МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ ПІДПРИЄМСТВА: ЗАГРОЗИ ТА МЕТОДИ ПРОТИДІЇ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Василь КОРЖИК

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Василь КОРЖИК

Керівник:
к. держ. упр., доц Тетяна МУЖАНОВА

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УІКБ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Коржику Василю Васильовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ ПІДПРИЄМСТВА: ЗАГРОЗИ ТА МЕТОДИ ПРОТИДІЇ "

керівник кваліфікаційної роботи Тетяна МУЖАНОВА, к. держ. упр., доц.
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. № 145.
2. Строк подання кваліфікаційної роботи "18" грудня 2023 р.
3. Вихідні дані до кваліфікаційної роботи: безпека мобільних пристроїв підприємства, загрози і вразливості безпеці мобільних пристроїв, технології безпеки мобільних пристроїв, життєвий цикл мобільних пристроїв.
4. Перелік питань, які потрібно розробити:
   1. Встановити виклики, загрози і вразливості безпеки мобільних пристроїв.
   2. Проаналізувати технології мобільної безпеки, в тому числі технології управління й безпеки пристрою та технології мобільної безпеки підприємства.
   3. Дослідити засади розгортання й управління мобільними пристроями відповідно до їх життєвого циклу.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури.	23.10.2023	
3.	Вивчення викликів, загроз і вразливостей безпеки мобільних пристроїв.	27.10.2023	
4.	Аналіз технологій мобільної безпеки.	10.11.2023	
5.	Дослідження засад розгортання й управління мобільними пристроями відповідно до їх життєвого циклу.	15.11.2023	
6.	Формулювання висновків за результатами проведеного дослідження.	22.11.2023	
7.	Оформлення роботи.	04.12.2023	
8.	Оформлення презентації.	14.12.2023	
9.	Отримання рецензії на роботу.	18.12.2023	
10.	Захист в ДЕК.	17.01.2024	

Здобувач вищої освіти _____ Василь КОРЖИК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Коржик В.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ ПІДПРИЄМСТВА: ЗАГРОЗИ ТА МЕТОДИ ПРОТИДІЇ"
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **КОРЖИК Василь** у кваліфікаційній роботі встановив виклики, загрози і вразливості безпеки мобільних пристроїв; проаналізував технології мобільної безпеки, в тому числі технології управління й безпеки пристрою та технології мобільної безпеки підприємства; дослідив засади розгортання й управління мобільними пристроями відповідно до їх життєвого циклу. **КОРЖИК Василь** показав розуміння проблеми дослідження і вміння самостійно знаходити шляхи її вирішення, проявив хорошу теоретичну і практичну підготовку, а також володіння англійською мовою професійного спрямування, про що свідчить список використаних джерел. Результати дослідження апробовані на конференції "Актуальні проблеми кібербезпеки" 2023 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **КОРЖИКА Василя** на оцінку "відмінно" та присвоїти йому кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Коржик В.В. допускається дозахисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедрою
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

Здобувача вищої освіти Коржика Василя Васильовича
На тему: УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ ПІДПРИЄМСТВА: ЗАГРОЗИ ТА МЕТОДИ ПРОТИДІЇ

Актуальність: Широке впровадження мобільних технологій у бізнес-діяльність поряд з багатьма перевагами, серед яких оптимізація процесу прийняття рішень, підвищення продуктивності і забезпечення ситуаційної обізнаності, створює унікальні загрози для підприємства, пов'язані з обробкою, зберіганням і передаванням конфіденційних даних, постійним підключенням до Інтернету, недооцінюванням критичної важливості мобільної безпеки для бізнесу, а також недостанім досвідом впровадження заходів мобільної безпеки.

У зв'язку з цим дослідження загроз та методів забезпечення безпеки мобільних пристроїв підприємства є актуальним науковим завданням.

Позитивні сторони. У кваліфікаційній роботі встановлено виклики, загрози і вразливості безпеки мобільних пристроїв на сучасному етапі; проаналізовано технології мобільної безпеки, в тому числі технології управління й безпеки пристрою та технології мобільної безпеки підприємства; досліджено засади розгортання й управління мобільними пристроями відповідно до їх життєвого циклу.

Робота оформлена відповідно до вимог. Структура роботи забезпечує досягнення поставленої мети. Кваліфікаційна робота засвідчила розуміння студентом проблеми, володіння методами дослідження та здатність вирішувати прикладні завдання, відмінне знання англійської мови.

За результатами дослідження надано рекомендації щодо розгортання й управління мобільними пристроями відповідно до їх життєвого циклу.

Недоліки

1. Доцільно було б навести більше прикладів практичного використання технологій мобільної безпеки, в тому числі з урахуванням вітчизняної специфіки.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на високому науково-методичному рівні, заслуговує оцінки «відмінно» і рекомендується до захисту, а здобувач Коржик Василь Васильович заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Рецензент: професор кафедри
інформаційної та кібернетичної
безпеки,
д.т.н, професор _____ Галина ГАЙДУР
підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 93 стор., 14 рис., 2 табл., 61 джерело.

Метою роботи є дослідження загроз та методів забезпечення безпеки мобільних пристроїв підприємства.

Об'єктом дослідження є забезпечення безпеки мобільних пристроїв підприємства.

Предмет дослідження - загрози та методи забезпечення безпеки мобільних пристроїв підприємства.

Методи дослідження. Для вирішення завдань дослідження використовувалися методи аналізу та синтезу, узагальнення, порівняння, класифікації, моделювання, методи комплексного підходу й теорії управління мобільною безпекою.

Короткий зміст роботи. Як результат у роботі встановлено виклики, загрози і вразливості безпеки мобільних пристроїв на сучасному етапі; проаналізовано технології мобільної безпеки, в тому числі технології управління й безпеки пристрою та технології мобільної безпеки підприємства; досліджено засади розгортання й управління мобільними пристроями відповідно до їх життєвого циклу, який охоплює такі етапи: визначення вимог до мобільних пристроїв; здійснення оцінювання ризиків; впровадження корпоративної стратегії мобільної безпеки; експлуатація і підтримка функціонування, утилізація та/або повторне використання мобільних пристроїв.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи заходів з управління мобільною безпекою підприємства, в тому числі з урахуванням життєвого циклу мобільних пристроїв.

КЛЮЧОВІ СЛОВА: БЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ ПІДПРИЄМСТВА, ЗАГРОЗИ І ВРАЗЛИВОСТІ БЕЗПЕЦІ МОБІЛЬНИХ ПРИСТРОЇВ, ТЕХНОЛОГІЇ БЕЗПЕКИ МОБІЛЬНИХ ПРИСТРОЇВ, ЖИТТЄВИЙ ЦИКЛ МОБІЛЬНИХ ПРИСТРОЇВ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 93 pages, 14 figures, 2 tables, 61 sources.

The purpose of the work is to study threats and methods of ensuring the enterprise`s security of mobile devices.

Object of research is the enterprise`s security of the mobile devices.

Subjec*t *of research is the threats and methods of the enterprise`s security of mobile devices.

Research methods Methods of analysis and synthesis, generalization, comparison, classification, modeling, methods of comprehensive approach and theory of mobile security used to solve research problems.

Brief content of research. As a result, the work identifies challenges and threats to the security of mobile devices at the current stage, analyzes the mobile security technologies, including device-side management and security technologies and enterprise mobile security technologies, learns the basics of deploying and managing mobile devices according to their life cycle, which includes the following stages: definition of requirements for mobile devices; carrying out risk assessment; implementation of a corporate mobile security strategy; operation and maintenance of operation, disposal and/or reuse of mobile devices.

Field of research. The developed approaches can be used in the planning and implementing the system of measures for managing the enterprise's mobile security, including taking into account the life cycle of mobile devices.

