристрої – еталон надійності і безпеки не позбавлені недоліків. У 2019 році було виявлено на 25% уразливостей більше порівняно з 2018 роком, проте кількість критичних нижча приблизно на 20% порівняно з Android. А отже, основною ціллю кіберзлочинців, як і раніше є пристрої Android.

Аналіз останніх досліджень і публікацій, у яких започатковано розв'язання проблеми захисту корпоративної інформації на мобільних пристроях, показав,

що такі науковці, як Метью Монтгомері, Кевін Курран, Вівіан Мейнс, Деклан Харкін, Нікола Благоєвич та інші, присвятили різним засобам захисту, таким як DPL, MDM, MAM, EMM, VPN багато уваги та часу.

Сучасні мобільні пристрої все менше відрізняються від ПК з позицій зберігання на них корпоративної інформації. Доступ до електронної пошти, корпоративних документів, спеціалізованих сервісів, ділові контакти та календарі, замітки, плани і графік робіт – це і багато іншого може отримати зловмисник, заволодівши таким пристроєм, або отримавши до нього доступ.

Величезним фактором ризику в разі втрати або крадіжки пристрою є неможливість миттєво повідомити відповідальних осіб, або заблокувати доступ до пристрою.

Також, мобільні пристрої в більшій мірі схильні до атак класу «Man-in-the-Middle», тому що змусити підключитися смартфон до «відомої» точки доступу досить легко. Після підключення до точки доступу, в більшості випадків без відома і бажання власника можна здійснювати перехоплення і підміну трафіку, а то й прямо атакувати пристрій (у випадку з Android можна скористатися спеціальними модулями Metasploit Framework).

Також, у разі Android-пристроїв велика ймовірність зараження тієї чи іншої шкідливою програмою. Це обумовлено деякими немало важливими факторами, як світова більшість користувачів, зростаюча кількість вразливостей у системі безпеки даної операційної системи та незахищений магазин додатків, через який є ймовірність скачування небезпечного ПЗ.

У разі рутованих/джейлбрекнутих пристроїв, ризик втрати або крадіжки даних зростає ще вище: це і завантаження програм з невідомих джерел, необмежені і недостатньо контрольовані права, більшість користувачів не читає попереджень і підтверджує практично будь-які запити від додатків.

Найнебезпечнішою є загроза витоку інформації. У 2019 році частка витоку даних через мобільні пристрої зросла на 5% у порівнянні з попереднім періодом.

При цьому 60% подібних інцидентів визнані великими, а інші 40% великими з довгостроковими наслідками.

Якщо ми говоримо про витік інформації, то ймовірними шляхами або причинами несанкціонованого доступу до корпоративної інформаційна мобільних пристроях може бути:

- зберігання незашифрованих даних;
- необґрунтовані дозволи додаткам на використання інформаційних ресурсів;
- унікальний ідентифікатор пристрою IMEI (для Android пристроїв);
- вбудовані датчики;
- тощо.

Особлива увага має приділятися корпоративній інформації у відкритому вигляді на мобільних пристроях, так як зашифрована вже є захищеною і надійність її безпеки залежить лише від стійкості використовуваного криптоалгоритму. На даний час стандартом у сфері криптографії є AES – симетричний алгоритм блочного шифрування. Тож, якщо конфіденційна або важлива робоча інформація зберігаються в телефоні у відкритому вигляді, втрата або крадіжка пристрою можуть дорого обійтися компанії. Багато користувачів просто не усвідомлюють всіх ризиків своєї недбалості, наприклад, віддаючи телефон у ремонт або обмін, чи не зачистивши пам’ять або не вилучивши доступи до аккаунтів.

Дані з незашифрованого телефону можна витягти майже в 100 % випадків. «Майже» тут відноситься скоріше до випадків, коли телефон спробували фізично пошкодити або знищити безпосередньо перед зняттям даних. У багатьох пристроях Android і Windows Phone є сервісний режим, що дозволяє злити всі дані з пам’яті апарату через звичайний USB-кабель. Це стосується більшості пристроїв на платформі Qualcomm (режим HS-USB, який працює навіть тоді, коли завантажувач заблокований), на китайських смартфонах з процесорами

MediaTek, Spreadtrum і Allwinner (якщо розблоковано завантажувач), а також всіх смартфонів виробництва LG.

Якщо мобільний пристрій належить компанії, його простіше і ефективніше захищати використовуючи загальноприйняті світові практики захисту BYOD. У корпоративних мобільних пристроях частка змішування особистих і професійних даних мала, тому деякі обмеження свободи дій користувача виправдані і доцільні. В цьому випадку баланс зміщений в сторону захисту даних, ніж зручності використання, чого не можна сказати про персональні пристрої, які більшою мірою залишаються неконтрольованими.

2.2 Вибір та план механізмів захисту інформаційних ресурсів, що зберігаються на мобільних пристроях

Перш ніж обрати технології забезпечення безпеки, компанії необхідно скласти план впровадження безпеки пристроїв, який може, наприклад, включати в себе такі кроки:

- визначити загрози і елементи ризику використання тієї чи іншої інформації на мобільному пристрої;
- необхідно скласти політику доступу до корпоративних даних поза периметром компанії;
- забезпечити додаткові заходи безпеки хмарного зберігання;
- встановити контроль додатків;
- забезпечення належної парольної політики;
- впровадження і підтримка в актуальному стані засобів захисту;
- реалізувати заходи щодо шифрування даних;
- встановити можливість віддаленого управління пристроєм;
- забезпечити заходи знищення інформації в разі втрати або крадіжки пристрою;

- прийняти заходи щодо утилізації пристрою або повернення у випадку звільнення працівника;

- впровадження адміністративних заходів щодо порушення політики *BYOD.*

Для захисту інформації на мобільних пристроях рекомендовано використовувати ряд таких технічних засобів: DLP-системи для контролю за конфіденційною інформацією, MDM-системи для контролю за самими мобільними пристроями та MAM-системи для контролю за програмними додатками на цих пристроях, або EEM-системи, що поєднують у собі всі попередні функції.

Сьогоденні технології DLP-продуктів використовуються головним чином для захисту інформації від витоків. Технології категоризації інформації складають ядро DLP-систем. Зазвичай на пристрої встановлюється спеціальний агент, який буде моніторити інформацію відповідно до встановлених тегів з рівнем її секретності та активізувати відповідну дію: блокування, аудит і тому подібне.

Завдяки рішенням MAM організації можуть надавати користувачам доступ до каталогу внутрішніх програм і перевірених бізнес-рішень від сторонніх постачальників, потрібних у роботі. На додачу до списку схвалених програм адміністратори також можуть створити чорний список програм, які не задовольняють необхідним критеріям. Заради зручності рішення MAM зазвичай дають адміністраторам змогу оновлювати та навіть вилучати дані віддалено, без прямого доступу до пристроїв. Це чудовий вибір для організацій із великим штатом віддалених співробітників.

Управління мобільними пристроями (MDM) – це тип програмного забезпечення для захисту, що використовується IT-відділом для моніторингу, управління та захисту мобільних пристроїв співробітників (ноутбуків, смартфонів, планшетів тощо), які розгортаються у багатьох постачальників

послуг мобільного зв’язку та на декількох мобільних пристроях [Додаток (Рис. 5)].

MDM-рішення складається з двох частин: контрольного центру і клієнтського програмного забезпечення. Клієнтське програмне забезпечення може включати засоби шифрування, що дозволяють забезпечити конфіденційність робочих даних незалежно від особистої інформації користувача, а також ряд інструментів, призначених для віддаленого моніторингу та управління пристроєм. Серед найпоширеніших функцій віддаленого управління можливість дистанційного видалення даних, установка додатків і оновлень, спливаючі оповіщення і набір інструментів «антизлодій» (що включає відстеження географічного положення пристрою, його блокування та фотографування навколишнього викрадача обстановки).

MDM-системи можуть мати вбудоване антивірусне рішенням, також можуть бути частиною мультиплатформової системи інформаційної безпеки. Рішення з управління мобільними пристроями існують для більшості популярних мобільних платформ (Android, iOS, Windows Phone, Blackberry, Symbian). Однак набір доступних функцій, залежно від операційної системи, може помітно відрізнятися. Це обумовлено відмінностями в ідеології платформ і, як наслідок, в різному рівні доступу до даних для розробників MDM-рішень.

Мобільне управління додатками застосовує функції керування та управління політикою до окремих програм. Ця можливість необхідна, коли операційна система пристрою (наприклад, iOS, Android, Windows Phone) не надає необхідних можливостей управління або коли організації вирішили не встановлювати на пристрої профіль MDM. Існує дві основні форми управління мобільними додатками:

- попередньо налаштовані програми: До них, як правило, належать захищений менеджер персональних даних (PIM) для електронної пошти, календарів та управління контактами, а також захищений браузер, наданий

постачальником послуг з управління мобільними послугами або третьою стороною;

- розширення додатків: Вони застосовують політику до програм за допомогою набору для розробки програмного забезпечення (SDK) або шляхом обгортання. Ця можливість необхідна, коли ОС не надає необхідних можливостей управління або коли організації вирішили не встановлювати агент MDM на пристрій.

Усі перераховані заходи можна застосовувати з використанням систем класу Mobile Device Management (MDM), які дозволяють віддалено (централізовано) управляти безліччю мобільних пристроїв, будь-то пристрою, надані співробітникам компанією або власні пристрої співробітників. Управління мобільними пристроями зазвичай включає в себе такі функції, як віддалений оновлений регламент безпеки (без підключення до корпоративної мережі), поширення додатків і даних, а також управління конфігурацією для забезпечення всіх пристроїв необхідними ресурсами. MDM-рішення - один із засобів реалізації політики ІБ організації і, як будь-який інший інструмент, ефективний за умови використання за призначенням і правильного налаштування.

Однак і це рішення не є панацеєю від усіх загроз – можливість віддаленого управління пристроєм тільки при наявності мережі робить пристрої уразливими до фізичних атак (при відключеному мережі передачі даних або копіювання пам’яті) клонування даних для аналізу в спеціалізованих середовищах або вилучення та можливого дешифрування даних, тому тільки дотримання контролю доступу та складу даних на мобільному пристрої може знизити ризики витоку або крадіжки критичних даних або доступу до них.

Без MDM інформація про викрадені або загублені пристрої не є захищеною, що може дозволити їй легко потрапити в чужі руки. Крім того, пристрої без MDM мають підвищений вплив шкідливих програм та інших вірусів, які можуть порушити конфіденційні дані. І після того, як конфіденційні дані

скомпрометовані, легкість досягнення порушення даних або інциденту злому значно зростає. Події, які можуть назавжди вплинути на репутацію компанії у споживачів та інших ділових партнерів. За даними Novell, ноутбук або планшет викрадають кожні 53 секунди, а 113 стільникових телефонів втрачають або крадуть щохвилини. Оскільки витрати на відновлення після порушення корпоративних даних з кожним роком стають усе дорожчими, все більше підприємств бачать цінність комплексного рішення EMM.

Поточні пакети EMM складаються з інструментів управління політикою та конфігурацією, які поєднані з накладеним накладанням для програм і вмісту, призначеного для мобільних пристроїв, що стосуються ОС смартфонів. IT-організації та провайдери послуг використовують пакети EMM для надання IT-підтримки кінцевим користувачам мобільних пристроїв і підтримки політики безпеки.

Сучасні апартаменти EMM забезпечують такі основні функції:

- інвентар обладнання;
- інвентаризація заявок;
- управління конфігурацією ОС;
- розгортання, оновлення та видалення мобільних додатків;
- конфігурація мобільного додатка та управління політикою;
- віддалений перегляд та управління для усунення неполадок;
- виконування віддалених дій, наприклад, віддалене форматування;
- управління мобільним вмістом.

Мобільні пристрої більшу частину часу підключені до Інтернету, будь-то домашня мережа або загальнодоступна точка доступу Wi-Fi. Якщо не використовувати програму VPN на своєму пристрої iPhone або Android, ви автоматично стаєте привабливою мішенню для кіберзлочинців. Багато важливої корпоративної інформації стає легко доступною для злодіїв даних: повідомлення

в месенджері, конфіденційні електронні листи, дані банківського рахунку та інші дані.

Мобільний VPN подібен до будь-якого іншого типу служби VPN. Він просто пропонує захист пристрою Android або iOS через додаток, який ви можете отримати в Google Play Store та App Store.

Використання VPN гарантує захист даних під час переключення між різними мережами Wi-Fi. Частиною MDM-рішення також виступає VPN з'єднання для доступу до корпоративних ресурсів (Email, Sharepoint, Keynote, Joplin, Office) та контролю трафіка, а також його інспекції. Зі своєї сторони рішення MDM дозволяє спростити доставку сертифікату та налаштувань VPN з'єднання. Якщо компанія вирішить налаштувати VPN вручну, то постане питання, який протокол VPN використовувати. Серед них представлені такі: OpenVPN; L2TP; IPSec.

Одним з найпопулярніших і рекомендованих протоколів, OpenVPN є високозахищеною, легко налаштовуваною платформою з відкритим кодом, яка може використовувати 256-бітове шифрування AES і особливо хороша в обхід брандмауерів. OpenVPN працює на всіх основних операційних системах, включаючи Android та iOS. Однак він не підтримується на жодній платформі, а це означає, що ви повинні додати його на свій мобільний пристрій через сторонній клієнт. L2TP розшифровується як протокол тунелю рівня 2. Сам по собі L2TP – це протокол тунелювання, який не забезпечує жодного шифрування, тому, як правило, він поєднаний із IPSec-шифруванням. Разом цей дует досить простий у налаштуванні та підтримується на багатьох пристроях. Це забезпечує хороший захист, але є певна стурбованість тим, оскільки він використовує один порт (UDP-порт 500), його також легше заблокувати та не так добре обійти брандмауери, як OpenVPN. Крім того, оскільки це двоетапний процес перетворення та шифрування, він не такий швидкий. IPSec також можна використовувати самостійно і він підтримується на пристроях iOS.

3 ПОЛІТИКА ВІДОМИХ КОМПАНІЙ ЩОДО ЗАХИСТУ ТА БЕЗПЕКИ КОРПОРАТИВНИХ ДАНИХ

3.1 Захист корпоративних даних від компанії «Apple»

Підприємства повсюдно розширюють можливості своїх співробітників за допомогою iPhone та iPad. Ключем до успішної мобільної стратегії є баланс між IT-контролем та можливостями користувачів. Персоналізуючи пристрої iOS своїми власними програмами та контентом, користувачі беруть на себе більше відповідальності, що призводить до підвищення рівня залученості та підвищення продуктивності. Цьому сприяє система управління Apple, яка забезпечує інтелектуальні способи управління корпоративними даними та додатками роздільне управління корпоративними даними та додатками, плавно відокремлюючи робочі дані від особистих. Крім того, користувачі розуміють, як управляються їх пристрої, і впевнені, що їх конфіденційність захищена.

iOS Deployment Reference, всеосяжний онлайновий технічний довідник з розгортання та управління пристроями iOS. Довідник з розгортання та управління пристроями iOS на вашому підприємстві.