KEYWORDS: ENTERPRISE MOBILE DEVICE SECURITY, MOBILE DEVICE SECURITY THREATS, MOBILE DEVICE SECURITY TECHNOLOGIES, MOBILE DEVICE LIFE CYCLE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

API	Application Programming Interface
BYOD	Bring Your Own Device
COPE	Corporate-Owned Personal Enabled
COTS	Commercial Off-The-Shelf
CVSS	Common Vulnerability Scoring System
CYOD	Choose Your Own Device
EDR	Endpoint Detection and Response
EMM	Enterprise Mobility Management
GDPR	General Data Protection Regulation
MAM	Mobile Application Management
MAV	Mobile Application Vetting
MCDF	Mobile Computing Decision Framework
MDM	Mobile Device Management
MTD	Mobile Threat Defence
MTP	Mobile Threat Protection
PIV	Personal Identity Verification
SaaS	Software as a Service
SDK	Software Development Kit
SoC	System-on-a-Chip
TLS	Transport Layer Security
TPM	Trusted Platform Module
UEM	Unified Endpoint Management
VDI	Virtual Desktop Infrastructure
VMI	Virtual Mobile Infrastructure
VPN	Virtual Private Networks

ВСТУП

Актуальність теми. Сучасні компанії у процесі своєї діяльності широко використовують мобільні технології, які вже досить давно вийшли за рамки надання можливостей телефонного зв'язку, а є повноцінними обчислювальними платформами. Використання мобільних пристроїв і додатків у бізнес-діяльності сприяє оптимізації процесу прийняття рішень, підвищенню продуктивності персоналу і забезпечує ситуаційну обізнаність.

Водночас мобільні пристрої створюють унікальні загрози для особи і підприємства, пов'язані з обробкою, зберіганням і передаванням конфіденційних даних. У міру того, як споживачі й організації все більше використовують мобільні технології для виконання виробничих і управлінських завдань, змінюється ландшафт мобільних загроз. Так, мобільні пристрої є ідеальною мішенню для хакерів, адже вони постійно підключені до Інтернету, часто використовуються в громадських місцях, де легко отримати до них доступ.

Однак, як свідчать опитування, більшість компаній не до кінця усвідомлюють критичну важливість мобільної безпеки для бізнесу, а також не володіють повною інформацією про належне впровадження комплексу заходів управління й захисту мобільних пристроїв, програм, даних і доступу до них.

З огляду на зазначене дослідження загроз та методів забезпечення безпеки мобільних пристроїв підприємства є актуальним науковим завданням.

Мета і завдання дослідження. **Мета роботи** полягає у дослідженні загроз та методів забезпечення безпеки мобільних пристроїв підприємства.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Встановити виклики, загрози і вразливості безпеки мобільних пристроїв.

2. Проаналізувати технології мобільної безпеки, в тому числі технології управління й безпеки пристрою та технології мобільної безпеки підприємства.

3. Дослідити засади розгортання й управління мобільними пристроями відповідно до їх життєвого циклу.

Об’єкт дослідження - забезпечення безпеки мобільних пристроїв підприємства.

Предмет дослідження – загрози та методи забезпечення безпеки мобільних пристроїв підприємства.

Методи дослідження. Для вирішення завдань дослідження використовувалися методи аналізу та синтезу, узагальнення, порівняння, класифікації, моделювання, методи комплексного підходу й теорії управління мобільною безпекою.

Наукова новизна одержаних результатів. У роботі досліджені комплексні підходи до управління й захисту мобільних пристроїв відповідно до їх життєвого циклу, а також представлений ґрунтовний аналіз передових технологій мобільної безпеки, в результаті впровадження яких буде підвищена ефективність управління й захисту мобільного середовища підприємства.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити обґрунтований вибір заходів і технологій управління й забезпечення безпеки мобільного середовища підприємства відповідно до кращих світових зразків.

РОЗДІЛ 1
БЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ: ВИКЛИКИ, ЗАГРОЗИ, ВРАЗЛИВОСТІ

1.1 Виклики безпеці мобільних пристроїв

Сучасні мобільні пристрої, які, по суті, вже впродовж десятиліть є обчислювальними платформами загального призначення, здатними виконувати завдання, що виходять за рамки можливостей телефонного зв’язку перших поколінь, широко поширені в сучасних корпоративних мережах.

Мобільність змінила спосіб і форми надання корпоративних послуг у сфері IT. Однак, мобільні пристрої, які були розроблені для надання споживачам особистого доступу до комунікацій, інформації та послуг, мають відповідати більш високим вимогам для використання в бізнесі.

Використання мобільних пристроїв і мобільних додатків для отримання доступу до послуг, додатків і даних у будь-який час і будь-якому місці сприяє підвищенню продуктивності персоналу і покращує процес прийняття рішень і ситуаційну обізнаність.

Водночас ці пристрої створюють унікальні загрози для особи і підприємства, оскільки у ході виконання щоденних корпоративних завдань вони регулярно обробляють, зберігають і передають конфіденційні дані. З огляду на портативність, невеликі розміри та звичайне використання поза мережею компанії мобільні пристрої часто є вразливішими для загроз, ніж інші кінцеві пристрої.

У міру того, як споживачі й підприємства все більше сприймають і використовують мобільні технології, змінюється ландшафт мобільних загроз. Це включає збільшення мобільного зловмисного ПЗ і вразливостей пристрою (наприклад, операційну систему, мікропрограму, процесор базової смуги, який

використовується для доступу до стільникових мереж), мобільних програм, мережі й інфраструктури управління [1].

Варто згадати ще кілька чинників, які сприяють вразливості мобільних пристроїв. Мобільні пристрої є ідеальною мішенню для хакерів, адже вони постійно підключені до Інтернету, часто використовуються в громадських місцях, де до них легко отримати доступ, зберігають велику кількість конфіденційних даних про своїх користувачів.

Недостатня обізнаність громадян з питань безпеки мобільних пристроїв, нерозуміння різниці між конфіденційністю даних і безпекою, незнання і недотримання мінімальних вимог щодо безпечного використання мобільних пристроїв роблять їх не просто мішенню для хакерів, але й легкою здобиччю.

Нарешті, інструменти злому стають легшими для доступу в Інтернеті й використовуються для створення більш досконалого шкідливого ПЗ і реалізації більш витончених загроз мобільним пристроям, які важче виявити, а також важче захиститися [2].

Різноманітність і складність мобільної екосистеми та швидкі темпи змін ускладнюють вибір, інтеграцію й управління мобільними технологіями в корпоративних IT-середовищах. Щоб зменшити ризики для конфіденційних даних і систем, компаніям необхідно запроваджувати комплекс різноманітних заходів для управління та захисту мобільних пристроїв, програм, даних і доступу до них.

Мобільна безпека (безпека мобільних пристроїв) є галуззю кібербезпеки, яка має на меті захист мобільних пристроїв від загроз несанкціонованого доступу, використання чи модифікації.

У процесі забезпечення безпеки мобільних пристроїв треба враховувати декілька аспектів (Рис. 1.1):

Безпека пристрою: захист самого пристрою від крадіжки та використання для доступу до інформації власника.

Безпека даних: захист даних, що зберігаються на пристрої, будь то особисті, фінансові чи пов’язані з роботою.

Рис. 1.1. Аспекти безпеки мобільних пристроїв

Безпека програм: захист програм, встановлених на пристрої, від зловмисного програмного забезпечення та інших загроз.

Безпека мережі: захист пристрою, коли він підключений до мережі, наприклад стільникової або Wi-Fi мережі [2].

Тим не менше, більшість компаній не до кінця усвідомлюють критичну важливість мобільної безпеки для бізнесу. Так, результати дослідження Verizon's Mobile Security Index 2020 [3] показали, що компанії часто жертвують безпекою мобільних пристроїв заради більшої швидкості (62%), більшої зручності (52%) або можливості отримати більшу прибутковість (46%). І лише 13% підприємств запровадили регулярну перевірку безпеки, шифрування даних, доступ за потребою та відмовилися від паролів за замовчуванням у масштабах компанії.