За допомогою iOS ви можете спростити оптимізацію iPhone та iPad, використовуючи ряд інструментів. Вбудовані методи, які дозволяють спростити налаштування облікового запису, налаштувати політику, розповсюджувати програми та дистанційно застосовувати обмеження щодо пристроїв.

Завдяки уніфікованій структурі керування Apple в iOS, macOS, tvOS, IT можуть налаштовувати та оновлювати параметри, розгортати програми, стежити за відповідністю, а також віддалено стирати чи блокувати пристрої. Фреймворк підтримує корпоративні та користувацькі пристрої, а також особисті пристрої. Apple – уніфікована структура управління в iOS є основою для керування мобільними пристроями. Ця структура вбудована в iOS, що дозволяє організаціям керувати чим вони повинні. В результаті уніфікована структура

управління Apple в iOS забезпечує детальний контроль за допомогою стороннього керування мобільними пристроями (MDM) рішення ваших пристроїв, програм і даних. І найголовніше, ви отримуєте контроль, який вам потрібен, не погіршуючи користувацький досвід і не завдаючи шкоди конфіденційності ваших співробітників. Інші методи керування пристроями на ринку можуть використовувати різні назви, описувати функціональні можливості MDM, наприклад керування корпоративною мобільністю (EMM) або управління мобільними додатками (MAM). Ці рішення мають ту саму мету - для керування пристроями та корпоративними даними вашої організації по повітрю. А оскільки структура керування Apple вбудована в iOS, вам не потрібно окрему програму агента від вашого постачальника рішень MDM.

Керований вміст охоплює встановлення, налаштування, керування та видалення App Store і спеціальних внутрішніх програм, облікових записів, книг і доменів.

Керовані програми. Програми, встановлені за допомогою MDM, називаються керованими програмами. Вони можуть бути безкоштовні або платні у App Store. Програми можна встановити по повітрю за допомогою MDM. Керовані програми часто містять конфіденційні дані інформації та забезпечують більше контролю, ніж програми, завантажені користувачем. Сервер MDM може видаляти керовані програми та пов’язані з ними дані на вимогу, або вкажіть, чи потрібно видаляти програми, коли профіль MDM видалено. Крім того, сервер MDM може запобігти передачі даних керованих програм завдяки резервному копіюванню в iTunes та iCloud;

Керовані облікові записи. MDM може допомогти вашим користувачам швидко почати роботу автоматично налаштувати свої поштові та інші облікові записи. Залежно від MDM постачальник рішень та інтеграція з вашими внутрішніми системами, корисними навантаженнями облікового запису, також можна попередньо заповнити ім’я користувача, адресу електронної пошти та де

застосовується, ідентифікатори сертифікатів для аутентифікації та підпису. MDM може налаштувати такі типи облікових записів: IMAP/POP, CalDAV, Календарі, CardDAV, Exchange ActiveSync і LDAP;

Керовані книги. Використовуючи MDM, можна використовувати книги, книги ePub та документи PDF автоматично переміщуватися на пристрої користувачів, тому співробітники завжди мають те, що вони їм потрібно. Керованими книгами можна ділитися лише з іншими керованими програмами або надсилати поштою. За допомогою керованих облікових записів. Коли матеріали більше не потрібні, їх можна видалити дистанційно;

Керовані домени. Завантаження з Safari вважаються керованими документами, якщо вони виходять із керованого домену. Визначені URL-адреси та піддомени можуть бути керованими. Наприклад, якщо користувач завантажує PDF-файл з керованого домену, домен вимагає, щоб PDF відповідав усім параметрам керованого документа. Шляхи, що йдуть за доменом, керуються за замовчуванням.

Кероване поширення дозволяє використовувати рішення MDM або Apple Configurator 2 для керування програмами та книгами, придбаними в Apple Business Manager. Щоб увімкнути кероване розповсюдження, необхідно спочатку зв'язати ваше MDM-рішення з обліковим записом Apple Business Manager за допомогою захищеного маркера. Після того як ваш MDM сервер підключений до Apple Business Manager, призначайте програми безпосередньо на пристрій без необхідності наявності у користувача Apple ID. Користувач отримує запит, коли програми готові до встановлення на пристрій. Якщо пристрій перебуває під наглядом, програми будуть установлені без попередження користувача [Додаток (Рис. 6)].

При керованій конфігурації програм MDM використовує вбудовану структуру керування iOS для настроювання програм під час або після розгортання. Ця структура дозволяє розробникам визначити параметри

конфігурації, які мають бути коли їхня програма встановлюється як керована програма. Співробітники можуть розпочати використовувати програми, які були налаштовані таким чином, відразу ж, не вимагаючи індивідуального налаштування. ІТ-відділ отримує впевненість у тому, що корпоративні дані у додатках обробляються безпечно, без необхідності використання власних SDK або обгортання програм.

Розробникам програм доступні можливості, які можна увімкнути за допомогою керованої конфігурації програми, наприклад, для запобігання резервному копіюванню програми, вимкнення захоплення екрана та віддалене стирання програми.

Спільнота AppConfig зосереджена на наданні інструментів та кращих практик для використання нативних можливостей мобільних операційних системах. Постачальники MDM-рішень із цієї спільноти створили стандартну схему, яку можуть використовувати всі розробники додатків. Розробники можуть використовувати підтримку керованої конфігурації додатків. Забезпечуючи більш послідовний, відкритий та простий спосіб конфігурування та забезпечення безпеки мобільних додатків. Спільнота допомагає підвищити рівень впровадження мобільних програм у бізнесі.

MDM-рішення надають спеціальні функції, які дозволяють керувати корпоративними даними керувати на гранулярному рівні, щоб вони не просочувалися в особисті програми користувачів та хмарні послуги, додатків та хмарним сервісам [Додаток (Рис. 7)].

Керований Open In. Управління Open In використовує набір обмежень, які запобігають відкриття вкладень або документів із керованих джерел у некерованих місцях призначення, і навпаки.

Наприклад, ви можете запобігти відкриття конфіденційного вкладення електронної пошти у вашій, можна заборонити відкривати конфіденційне вкладення електронної пошти в керованому поштовому обліковому записі

організації в особистих програмах користувачів. Тільки програми, встановлені та керовані MDM, можуть відкрити цей документ. Некеровані особисті програми користувача не відображаються у списку програм, доступних для відкриття вкладення.

Розширення додатків надають стороннім розробникам можливість надавати функціональність іншим програмам або навіть ключовим системам, вбудованим в iOS, таким як Центр повідомлень, забезпечуючи нові робочі процеси між програмами. Використання керованих Open In запобігає некерованій функціональності розширень від взаємодіяти з керованими програмами. У наступних прикладах показані різні типи розширень:

Розширення Document Provider дозволяють програмам для підвищення продуктивності відкривати документи із різних хмарних служб без необхідності робити непотрібні копії;

Розширення дій дозволяє користувачам маніпулювати вмістом або переглядати його в контексті іншої програми. Наприклад, користувачі можуть використовувати дію для перекладу тексту з іншої мови прямо у Safari;

Розширення Custom Keyboard надають клавіатури крім тих, що вже вбудованих в iOS. Відкритий вхід, що управляється, може запобігти появі неавторизованих клавіатур у ваших корпоративних додатках;

Розширення Today, також відомі як віджети, використовуються для надання зручної для перегляду інформації в поданні "Сьогодні" в Центрі повідомлень. Це стає чудовим способом для користувачів отримати негайну, актуальну інформацію з програми, зі спрощеною взаємодією, яка дозволяє перейти до повної програми для отримання додаткової інформації.

Розширення Share надають користувачам зручний спосіб поділитися вмістом з іншими наприклад, із веб-сайтами соціального обміну або службами завантаження. Наприклад, у програмі, в якій є кнопка "Поділитися", користувачі можуть вибрати розширення "Поділитися". Яке представляє веб-сайт

соціального обміну, а потім використовувати його для публікації коментаря або іншого контенту.

Уніфікована система управління Apple в iOS є гнучкою та пропонує збалансований підхід до управління як користувачами, так і пристроями на вашому підприємстві. Якщо ви використовуєте MDM-рішення стороннього виробника разом з iOS, ваші можливості керування пристроями знаходяться на континуумі, який варіюється від застосування відкритої методології до максимально деталізованого керування.

При розгортанні пристроїв, що належать користувачам, iOS пропонує персоналізоване налаштування та прозорість налаштування пристроїв, а також гарантію того, що особисті дані користувачів не будуть доступні вашій організації [Додаток (Рис. 8)].

Реєстрація за бажанням та без нього. Коли пристрої купуються та налаштовуються, зазвичай це називається BYOD – ви можете надати доступ до корпоративних сервісів, таких як Wi-Fi, пошта та календар. Користувачі просто вибирають зареєструватися в MDM-рішенні вашої організації. Коли користувачі реєструються в MDM вперше на пристрої iOS, їм надається інформація про те, до чого сервер MDM може отримати доступ на їх пристрої. MDM-сервер може отримати доступ до їх пристроїв та функцій, які він налаштовуватиме. Це забезпечує прозорість для користувачів щодо того, що знаходиться під керуванням, та встановлює довіру між вами та користувачами. Важливо дати користувачам зрозуміти, що якщо будь-якої миті їх не влаштує таке управління, вони можуть відмовитися від нього. Видаливши профіль керування зі свого пристрою. Після цього всі корпоративні облікові записи та програми, встановлені MDM, будуть видалені.

Після того, як користувачі зареєстровані в MDM, співробітники можуть легко переглядати в Налаштуваннях, які програми, книги та облікові записи знаходяться під керуванням та які обмеження було введено. Усі корпоративні

налаштування, облікові записи та контент, встановлені за допомогою MDM, позначаються iOS як "керовані" [Додаток (Рис. 9)].

Конфіденційність користувачів. Хоча сервер MDM дозволяє взаємодіяти з пристроями iOS, не всі установки та інформація про обліковий запис відкриті. Ви можете керувати корпоративними обліковими записами, налаштуваннями та інформацією, наданою через MDM, але особисті облікові записи користувачів недоступні. Фактично, ті ж функції, які забезпечують безпеку даних у програмах, керованих корпорацією, також захищають особистий контент користувача від влучення в корпоративний потік даних.

Персоналізація пристроїв. Підприємства виявили, що надання користувачам можливості персоналізувати пристрій за допомогою власного Apple ID призводить до підвищення рівня відповідальності серед користувачів, а їх продуктивність підвищується тому що тепер вони можуть вибирати програми та контент, які їм необхідні для найкращого виконання своєї роботи.

При використанні Apple Business Manager ваше MDM-рішення автоматично налаштує ваші iOS-пристрою під час роботи помічника з налаштування [Додаток (Рис. 10)].

Apple Business Manager дозволяє автоматизувати реєстрацію MDM під час початкового налаштування пристроїв iPhone та iPad та Mac-системи, якими володіє ваша організація. Ви можете зробити реєстрацію обов'язковою. Ви також можете перевести пристрої в контрольований режим під час процесу реєстрації та дозволити користувачам пропустити деякі кроки налаштування.

Контрольовані пристрої. Нагляд надає додаткові можливості керування пристроями iOS, що належать до вашої організації. До них відноситься можливість увімкнути веб-фільтр через глобальний проксі-сервер, щоб переконатися, що веб-трафік користувачів не виходить за межі правил організації. Заборонити користувачам скидати налаштування пристрою до заводських налаштувань за замовчуванням та багато іншого. За замовчуванням усі пристрої

iOS не контролюються. Використовуйте Apple Business Manager, щоб увімкнути контрольований режим автоматично, або використовуйте Apple Configurator 2, щоб увімкнути режим спостереження вручну.

Навіть якщо ви не плануєте використовувати будь-які функції під наглядом зараз, подумайте, щоб контролювати свої пристрої при їх налаштуванні, що дозволить вам скористатися перевагами функціями лише під наглядом у майбутньому. В іншому випадку вам доведеться обнулювати пристрої які вже були розгорнуті. Нагляд – це не блокування пристрою. Можливості керування. У довгостроковій перспективі контроль надає ще більші можливості для вашого підприємства.

З iOS 9.3 або пізнішої версії ваше MDM-рішення може перевести контрольований пристрій у режим "Втрата". Ця дія блокує пристрій та дозволяє відобразити повідомлення з номером телефону на екрані блокування. За допомогою режиму Lost Mode можна визначити місцезнаходження втрачених або вкрадених контрольованих пристроїв, оскільки MDM віддалено запитує їхнє розташування в останній раз, коли вони були в мережі. Режим Lost Mode не вимагає увімкнення функції Find My iPhone. Якщо MDM віддалено відключає режим Lost Mode, пристрій розблокується та його розташування буде відоме. Для підтримки прозорості користувач повідомляє про те, що режим Lost Mode вимкнено [Додаток (Рис. 11)].

Блокування активації в iOS 7.1 або пізнішій версії використовуйте MDM для блокування активації, коли користувач включає Find My iPhone на контрольованому пристрої. Це дозволить вашій організації скористатися функціональністю блокування активації як засіб захисту від крадіжки, але водночас дозволить вам обійти цю функцію, якщо, наприклад, користувач залишає вашу організацію без попереднього зняття блокування активації за допомогою Apple ID.

Ваше рішення MDM може отримати код обходу та дозволити користувачеві увімкнути Activation Lock на пристрої на підставі наступного:

- якщо функція Find My iPhone увімкнена, коли ваше рішення MDM дозволяє Activation Lock, Activation Lock включається у цей момент;

- якщо Find My iPhone вимкнено, коли ваше рішення MDM дозволяє Activation Lock, Activation Lock включається наступного разу, коли користувач активує Find My iPhone.

3.2 Захист корпоративних даних від компанії «Microsoft»

Компанія Microsoft використовує для захисту корпоративних даних на мобільних пристроях такі програми, як Configuration Manager та Windows Intune.

Configuration Manager. Починаючи з версії 1910, Configuration Manager тепер є частиною Microsoft Endpoint Manager.

Microsoft Endpoint Manager – це інтегроване рішення для керування всіма вашими пристроями. Microsoft об'єднує Configuration Manager та Intune без складної міграції та зі спрощеним ліцензуванням. Продовжуйте використовувати існуючі інвестиції в Configuration Manager, одночасно використовуючи переваги хмари Microsoft у зручному для вас темпі.

Наступні рішення Microsoft для управління тепер є частиною торгової марки Microsoft Endpoint Manager:

- менеджер конфігурації;
- Intune;
- аналітика робочого столу;
- автопілот;
- інші функції в консолі адміністрування керування пристроями.