За підсумками цьогорічного дослідження Verizon's Mobile Security Index зроблено висновок, що політика використання власного пристрою (BYOD), гібридна робота та поширення Інтернету речей (IoT) збільшили масштаби і складність захисту мобільних пристроїв. Встановлено, що більше третини (34%) мобільних користувачів здійснили одну з п'яти основних помилок безпеки:

- перехід за фішинговим посиланням (18%)
- завантаження шкідливих програм зі smish (SMS-фішинг) (13%)
- завантаження шкідливих програм (11%)
- передача особистої інформації шахраю (9%)
- передача пароля ненадійному джерелу (8%) [4].

1.2 Вразливості безпеки корпоративної мобільності

Мобільні пристрої підтримують низку завдань безпеки, які тим не менше можуть відрізнятися залежно від компанії. Цілі мобільної безпеки можна досягти за допомогою комбінації функцій безпеки, вбудованих у мобільні пристрої, встановлених на них або керованих зовні. Досягнення цілей безпеки підприємства часто вимагає, щоб пристрої були захищені від різноманітних загроз.

Мобільні пристрої, як правило, повинні підтримувати кілька цілей безпеки. Це можна досягти за допомогою поєднання функцій безпеки, вбудованих у мобільні пристрої, і додаткових елементів керування безпекою, застосованих до мобільних пристроїв та інших компонентів IT-інфраструктури підприємства. Традиційними цілями безпеки для мобільних пристроїв є:

– конфіденційність - передані та збережені дані не можуть бути прочитані неавторизованими сторонами;

– цілісність – передані і збережені дані не можуть бути навмисно чи ненавмисно змінені;

– доступність – тільки авторизовані користувачі можуть отримати доступ до даних за допомогою мобільних пристроїв, коли це необхідно [5].

Як відзначено вище, мобільні пристрої часто потребують додаткового захисту, оскільки за своєю природою вони зазвичай більше схильні до загроз, ніж інші кінцеві пристрої (наприклад, настільні та портативні пристрої, які використовуються лише на об’єктах та в мережах підприємства).

Перед розробкою та розгортанням рішень для мобільних пристроїв компанії повинні розробити моделі системних загроз для мобільних пристроїв і ресурсів, доступ до яких здійснюється через мобільні пристрої. Моделювання загроз передбачає ідентифікацію ресурсів і можливих загроз, вразливостей і заходів безпеки, пов’язаних із цими ресурсами, потім кількісну оцінку

ймовірності успішних атак та їхніх наслідків і, нарешті, аналіз цієї інформації, щоб визначити, де заходи безпеки потрібно вдосконалити або додати.

Для початку розглянемо основні вразливості безпеки мобільних технологій, перелік яких представлено у NIST SP 800-124r2 [6] (Рис. 1.2).

Варто наголосити, розглядаючи основні категорії вразливостей мобільної безпеки і пропонуючи підходи до їх пом'якшення, автори публікації дотримуються принципу, відповідно до якого будь-яким пристрою, програмі чи мережі не можна довіряти, якщо немає абсолютної впевненості в їх надійності.

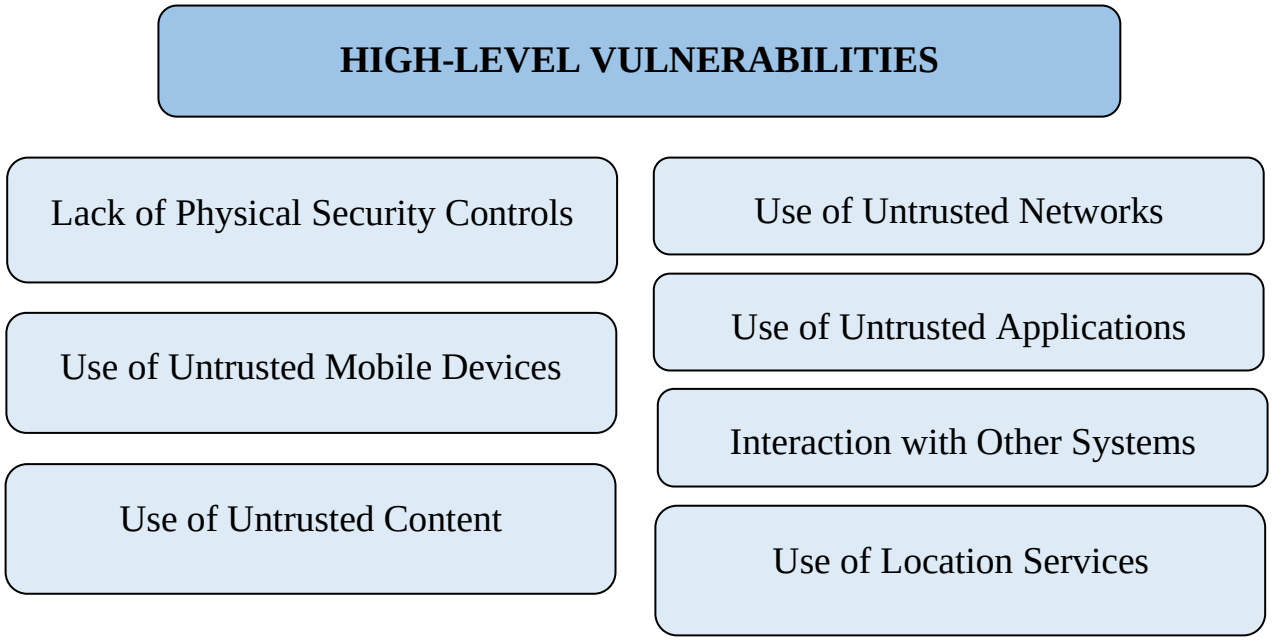

Рис. 1.2. Вразливості безпеки мобільних технологій

Відсутність засобів контролю фізичної безпеки. Мобільні пристрої зазвичай використовуються в різних місцях, які не контролюються підприємством, наприклад за місцем проживання працівників, у кафе, готелях і на конференціях. Навіть мобільні пристрої, які використовуються лише на об'єктах компанії, часто переміщують з місця на місце в межах об'єктів. Власне мобільна природа пристроїв значно підвищує ймовірність їх втрати або викрадення у порівнянні з іншими пристроями. Тому мобільні дані піддаються підвищеному ризику зламу.

Плануючи політику безпеки мобільних пристроїв і засоби контролю, організації повинні припускати, що зловмисники отримають мобільні пристрої і намагатимуться відновити конфіденційні дані безпосередньо з самих пристроїв

або опосередковано, використати їх для доступу до віддалених ресурсів компанії.

Стратегія пом'якшення такої ситуації є багаторівневою. Перший рівень включає вимогу автентифікації перед отриманням доступу до мобільного пристрою або ресурсів компанії, доступних через пристрій. Оскільки у більшості випадків мобільний пристрій має лише одного користувача, у нього є один автентифікатор, а не окремий обліковий запис. Отже, немає імені користувача, лише пароль, яким часто є PIN-код. Більш надійні форми автентифікації, такі як автентифікація на основі маркерів, автентифікація мережевих пристроїв і автентифікація домену, використовують замість вбудованих можливостей автентифікації пристрою або додатково до них.

Другий рівень пом’якшення передбачає захист конфіденційних даних, тобто шифрування сховища мобільного пристрою, щоб конфіденційні дані не могли бути відновлені з нього неавторизованими сторонами, або заборону зберігання конфіденційних даних на мобільних пристроях. Навіть якщо мобільний пристрій завжди знаходиться у володінні його власника, існують інші ризики для фізичної безпеки, наприклад, зловмисник заглядає через плече дистанційного працівника в кафе і переглядає конфіденційні дані на екрані мобільного пристрою (наприклад, введення паролю).

Нарешті, ще один рівень пом’якшення включає навчання і формування обізнаності користувачів, щоб вони розуміли сутність і загрози небезпечного поводження з пристроєм на рівні фізичної безпеки [6].

Використання ненадійних мобільних пристроїв. Багато мобільних пристроїв, особливо ті, які є особистою власністю працівника («Принесіть свій власний пристрій», Bring Your Own Device, BYOD), не завжди є надійними. Загалом BYOD - це політика, яка дозволяє працівникам компанії використовувати свої особисті пристрої для виконання завдань, пов’язаних із роботою. Ці дії можуть включати доступ до електронної пошти, підключення до корпоративної мережі та доступ до корпоративних програм і даних [7].

У більшості сучасних мобільних пристроїв відсутні основні функції довіри (наприклад, надійні модулі платформи, Trusted Platform Module, TPM), які все частіше вбудовуються в ноутбуки, виконують криптографічні операції, включаючи генерацію ключів, і захищають невеликі обсяги конфіденційної інформації, такої як паролі та криптографічні ключі [8].

Також часто відбувається зламування мобільних пристроїв (джейлбрейк (Jailbreak) або рутинг (Rooting), що означає, що вбудовані обмеження щодо безпеки, використання операційної системи тощо були обійдені. Тому організаціям слід припускати, що всі мобільні пристрої є ненадійними, якщо вони незахищені належним чином і не перебувають під її постійним контролем у процесі використання корпоративних програм або даних.

Існує кілька можливих стратегій запобігання використанню ненадійних мобільних пристроїв. Одним із варіантів є обмеження або заборона використання пристроїв BYOD, таким чином віддаючи перевагу пристроям, виданим підприємством. Інший ефективний метод полягає в тому, щоб повністю захистити кожен мобільний пристрій, виданий компанією; завдяки цьому мобільний пристрій переходить у максимально надійний стан, а відхилення від цього безпечного стану компанія може відстежувати й усувати.

Існують також технічні рішення для досягнення рівня довіри до пристроїв BYOD, наприклад запуск корпоративного ПЗ в захищеній ізольованій пісочниці / захищеному контейнері на мобільному пристрої або використання програм сканування цілісності пристрою. Пісочниця (Sandbox) – система, яка дозволяє ненадійній програмі працювати в строго контрольованому середовищі, де дозволи програми обмежені основним набором дозволів комп’ютера. Зокрема, програмі в пісочниці зазвичай забороняється доступ до файлової системи або мережі [8].

Використання ненадійних мереж. Оскільки для доступу в Інтернет мобільні пристрої переважно використовують некорпоративні мережі, підприємства зазвичай не контролюють безпеку зовнішніх мереж, якими користуються пристрої. Системи зв’язку можуть включати бездротові (Wi-Fi) і

стільникові мережі. Ці системи зв’язку є вразливими до прослуховування, що ставить передану конфіденційну інформацію під загрозу компрометації. Атаки типу «Man-in-the-Middle» (MitM) також можуть застосовуватися для перехоплення та модифікації комунікацій [9].

Якщо немає абсолютної впевненості, що мобільний пристрій буде використаний лише в надійних мережах, підконтрольних підприємству, необхідно планувати безпеку мобільного пристрою, виходячи з того, що мережі між мобільним пристроєм і компанією не можна довіряти. Крім того, бувають випадки, коли один мобільний пристрій підтримує кілька облікових записів користувачів, що створює додаткові загрози його безпеці.

Ризик від використання ненадійних мереж можна зменшити за допомогою надійних технологій шифрування (таких як віртуальні приватні мережі, VPN) для захисту конфіденційності й цілісності зв’язку, а також за допомогою механізмів взаємної автентифікації для перевірки ідентичності обох кінцевих точок перед передачею даних.

Іншим можливим засобом пом’якшення є заборона використання незахищених мереж Wi-Fi, наприклад тих, які використовують відомі вразливі протоколи. Крім того, усі мережеві інтерфейси, які не потрібні пристрою, можна відключити, таким чином зменшуючи поверхню атаки.

Використання ненадійних програм. Мобільні пристрої створені для полегшення пошуку, придбання, встановлення та використання програм сторонніх розробників із магазинів програм для мобільних пристроїв. Це створює очевидні ризики безпеці, особливо для платформ мобільних пристроїв і магазинів програм, які не встановлюють обмежень безпеки чи інших обмежень на вивантаження сторонніх програм. Компанії повинні планувати безпеку своїх мобільних пристроїв, враховуючи, що додаткам для мобільних пристроїв третіх сторін, які завантажують користувачі, не можна довіряти.

Ризик від цих програм можна зменшити кількома способами, наприклад,

– заборонити будь-яке встановлення програм сторонніх розробників,

– запровадити білий список, щоб дозволити встановлення лише схвалених програм,

– перевірити, чи програми отримують лише необхідні дозволи на мобільному пристрої, або

– запровадити безпечне пісочне програмне середовище/захищений контейнер, який ізолює дані й програми компанії від усіх інших даних і програм на мобільному пристрої.

Іншим можливим засобом пом’якшення є проведення оцінки ризиків для кожної програми третьої сторони перед тим, як дозволити її використання на мобільних пристроях підприємства.

Важливо відзначити, що навіть якщо ці стратегії пом’якшення реалізовано для програм сторонніх розробників, користувачі все одно зможуть отримати доступ до ненадійних веб-програм через браузери, вбудовані в їхні мобільні пристрої. Ризики, пов’язані з цим, можна зменшити, заборонивши або обмеживши доступ браузера; примусово направивши трафік мобільного пристрою через безпечні веб-шлюзи, проксі-сервери HTTP або інші проміжні пристрої для оцінки URL-адрес, перш ніж дозволити з ними зв’язатися; або використовуючи окремий браузер у безпечному ізольованому програмному середовищі/захищеному контейнері для всіх спроб доступу через браузер, пов’язаних з компанією, залишаючи вбудований браузер мобільного пристрою для інших цілей [6].

Взаємодія з іншими системами. Мобільні пристрої можуть взаємодіяти з іншими системами з точки зору обміну даними (включаючи синхронізацію) і зберігання. Взаємодія з локальною системою зазвичай передбачає бездротове підключення мобільного пристрою до настільного комп’ютера, ноутбука або за допомогою кабелю для синхронізації. Це також може передбачати використання модема, наприклад використання одного мобільного пристрою для надання доступу до мережі для іншого мобільного пристрою.

Віддалена взаємодія з системою найчастіше передбачає автоматичне резервне копіювання даних у хмарному сховищі. Коли всі ці компоненти

знаходяться під контролем підприємства, ризик, як правило, є прийнятним, але часто один або кілька з цих компонентів є зовнішніми. Приклади включають підключення особистого мобільного пристрою до ноутбука, виданого компанією, підключення мобільного пристрою, виданого компанією, до персонального ноутбука, підключення корпоративного мобільного пристрою до служби віддаленого резервного копіювання та підключення будь-якого мобільного пристрою до ненадійної зарядної станції. У всіх цих сценаріях дані компанії ризикують зберігати в незахищеному місці поза її контролем; також можлива передача зловмисного ПЗ з пристрою на пристрій. Є також побоювання щодо мобільних пристроїв, які обмінюються даними між собою.

Стратегії пом'якшення залежать від типу прикріплення. Запобігання синхронізації мобільного пристрою, виданого компанією, з особистим комп’ютером, потребує заходів безпеки на мобільному пристрої, які обмежують перелік пристроїв, з яким він може синхронізуватися.

Запобігання синхронізації особистого мобільного пристрою з комп’ютером, виданим підприємством, потребує засобів контролю безпеки на корпоративному комп’ютері, що обмежує підключення мобільних пристроїв.

Запобігти використанню служб віддаленого резервного копіювання можна заблокувавши використання цих служб (наприклад, заборонивши зв’язуватися зі службами домену) або налаштувавши мобільні пристрої, щоб вони не використовували такі служби. У такому випадку користувачів слід повідомити про заборону підключення своїх мобільних пристроїв до невідомих зарядних установок, а також вимогу носити й використовувати власні зарядні пристрої. Нарешті, можна заборонити мобільним пристроям обмінюватися даними один з одним за допомогою логічних або фізичних засобів (блокування використання служб через налаштування або фізичне екранування тощо) [10].