Configuration Manager був створений для того, щоб допомогти вам у наступних діях з управління системами:

- підвищити продуктивність та ефективність IT, скоротивши кількість виконуваних вручну операцій та дозволивши вам зосередитись на важливих проектах;

- максимізувати інвестиції в обладнання та програмне забезпечення;

- підвищити продуктивність користувачів, надаючи потрібне програмне забезпечення у потрібний час.

Configuration Manager допомагає вам надавати ефективніші IT-послуги, дозволяючи:

- безпечне та масштабоване розгортання програм, оновлень програмного забезпечення та операційних систем;

- події у режимі реального часу на керованих пристроях;

- хмарна аналітика та управління для локальних та інтернет-пристроїв;

- управління налаштуваннями відповідності;

- комплексне управління серверами, настільними комп'ютерами та ноутбуками.

Configuration Manager розширюється і працює разом з багатьма технологіями та рішеннями Microsoft. Наприклад, Configuration Manager інтегрується з:

- Microsoft Intune для спільного керування широким спектром платформ мобільних пристроїв;

- Microsoft Azure для розміщення хмарних служб для розширення ваших служб керування;

- служби оновлень Windows Server (WSUS) для керування оновленнями програмного забезпечення;

- служби сертифікації;

- Exchange Server та Exchange Online;

- групова політика;

- DNS;

- пакет автоматичного розгортання Windows (Windows ADK) та засіб міграції користувача середовища (USMT);

- служби розгортання Windows (WDS);

- віддалений робочий стіл та віддалена допомога.

Configuration Manager також використовує:

1. Доменні служби Active Directory та Azure Active Directory для забезпечення безпеки, визначення розташування служб, налаштування та виявлення користувачів та пристроїв, якими ви хочете керувати;

2. Microsoft SQL Server як розподілена база даних керування змінами - і інтегрується зі службами звітів SQL Server (SSRS) для створення звітів для моніторингу та відстеження дій з управління;

3. Ролі системи сайту, які розширюють функціональні можливості керування та використовують веб-служби інформаційних служб Інтернету (IIS);

4. Оптимізація доставки, Windows Low Extra Delay Background Transport (LEDBAT), Background Intelligent Transfer Service (BITS), BranchCache та інші технології однорангового кешування, які допомагають керувати контентом у ваших мережах та між пристроями.

Щоб успішно використовувати Configuration Manager у виробничому середовищі, потрібно ретельно спланувати та протестити функції керування. Configuration Manager – це потужна програма для керування, яка може впливати на кожен комп'ютер у організації. Коли розгортаєте та керуєте Configuration Manager з ретельним плануванням та обліком ваших бізнес-вимог, Configuration Manager може скоротити адміністративні витрати та загальну вартість володіння.

Windows Intune – інтегроване, засноване на хмарі рішення для керування клієнтами, яке містить засоби, звіти та ліцензії на оновлення до найновіших версій Windows, а також забезпечує захист та оновлення комп'ютерів. Крім того, за допомогою Windows Intune можна керувати мобільними пристроями всередині вашої мережі, за допомогою Exchange ActiveSync або безпосередньо, за

допомогою Windows Intune. Пряме керування за допомогою Windows Intune відкриває розвинені можливості керування пристроями iOS, Windows RT та Windows Phone 8.

Інтегроване рішення для управління оновленнями, моніторингу, отримання сповіщень та формування звітності:

- Windows Intune забезпечує моніторинг стану, антивірусний захист, запити на віддалене обслуговування, інвентаризацію та звіти щодо використання ліцензій. Рішення "все в одному" для забезпечення контролю відразу всіх "гарячих" точок;

- адміністратори можуть отримувати сповіщення та надавати віддалену допомогу безпосередньо з консолі Windows Intune;

- простий web-інтерфейс для вирішення повсякденних завдань обслуговування:

- панель адміністратора Windows Intune проста для освоєння і розроблена так, щоб IT-адміністратори могли швидко визначити завдання та пріоритет проблем, які можуть вплинути на продуктивність;

- спрощує управління IT системами, виділяючи лише суттєві події та повідомлення. Адміністратори можуть легко отримати доступ до додаткових даних або налаштувати повідомлення так, щоб отримати більш детальну інформацію.

Гнучке управління та звітність:

- дозволяє IT менеджерам помістити один ПК у кілька адміністративних груп (наприклад, «Відділ продажів» або «Ноутбуки»). Це дозволить правильно застосовувати, керувати та відслідковувати активи та відповідність IT політиці компанії;

- фільтри дозволяють адміністраторам генерувати огляди та звіти та експортувати дані безпосередньо з панелі адміністрування.

Microsoft повністю володіє інфраструктурою обслуговування Windows Intune, гарантує надійність та безпеку обслуговування, та надає клієнтам єдину точку звернення службу підтримки лідера у наданні надійних послуг у глобальних масштабах:

- Windows Intune створений з нуля як надійний хмарний сервіс, що добре масштабується;

- Microsoft має понад 15 років досвіду у створенні найбільших web-сервісів, включаючи інфраструктуру Windows Update, на якій базуються технології апдейтів усіх операційних систем Windows у світі;

- надаються фінансові гарантії працездатності служби 99.9% часу, зафіксовані в угоді про рівень обслуговування (SLA);

- забезпечує технічну підтримку сервісу та вирішення проблем у режимі 24×7 для користувачів Windows Intune в Україні українською мовою.

3.3 Захист корпоративних даних від компанії «Google»

Програма Google Apps Device Policy забезпечує дотримання політик безпеки організації на керованих співробітниками пристроях Android, захищаючи їх та підвищуючи їхню безпеку. Якщо політика безпеки порушена, особливо важливо переконатися, що корпоративні дані недоступні на цьому пристрої, доки він знову не буде відповідати вимогам [Додаток (Рис. 12 та Рис. 13)].

Маючи це на увазі, програма Device Policy тепер буде відключати доступ до некритичних програм на будь-якому робочому профілі або корпоративному пристрої Android, який визначає як невідповідний. Користувачі побачать повідомлення про те, що їхній пристрій порушив політику безпеки, і деякі програми можуть бути відключені. Ці програми будуть повторно увімкнені, коли їх пристрій буде відповідати всім політикам безпеки організації.

Некритичні програми – це будь-які програми, які не потрібні для роботи пристрою. Наприклад, номеронабирач - це критичне додаток, а Gmail – некритичне додаток.

4 ОСОБИСТІ РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ ПРИ ВЗАЄМОДІЇ З МОБІЛЬНИМИ КОРИСТУВАЧАМИ

Минули часи, коли найконфіденційнішою інформацією в телефоні співробітника були контактні імена та номери телефонів. Тепер за допомогою смартфона або планшета можна отримати доступ до всього: від електронної пошти до збережених паролів та особистих даних компанії та комерційної таємниці. З появою технології 5G, що спрощує та прискорює доступність, все більше і більше компаній готові прийняти мобільні технології як звичайну частину бізнесу.

Залежно від того, як організація використовує такі пристрої, несанкціонований доступ до смартфону, планшета або іншого пристрою може призвести до катастрофічного кібер-інциденту, що стосується всієї IT-інфраструктури організації. Незважаючи на важливість реалізації заходів кібербезпеки в цілому, такі заходи допоможуть уникнути проблем з безпекою мобільних пристроїв, зокрема, та забезпечити безпеку ваших даних.

1. Встановіть політику безпеки мобільних пристроїв.