Використання ненадійного вмісту. Мобільні пристрої можуть використовувати ненадійний вміст, з яким інші типи пристроїв зазвичай не стикаються. Прикладом є коди швидкого реагування (QR), які спеціально розроблені для перегляду й обробки камерами мобільних пристроїв.

Кожен QR-код перекладається на текст, як правило, URL-адресу, тому шкідливі QR-коди можуть спрямовувати мобільні пристрої на шкідливі веб-сайти. Це може дозволити цілеспрямовану атаку, наприклад розміщення шкідливих QR-кодів у місцях збирання цільових користувачів.

Основною стратегією пом'якшення є ознайомлення користувачів із ризиками, пов'язаними з ненадійним вмістом, і запобігання їх доступу до ненадійного вмісту за допомогою мобільних пристроїв, які вони використовують для роботи.

Іншим способом пом'якшенням є використання програм, таких як QR-зчитувачі, які відображають незашифрований вміст (наприклад, URL-адресу) і дозволяють користувачам прийняти або відхилити його, перш ніж продовжити.

Залежно від конфігурації мережі також є можливим використання безпечних веб-шлюзів, проксі-серверів HTTP або інших проміжних пристроїв для перевірки URL-адрес, перш ніж дозволити з ними зв'язатися. У ситуаціях із високим рівнем безпеки можна обмежити використання периферійних пристроїв на мобільних пристроях, наприклад вимкнути використання камери, щоб запобігти обробці QR-кодів.

Використання служб визначення місцезнаходження. Мобільні пристрої з можливостями GPS зазвичай запускають так звані служби визначення місцезнаходження. Ці служби пов'язують місце, отримане за допомогою GPS, з відповідними підприємствами чи іншими організаціями, розташованими поблизу [10]. Служби визначення місцезнаходження активно використовуються соціальними мережами, навігацією, веб-браузерами та іншими програмами, орієнтованими на мобільні пристрої.

З точки зору безпеки компанії та особистої конфіденційності, мобільні пристрої з увімкненими службами визначення місцезнаходження піддаються підвищеному ризику цілеспрямованих атак, оскільки потенційним зловмисникам легше визначити, де знаходяться користувач і мобільний пристрій, і співвіднести цю інформацію з іншими джерелами про тих, з ким пов'язаний користувач, і види діяльності, які вони виконують у певних місцях.

Цю ситуацію можна пом’якшити, вимкнувши служби визначення місцезнаходження або заборонивши використання таких служб для певних програм, таких як програми для соціальних мереж або фото.

Користувачів також можна навчити вимикати служби визначення місцезнаходження під час перебування в чутливих місцях. Однак подібна проблема може виникнути, навіть якщо функції GPS або служби визначення місцезнаходження вимкнено. Веб-сайти та програми все частіше визначають місцезнаходження людини на основі її підключення до Інтернету, наприклад точки доступу Wi-Fi або діапазону IP-адрес [5]. Основним пом’якшенням цього є відмова від таких служб визначення місцезнаходження, коли це можливо.

Підприємства повинні знати, що увімкнення служб визначення місцезнаходження також може мати позитивний вплив на безпеку інформації. Наприклад, різні політики безпеки можуть застосовуватися залежно від того, чи використовується мобільний пристрій на території компанії чи за її межами.

1.3 Загрози мобільній безпеці підприємства

Під загрозою мобільній безпеці розумітимемо будь-які чинники, явища або події, які можуть бути причиною порушення політики мобільної безпеки і/або нанесення збитків мобільним пристроям і/або даним, що ними обробляються, зберігаються і передаються.

Загрози мобільній безпеці підприємства поділяють на два види: загрози для корпоративного використання мобільних пристроїв і загрози для систем управління мобільними пристроями.

Загрози для корпоративного використання мобільних пристроїв.

Схема типових загроз, пов’язаних із загальним використанням мобільних пристроїв, показана на рисунку 1.3 [12].

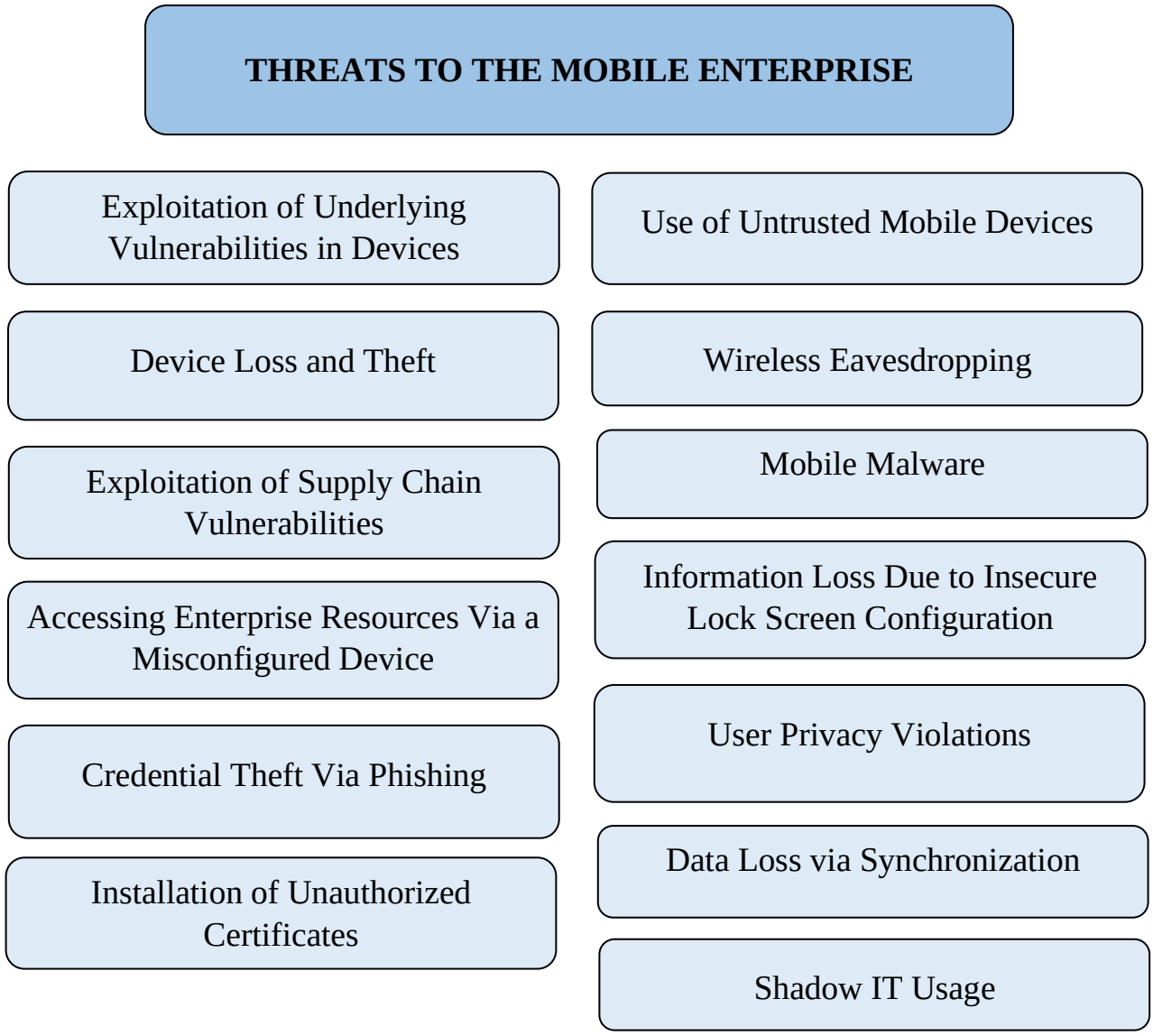

Рис. 1.3. Загрози використання мобільних пристроїв підприємства

Детальніше розглянемо кожну із зазначених загроз.

Використання базових уразливостей у пристроях. Розробка програмного забезпечення - це складна галузь, яка створює набір інструкцій для забезпечення роботи мобільних пристроїв і програм. У випадку типового ПЗ помилки та вразливості зустрічаються із приблизною частотою 25 помилок на 1000 рядків коду [13].

Під вразливістю будемо розуміти слабкість інформаційної системи, процедур безпеки системи, засобів внутрішнього контролю або впровадження, які можуть бути використані або спровоковані джерелом загроз [10].

Уразливості ПЗ існують на всіх рівнях стека мобільних пристроїв. Зважаючи на особливості розробки та виробництва мобільних пристроїв, кілька компаній розміщують ПЗ та мікропрограми для одного пристрою. Компанії-учасники можуть мати чи не мати надійних практик і процесів розробки ПЗ. Уразливість у коді будь-якого з цих постачальників може потенційно скомпрометувати пристрій. Прикладом є використання вразливостей у функціях голосової допомоги або швидкого доступу для обходу екрана блокування й отримання несанкціонованого доступу до мобільного пристрою.

Втрата та крадіжка пристрою. Мобільні пристрої використовуються в різних місцях поза контролем компанії, наприклад у помешканнях працівників, кафе, готелях і таксі. Деякі підприємства мають суворі правила щодо мобільних пристроїв, згідно з якими їх можна використовувати лише в межах компанії. Проте багато організацій мають кілька місць розташування чи приміщень, тому мобільні пристрої переносяться з місця на місце. Портативність мобільних пристроїв збільшує ймовірність їх втрати або викрадення, а наявність на них конфіденційних даних підвищує ризик компрометації для компанії.

Використання вразливостей ланцюга поставок. У ланцюжку постачання або в процесі розробки й розповсюдження пристроїв існує ймовірність вставлення зловмисного апаратного чи програмного забезпечення. Мобільні пристрої можуть містити шкідливі функції та бути вразливими через загрози для ланцюжка поставок.

Ці загрози в ланцюжку постачання можуть включати перехоплення зловмисником апаратного/програмного забезпечення мобільних пристроїв під час передачі пристроїв між постачальником і покупцем, або впровадження зловмисного коду у відкритий код, який зазвичай використовується для мобільних програм.

Уразливі місця, які виникають через загрози в ланцюжку поставок, можуть бути використані та спричинити серйозні проблеми, коли зачіпаються кілька пристроїв в компанії. Уразливості можуть включати бекдори, які надають зловмиснику віддалений кореневий доступ до пристрою.

Доступ до ресурсів підприємства через неправильно налаштований пристрій. Як і більшість інших інформаційних систем, мобільні пристрої можуть бути неправильно налаштовані. Мобільна ОС містить багато параметрів конфігурації, пов'язаних із безпекою та конфіденційністю, наприклад використання коду доступу, відстеження користувачів, VPN або інші методи, які забезпечують безпечне з'єднання з корпоративними ресурсами.

Однак, не всі параметри, пов'язані з безпекою та конфіденційністю, розташовані в області параметрів безпеки інтерфейсу мобільної ОС. Деякі програми, встановлені на пристрої, можна налаштувати в адміністративній області пристрою, а також у самій програмі. Відповідні конфігурації включають автентифікацію в програмі, відстеження користувачів і належне використання шифрування. Підключення неправильно налаштованого пристрою до ресурсу компанії, такого як корпоративний файловий ресурс, може надати інформацію суб'єктам, які контролюють мережу або неправильно отримують прямий доступ до пристрою.

Крадіжка облікових даних шляхом фішингу. Співробітники підприємства щодня отримують телефонні дзвінки, електронні листи, текстові повідомлення та повідомлення, пов'язані з додатками, на свої мобільні пристрої. Однак, інколи буває важко визначити справжність електронних листів і текстових повідомлень. Зловмисники часто намагаються викрасти або зробити запит на отримання облікових даних працівника за допомогою електронної пошти чи текстового повідомлення.

Прикладами фішингу є випадки, коли зловмисники намагаються обманом змусити особу повірити, що повідомлення надійшло з надійного джерела, і надати свої облікові дані або дати дозвіл на отримання неавторизованого доступу до свого мобільного пристрою, натиснувши гіперпосилання в електронному чи текстовому повідомленні [14].

Встановлення несанкціонованих сертифікатів. Цифрові сертифікати - це програмні криптографічні маркери, які використовуються, серед іншого, для автентифікації та підпису програмного забезпечення [15]. Ці сертифікати

можна розповсюджувати на пристрої через різні канали, включаючи веб-браузери, фізичні з’єднання (наприклад, USB-кабель) і профілі, застосовані через політику управління корпоративною мобільністю (Enterprise Mobility Management, EMM). Коли сертифікат надається в сховище сертифікатів мобільного пристрою, його можна використовувати для автентифікації та прийняття довірчих рішень щодо програм, показуючи користувачам попередження. Наявність зловмисного сертифіката може обманом змусити пристрій користувача довіритися фішинговому сайту або встановити підроблену фішингову чи троянську програму, наприклад банківську програму.

Використання ненадійних мобільних пристроїв. Багато мобільних пристроїв, особливо ті, що належать особисто працівникам, не є надійними. Наприклад, джейлбрейк або рутування пристрою обходять вбудовані обмеження щодо безпеки, використання ОС та інших функцій. Усі мобільні пристрої можна умовно вважати ненадійними, якщо компанія не захищає їх належним чином і не контролює їх безпеку постійно, поки пристрої використовуються для доступу до корпоративних програм або даних. Ненадійні пристрої є найбільш ризикованими мобільними пристроями, часто мають доступ до конфіденційної корпоративної інформації, і їх найлегше зламати.

Бездротове прослуховування. Мобільні пристрої використовують переважно некорпоративні мережі для доступу до Інтернету, а підприємства зазвичай не мають можливості контролювати безпеку зовнішніх комунікаційних мереж, до яких мають доступ пристрої, і мають обмежену видимість бездротового трафіку.

Серед засобів зв’язку можуть бути бездротові системи, такі як Bluetooth, Wi-Fi та стільникові мережі. Пристрої Bluetooth часто використовуються для передачі аудіоінформації (наприклад, голосового трафіку, музики), а також сповіщень та інформації про стан здоров’я від переносних пристроїв. Wi-Fi і стільниковий зв’язок можна використовувати для передачі різних типів трафіку, включаючи голос і дані. Усі ці мережеві протоколи та переносні засоби вразливі

до підслуховування й атак типу MitM, які можуть перехоплювати і модифікувати зв’язок між пристроєм і системою підприємства [12].

Шкідливі мобільні програми. Оскільки користувачі можуть завантажувати програми на свій пристрій, дозволяючи їх встановлення з ненадійних або невідомих джерел, виникають значні ризики для безпеки мобільних пристроїв і магазинів додатків, які не встановлюють обмежень безпеки чи інших обмежень на публікацію додатків сторонніх розробників. Тому організації повинні усвідомлювати, що будь-яка програма, встановлена на мобільному пристрої, може бути засобом компрометації пристрою й надання зловмиснику доступу до конфіденційної корпоративної інформації.

Мобільні пристрої мають багато датчиків, як-от мікрофони та камери, щоб покращити функціональність користувача, наприклад здійснювати телефонні дзвінки та робити розширені зображення. З огляду на це, шкідливі мобільні програми на мобільному пристрої можуть використовувати ці датчики для прихованого збору інформації про користувача чи адміністратора. Мікрофони та камери мають бути відкритими лише під час використання та захищеними в інший час.