Перш ніж видати співробітникам смартфони або планшети, потрібно встановити політику використання пристроїв. Надати чіткі правила про те, що є допустимим використанням. Вказати, які дії будуть вжиті, якщо працівники порушать політику. Важливо, щоб співробітники розуміли ризики безпеки, пов'язані з використанням смартфонів, та заходи безпеки, які вони можуть зробити для зниження цих ризиків. Добре поінформовані та відповідальні користувачі – ваша перша лінія захисту від кібератак.

2. Встановіть політику використання власних пристроїв.

Якщо компанія дозволяє співробітникам використовувати свої особисті пристрої для роботи компанії, потрібно переконатися, що є офіційна політика

використання власних пристроїв (BYOD). План безпеки BYOD також має включати:

1. Вимоги до встановлення програмного забезпечення для віддаленого очищення на будь-які персональні пристрої, що використовуються для зберігання даних компанії або доступу до них;

2. Навчання та навчання співробітників, як захистити дані компанії при доступі до бездротових мереж зі своїх мобільних телефонів та пристроїв;

3. Методи захисту даних, які включають вимогу надійних паролів та автоматичне блокування після періодів бездіяльності;

4. Протоколи для повідомлення про втрачені або вкрадені пристрої;

5. Використання певного антивірусного та захисного програмного забезпечення безпеки;

6. Вимоги до регулярного резервного копіювання;

7. Затверджений список для тих, хто хоче завантажити програми.

Оновлення програмного забезпечення для мобільних пристроїв часто містять виправлення для різних дірок у системі безпеки, які можуть бути відкритими дверима для мобільних шкідливих програм та інших загроз безпеці. Тому рекомендується встановлювати оновлення одразу.

Коли справа доходить до антивірусного програмного забезпечення для мобільних пристроїв, є багато варіантів на вибір, і все залежить від переваг. Деякі з них можна використовувати безкоштовно в магазині додатків, в той час як інші стягують щомісячну або щорічну платню і часто мають найкращу підтримку.

На додаток до антивірусної підтримки, багато з цих програм будуть відстежувати тексти служби коротких повідомлень (SMS), службу мультимедійних повідомлень (MMS) та журнали викликів на предмет підозрілої активності. Вони можуть використовувати чорні списки, щоб користувачі не могли встановлювати відомі шкідливі програми на пристрої.

3. Резервне копіювання вмісту пристрою на регулярній основі.

Систематизовано робити резервні копії даних на мобільних пристроях компанії. Якщо пристрій втрачено або викрадено, можна бути спокійним, знаючи, що цінні дані в безпеці та їх можна відновити.

4. Ретельно вибирайте паролі.

У США середня адреса електронної пошти пов'язана зі 130 обліковими записами в Інтернеті. Ці цифри вражаючі, але середній інтернет-користувач повторно використовує кілька паролів, щоб захистити їх усі. Очевидно, що хакери розраховують на відсутність обізнаності про безпеку для крадіжки даних. Скористайтеся наведеними нижче порадами, щоб паролі мобільних пристроїв було легко запам'ятати і було важко вгадати.

Вимагати від співробітників змінювати пароль для входу на пристрій не рідше одного разу на 90 днів. Впровадити двофакторну автентифікацію для підтвердження особи користувача. Паролі повинні складатися не менше ніж з восьми символів і включати великі та малі літери, цифри та спеціальні символи, такі як зірочки, знаки оклику.

Не використовуйте у паролі прості послідовності цифр, такі як «12345», або імена подружжя, дітей або домашніх тварин. Хакер може витратити лише кілька хвилин на сайт соціальної мережі, щоб з'ясувати цю інформацію.

Завдяки своїй зручності смартфони та планшети стали невід'ємною частиною сучасного ділового світу. У міру зростання використання стає все більш важливим вживати заходів для захисту вашої компанії та її конфіденційних даних від мобільних загроз, як нових, так і старих.

Зрештою, навіть за наявності найкращих рішень для забезпечення безпеки ніколи не буває 100% гарантії. Важливо захистити компанію від ризиків відповідальності, пов'язаних з кібератакою, через мобільний пристрій співробітника або сервер вашої компанії. Поговоріть сьогодні з консультантом зі стратегічних ризиків у McClone, щоб оцінити свій ризик та запропонувати додаткові рішення.

ВИСНОВКИ

Інформаційна безпека не несе за собою можливості заробітку, оскільки потребує певних витрат, але завдяки цим витратам можливо захистити установи від значних майбутніх збитків.

Враховуючи розвиток та поширення сучасних мобільних пристроїв, зростання їх апаратних можливостей, а також швидкості передачі даних в мережах мобільного зв'язку, для більш ефективного захисту треба бути уважнішим, використовувати перевірене програмне забезпечення, різні паролі для облікових записів, блокування пристрою (пін-код, пароль, тощо), віддалене управління на випадок втрати.

Необізнаність користувачів та адміністраторів мереж, що призводить до великої ймовірності перехоплення інформації вирішується навчанням правилам інформаційної безпеки. Ймовірність перехоплення інформації можна зменшити шляхом використання засобів захисту в повному обсязі, але проблема відсутності коректного налаштування може залишатись, через використання нестійких паролів.

Використовуючи спеціалізоване програмно-апаратне забезпечення є можливість підвищити рівень захисту мереж від зловмисних дій, а правильне налаштування та відповідальне використання особистої техніки допоможе ефективно та безпечно використовувати можливості сучасних мобільних пристроїв.

Таким чином важливо поєднувати зусилля в підвищенні обізнаності користувачів фахівцями у галузі інформаційної безпеки, виробниками мобільних пристроїв, провайдерами послуг та технічного забезпечення, адже більшість користувачів, нажаль навіть не замислюється над можливістю того, що їх пристрої можуть піддаватись загрозам.

Мобільні пристрої все більше розповсюджені у світі, тому критично важливо захистити дані на всіх етапах їхнього використання. Завдяки різноманітним заходам безпеки працівники зможуть працювати, де та коли захотять, практично з будь-якого пристрою. Щоб захист був максимальний, рішення для захисту мобільних даних зазвичай можна поєднувати. Наприклад, керуючи мобільними пристроями та програмами на них, організації можуть застосовувати захист і в хмарі, і в локальному середовищі. Корпоративні дані будуть у безпеці, незалежно від географічного розташування співробітників.

ПЕРЕЛІК ПОСИЛАНЬ

1. Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах / А.В. Платоненко. Матеріали Науково-технічної конференції «Світ телекомунікації та інформатизації». – ДУТ. – 2015 р.

2. Сучасні загрози інформаційної безпеки для державних та приватних установ України / А.В. Платоненко // Сучасний захист інформації. – 2015. – № 4, С.86-90.

3. Некоторые интересные факты о подборе паролей [Електронний ресурс] - Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=153530

4. Опубликованы наиболее часто используемые пароли 2016 года [Електронний ресурс] - Режим доступу: http://lead9.com/slide/slide.pdf

5. Hacker Claims To Push Malicious Firmware Update to 3.2 Million Home Routers [Електронний ресурс] - Режим доступу: https://motherboard.vice.com/en_us/article/hacker-claims-to-push-malicious-firmware-update-to-32-million-home-routers

6. Cisco исследовала основные тенденции в сфере информационной безопасности на украинском рынке [Електронний ресурс] - Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=153526

7. Украинцы постепенно отказываются от лишних SIM-карт [Електронний ресурс] - Режим доступу: http://itc.ua/news/ukraintsyi-postepenno-otkazyivayutsya-ot-lishnih-sim-kart

8. Mobile Phone Market Forecast - 2019 [Електронний ресурс] – Режим доступу: https://stats.areppim.com/stats/stats_mobilex2019.htm

9. Аналіз безпеки мобільних пристроїв: підсумки першого півріччя 2019 [Електронний ресурс] - Режим доступу: https://eset.ua/ua/news/view/717/analiz-bezopasnosti-mobilnykh-ustroystv-itogi-pervogo-polugodiya-2019

10. Захист корпоративної інформації від витоку через мобільні пристрої [Електронний ресурс] - Режим доступу: https://licenziya-fsb.com/utechka-mobilnye-ustroistva

11. Афонін О. Android і шифрування даних. Про те як все погано, і навряд чи стане краще [Електронний ресурс] - Режим доступу: https://xakep.ru/2016/05/02/android-encryption/

12. What is Mobile Device Management (MDM)? [Електронний ресурс] - Режим доступу: https://www.continuum.net/resources/mspedia/everything-to-know-about-mobile-device-management-mdm

13. Empey C. Why and how to set up a VPN on your iPhone or Android [Електронний ресурс] - Режим доступу: https://blog.avast.com/using-mobile-vpn-on-iphone-or-android

ДОДАТКИ

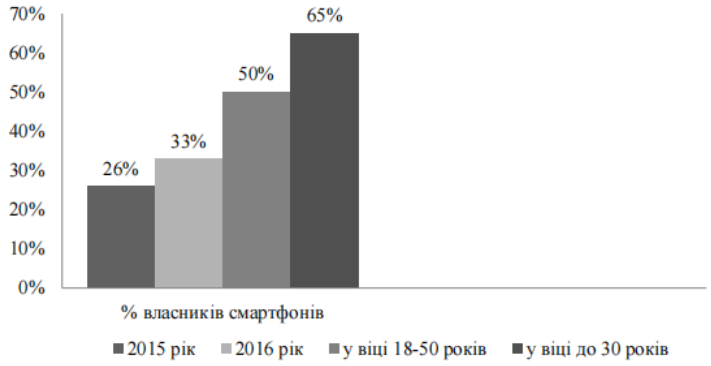

Рисунок 1 – Кількість власників смартфонів серед жителів України

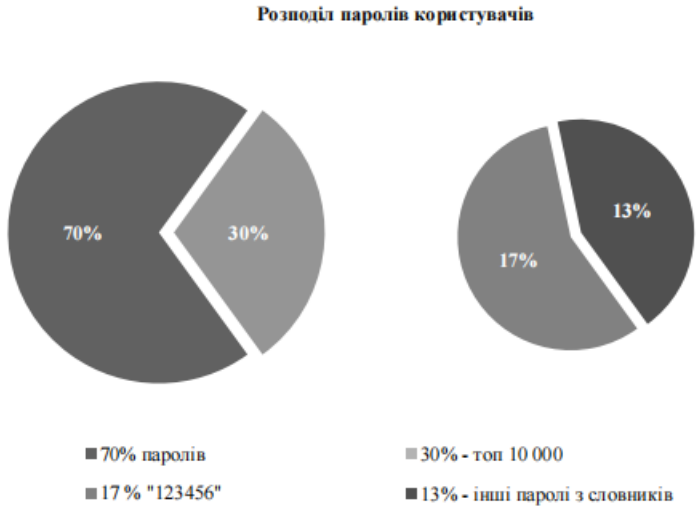

Рисунок 2 – Розподіл паролів користувачів

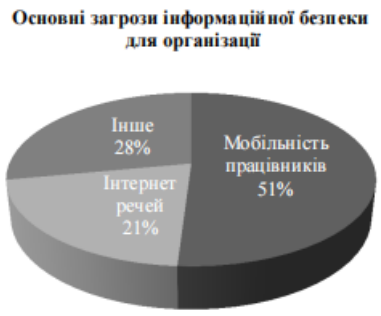

Рисунок 3 – Основні загрози інформаційної безпеки для організацій

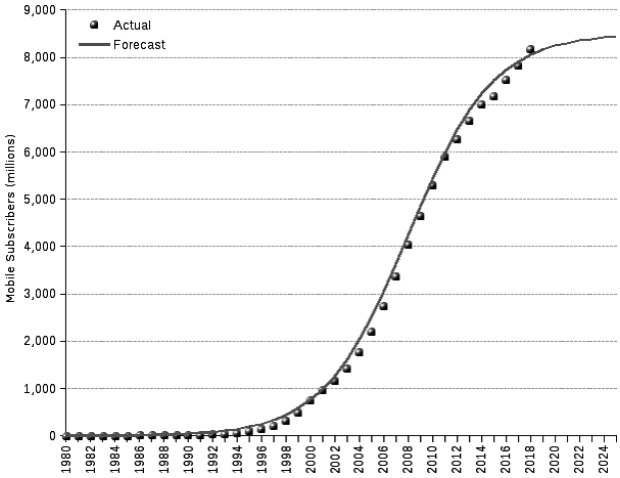

Рисунок 4 – Прогноз ринку мобільних телефонів ITU станом на 2019 рік

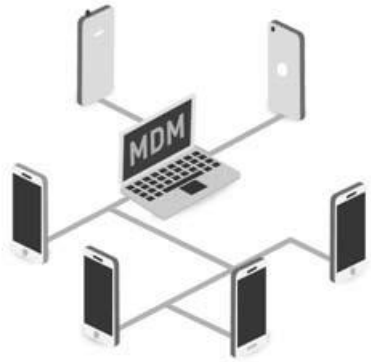

Рисунок 5 – MDM-рішення

Рисунок 6 – Щоб зберегти повний контроль над програмами за допомогою рішення MDM, завантажуйте програми безпосередньо на пристрій

Рисунок 7 – Щоб захистити корпоративні дані, лише програми, встановлені та керовані MDM, можуть відкрити цей робочий документ

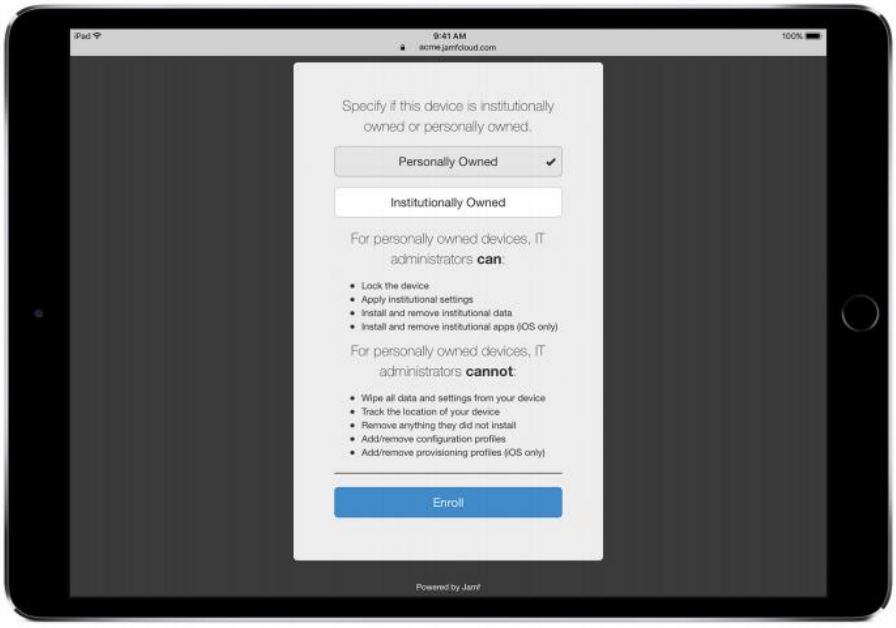

Рисунок 8 – Сторонні MDM-рішення, як правило, пропонують зручний інтерфейс для співробітників, так щоб вони відчували себе комфортно під час реєстрації