Втрата інформації через незахищену конфігурацію екрана блокування. Екран блокування є першим бар'єром, який має подолати неавторизований користувач, щоб отримати доступ до інформації, яка зберігається на мобільному пристрої. Екран блокування можна налаштувати за допомогою фактора автентифікації, щоб обмежити доступ до пристрою. Якщо заблокований екран погано захищено простим паролем, його можна зламати шляхом грубої атаки. Неавторизований користувач, який скомпрометував фактор автентифікації мобільного пристрою, може отримати доступ до всієї конфіденційної інформації, змінити інформацію та видати себе за власника пристрою, щоб отримати подальший доступ до корпоративних даних.

Екран блокування також можна налаштувати для відображення сповіщень, пов’язаних із пропущеними дзвінками чи повідомленнями, сповіщень програм, отриманих електронних листів тощо. Інформація, яка

відображається на екрані блокування, наприклад електронні листи, може відображати конфіденційну корпоративну інформацію. Ці сповіщення на екрані блокування можуть надати неавторизованому користувачеві інформацію і йому не потрібно буде розблоковувати мобільний пристрій.

Порушення конфіденційності користувачів. Збір і моніторинг даних користувачів або співробітників можуть значно підірвати особисту конфіденційність людини. Багато мобільних програм збирають і відстежують дані користувача, такі як місцезнаходження, контакти, історія веб-перегляду та загальна інформація про систему. Ця інформація зазвичай використовується в маркетингових цілях, щоб спрямовувати певну рекламу до користувача.

Однак, мобільні програми - не єдині системи, які збирають інформацію про користувачів. Більшість бізнес-систем, наприклад, системи управління корпоративною мобільністю EMM та захисту від мобільних загроз (Mobile Threat Defence, MTD), також можуть мати цю можливість, тобто роботодавець може збирати конфіденційну інформацію про працівника.

Цей тип збору даних дозволений, якщо бізнес публічно повідомляє користувачів про будь-які дані, які він зібрав, включаючи ідентифікаційну інформацію та іншу інформацію про користувачів. Збір даних без згоди користувача перешкоджає конфіденційності й може розглядатися як її порушення, оскільки зібрані дані можуть бути використані в небажаний спосіб без відома користувача [12].

Одним із поширених порушень конфіденційності є відстеження місцезнаходження користувача. Служби визначення місцезнаходження зазвичай використовуються такими програмами як соціальні мережі, програми навігації та погоди, а також веб-переглядачі. З точки зору безпеки й особистої конфіденційності, мобільні пристрої з увімкненими службами визначення місцезнаходження піддаються підвищеному ризику цілеспрямованих атак. Оскільки потенційним зловмисникам легше визначити, де знаходяться користувач і мобільний пристрій, і співвіднести цю інформацію з іншими джерелами про даних про нього. Хоча доступ до служб визначення

місцезнаходження може мати позитивний вплив на кібербезпеку (наприклад, увімкнення політик на основі місцезнаходження та конфігурації пристроїв), для цього потрібна згода користувача й детальний опис того, до якого типу особистої інформації підприємство може отримати доступ.

Втрата даних через синхронізацію. Мобільні пристрої можуть взаємодіяти з іншими системами для здійснення обміну, синхронізації та зберігання даних як локально, так і віддалено. Локальна синхронізація зазвичай включає підключення мобільного пристрою до настільного чи портативного комп'ютера бездротовим способом або через кабель. Синхронізація віддаленої системи часто передбачає автоматичне резервне копіювання даних у хмарну систему зберігання.

Коли всі ці компоненти знаходяться під корпоративним контролем, ризик, як правило, є прийнятним, але один або кілька з цих компонентів часто є зовнішніми для підприємства. Приклади включають підключення особистого мобільного пристрою до ноутбука, виданого компанією, підключення мобільного пристрою, виданого компанією, до персонального ноутбука, підключення корпоративного мобільного пристрою до віддаленої служби резервного копіювання фотографій і підключення мобільного пристрою до ненадійного зарядного устаткування. У всіх цих сценаріях дані компанії знаходяться під загрозою зберігання в незахищеному місці поза її контролем або передачі зловмисного ПЗ з одного пристрою на інший.

Тіньове використання ІТ. Підприємства, які впроваджують політику повного управління мобільними пристроями, повинні усвідомлювати ризики, пов'язані з тіньовими ІТ. Термін «тіньові ІТ» зазвичай означає використання співробітниками пов'язаного з роботою обладнання, ПЗ або хмарних служб без відома ІТ-департаменту компанії [16].

Типовим прикладом використання тіньових ІТ є відділ, який виконує критично важливу роботу, використовуючи незалежно придбаний сервер із програмним забезпеченням, що не схвалене, не контролюється чи навіть не відоме ІТ-спеціалістам підприємства. ІТ-персонал може не дізнатися про

існування цієї системи, доки вона не вийде з ладу або не буде зламана, що ставить під загрозу критичну місію.

Співробітники часто вдаються до використання тіньових ІТ-систем, коли надані підприємством системи і процеси вважаються громіздкими, заважають роботі, або коли компанія не може забезпечити придбання необхідних систем.

Прикладами використання тіньових ІТ є, коли працівники:

– використовують власні мобільні телефони, щоб обійти обмежувальні політики щодо мобільних пристроїв компанії;

– надсилають електронні листи чи робочі документи на свою особисту адресу електронної пошти, щоб забезпечити кращий доступ під час подорожей;

– використовують несхвалені програми чи хмарні служби для зберігання корпоративних даних або фотографує робочі матеріали камерою на своїх особистих пристроях;

– використовують тіньові ІТ, коли адміністративні обмеження компанії нібито порушують їх конфіденційність. Наприклад, у випадку, коли системним адміністраторам надано дозвіл контролювати весь зв’язок із корпоративних мобільних телефонів) [12].

Іншим прикладом є тетерінг (Tethering), який передбачає використання одного мобільного пристрою у якості точки доступу до мережі для іншого мобільного пристрою [16].

Ще одним потенційним засобом використання тіньових ІТ є модем. Якщо компанія дозволяє модем, вона повинна переконатися, що мережеві з’єднання, які включають модем, надійно захищені (наприклад, шифруванням зв’язку). Якщо компанія забороняє модем, вона повинна налаштувати мобільні пристрої для запобігання модема. Тіньові ІТ-системи не відповідають корпоративним вимогам щодо корпоративного контролю чи документації та можуть порушувати політику безпеки чи надійності. У деяких випадках тіньові ІТ можуть надавати переваги завдяки підвищенню продуктивності. Водночас, варто пам’ятати, що тіньові ІТ є потенційно небезпечними і для захисту в

процесі їх використання не існує єдиного повноцінного рішення. Наприклад, технології EMM не вирішують їх проблеми повністю.

Загрози для систем управління мобільними пристроями.

Схема типових загроз для систем управління мобільними пристроями показана на рисунку 1.4 [12].

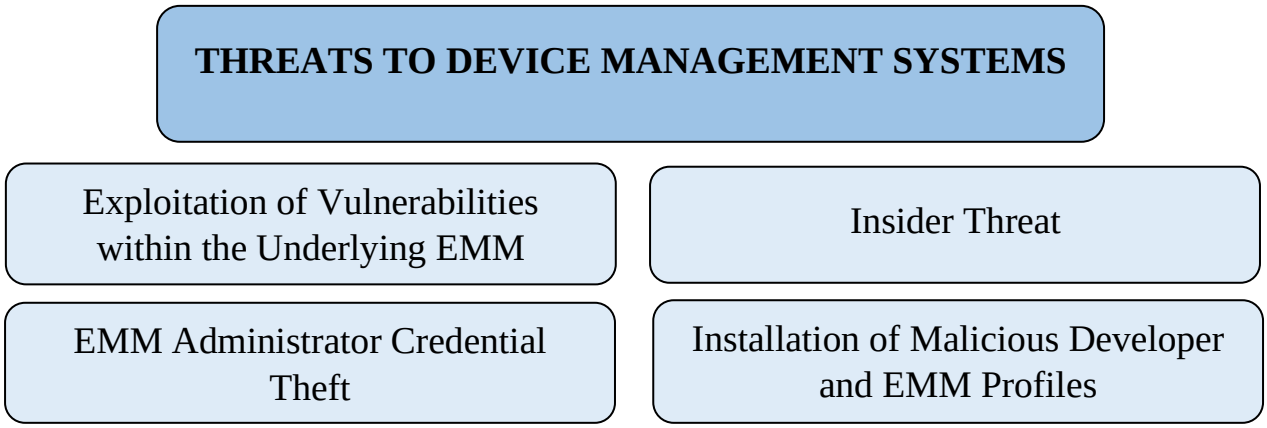

Рис. 1.4. Загрози для систем управління мобільними пристроями

Використання вразливостей базової платформи EMM. Інфраструктура EMM та її компоненти працюють на стандартному апаратному забезпеченні, вбудованому програмному забезпеченні та додатках, які є чутливими до загальновідомих програмних і апаратних недоліків. Незважаючи на те, що системи значною мірою налаштовуються, стандартне апаратне забезпечення та добре відомі ОС слід ідентифікувати й добре розуміти. Ці системи повинні належним чином налаштовуватися і регулярно встановлювати виправлення для усунення відомих вразливостей на основі Національної бази вразливостей [18].