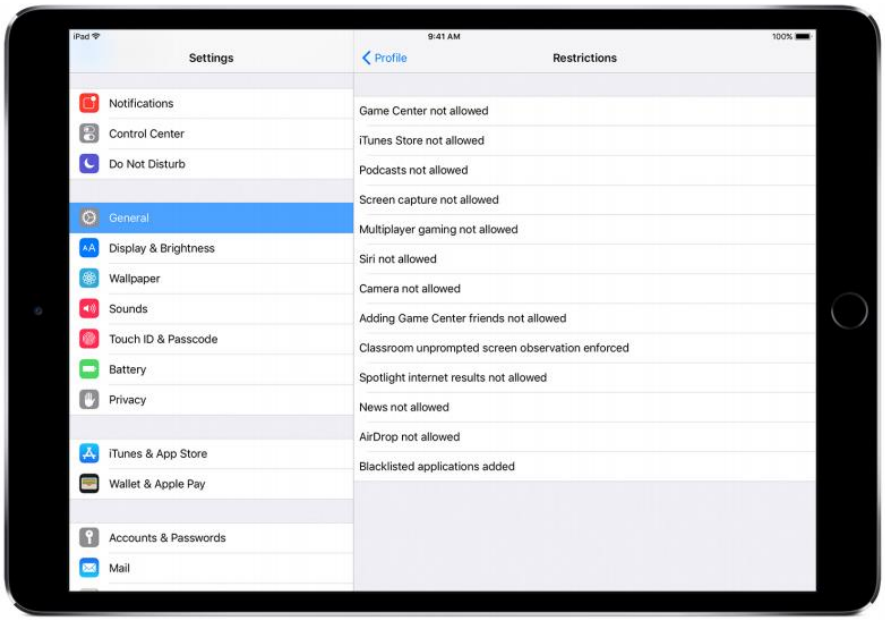

Рисунок 9 – Інтерфейс користувача для профілів конфігурації в налаштуваннях показує користувачам, що саме було налаштовано на їхньому пристрої

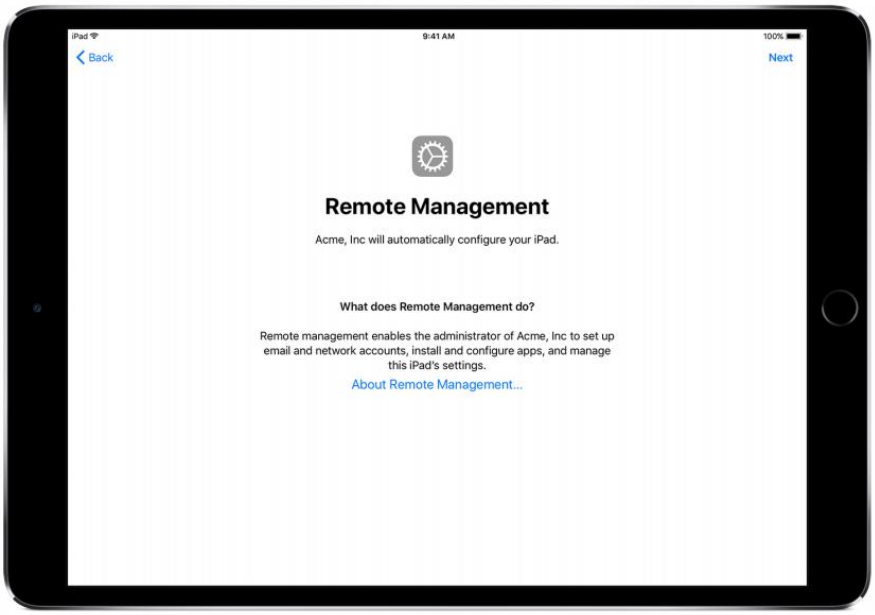

Рисунок 10 – При використанні Apple Business Manager ваше MDM-рішення автоматично налаштує ваші iOS-пристрою під час роботи помічника з налаштування

Рисунок 11 – Коли MDM переводить зниклий пристрій режим Lost Mode, він блокує пристрій та дозволяє повідомленням відображається на екрані визначаючи його розташування

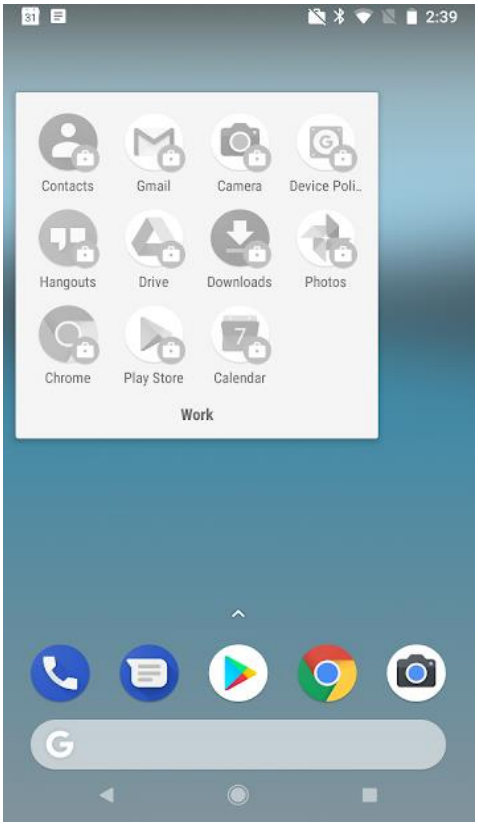

Рисунок 12 – Зовнішній вигляд заблокованих додатків через Google Workspace

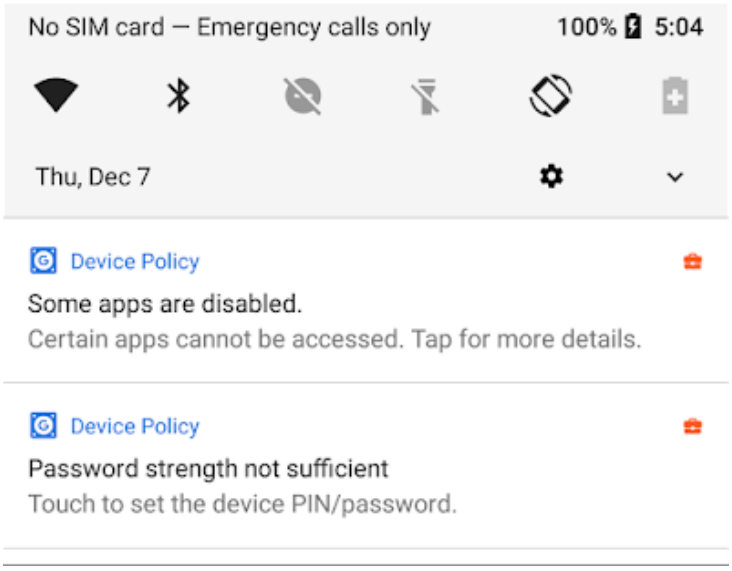

Рисунок. 13 – Зовнішній вигляд заблокованих додатків через Google Workspace