Крадіжка облікових даних адміністратора EMM. Крадіжка облікових даних є основною проблемою для працівників, але облікові дані системних адміністраторів, які працюють із консоллю EMM, також можуть бути скомпрометовані. Якщо зловмисники зможуть увійти в EMM як адміністратор, може статися втрата конфіденційної інформації, оскільки EMM зберігає різноманітну конфіденційну інформацію про персонал на всіх рівнях компанії (адреси електронної пошти, номери телефонів, імена користувачів, призначені ресурси, рівні доступу й метадані голосового і текстового спілкування).

Крім того, облікові дані адміністратора EMM дозволяють зловмиснику неправильно налаштовувати й переводити мобільні пристрої в незахищений стан, змінюючи політики, які до них застосовуються. Нарешті, зловмисник також може здійснити DoS атаку, видалити корпоративні записи з EMM і скасувати корпоративний доступ для всіх мобільних пристроїв.

Внутрішня загроза. Внутрішня загроза походить від нинішнього або колишнього співробітника, який використовує авторизований доступ до системи компанії, щоб порушити корпоративну політику безпеки. У таких випадках система EMM, яка є важливим інструментом для безпечного адміністрування мобільних пристроїв, може бути «палицею з двома кінцями». Зокрема, її можна використовувати і як механізм для захисту підприємства від внутрішніх загроз (наприклад, впровадження практик, зосереджених на управлінні паролями та обліковими записами, доступом, змінами системи та політиками використання програм), і як вектор атаки для зловмисного інсайдера [19].

Зловмисний інсайдер, який має доступ до системи EMM, може послабити дозволи, щоб увімкнути витік даних, зареєструвати неавторизовані пристрої чи сторонніх осіб, додати шкідливі програми до білого списку або здійснити інші неприйнятні дії. З огляду на це, слід ретельно контролювати використання систем EMM та інших інструментів адміністрування мобільних пристроїв, щоб виявити можливу зловмисну внутрішню діяльність.

Встановлення профілів зловмисного розробника та EMM. Встановлення профілів EMM дозволяє підприємству контролювати привілейовані операції, які надаються мобільними ОС. Є кілька способів, за допомогою яких користувачі мобільних пристроїв можуть бути зареєстровані в EMM і профілях, що виділені на їхні мобільні пристрої. Одним із найпоширеніших є встановлення програми EMM (іноді її називають агентом MDM) безпосередньо на мобільний пристрій. Коли це налаштування завершено, кінцеві користувачі можуть вводити інформацію, унікальну для своєї компанії, і автентифікуватися на сервері EMM. У цей момент користувачеві надається профіль EMM, який містить спеціальні дозволи й інші ресурси, схвалені адміністраторами [6].

Профілі EMM можна передати користувачеві різними способами, наприклад електронною поштою, текстовими повідомленнями або завантаженнями з автомобіля. Якщо користувач випадково приймає шкідливий профіль, наданий з використанням одного з цих методів, зловмиснику може бути надано привілейований доступ. Таким чином зловмисник може використовувати всі API управління доступом до корпоративних даних на пристрої та, можливо, навіть до інформації, що зберігається у серверній інфраструктурі компанії.

Підсумовуючи, варто відзначити, що NIST також створив і забезпечує постійне оновлення каталогу мобільних загроз (Mobile Threat Catalogue, MTC) [20], який описує, ідентифікує і структурує загрози для мобільних систем. Так, у каталозі усі загрози мобільній безпеці поділені на такі категорії, відповідно до об’єкта деструктивного впливу, зокрема для мобільних додатків; механізмів автентифікації; систем та інфраструктури стільникового зв’язку; мобільної екосистеми; корпоративних систем управління мобільністю; технологій GPS; локальних і персональних мереж (LAN & PAN); мобільних платежів; фізичного доступу до мобільних пристроїв; конфіденційності користувачів; стеку пристроїв і ПЗ, мікропрограм, що використовується для розміщення й управління пристроєм; ланцюга постачання пристроїв та їх компонентів.

Висновки до розділу 1

У результаті дослідження встановлено, що мобільні пристрої, крім очевидних переваг надання користувачам доступу до послуг, додатків і даних у будь-який час і будь-якому місці, створюють унікальні загрози для особи і підприємства, оскільки у ході виконання корпоративних завдань вони регулярно обробляють, зберігають і передають конфіденційні дані.

З огляду на зростаючу важливість мобільних технологій для компанії й успішності її бізнес-діяльності забезпечення мобільної безпеки має нагальне значення. Під безпекою мобільних пристроїв розумітимемо галузь кібербезпеки, яка має на меті захист мобільних пристроїв від загроз несанкціонованого доступу, використання чи модифікації. Безпека мобільного середовища підприємства включає безпеку пристрою, даних, програм і мережі.

Аналіз показав, що основними вразливостями безпеки мобільних технологій є: відсутність засобів контролю фізичної безпеки; використання ненадійних мобільних пристроїв, мереж, програм і контенту, взаємодія з іншими системами, використання служб визначення місцезнаходження.

З’ясовано, що загрози мобільній безпеці підприємства поділяють на два види: загрози для корпоративного використання мобільних пристроїв і загрози для систем управління мобільними пристроями. Загрози для корпоративного використання мобільних пристроїв включають: використання базових уразливостей, втрату і крадіжку пристроїв; використання вразливостей ланцюга поставок; доступ до ресурсів через неправильно налаштований пристрій; крадіжку облікових даних шляхом фішингу; встановлення несанкціонованих сертифікатів; використання ненадійних мобільних пристроїв; бездротове прослуховування; шкідливе ПЗ; порушення конфіденційності користувачів; втрату інформації через незахищену синхронізацію; тіньове використання ІТ.

Загрозу для систем управління мобільними пристроями становлять: використання вразливостей базової платформи ЕММ, крадіжка облікових даних адміністратора ЕММ, внутрішні загрози, встановлення профілів зловмисного розробника та ЕММ.

РОЗДІЛ 2
ОГЛЯД ТЕХНОЛОГІЙ МОБІЛЬНОЇ БЕЗПЕКИ

За останнє десятиліття технології мобільної безпеки розвинулися на стільки, що стали повнофункціональними пакетами управління безпекою. Для поглиблення керованості корпоративних пристроїв додаються нові можливості й функції, деякі з них вбудовані в пристрій, тоді як інші є послугами, що надаються третіми сторонами, і знаходяться на зовнішніх веб-серверах.

Технології мобільної безпеки поділяють на два види: технології управління й безпеки пристрою та технології мобільної безпеки підприємства.

2.1 Технології управління й безпеки пристрою

Технології управління та підвищення безпеки пристрою включають такі види [12] (Рис. 2.1). Розглядаючи дані технології, варто зауважити, що не всі мобільні пристрої мають однакові функції та можливості безпеки.

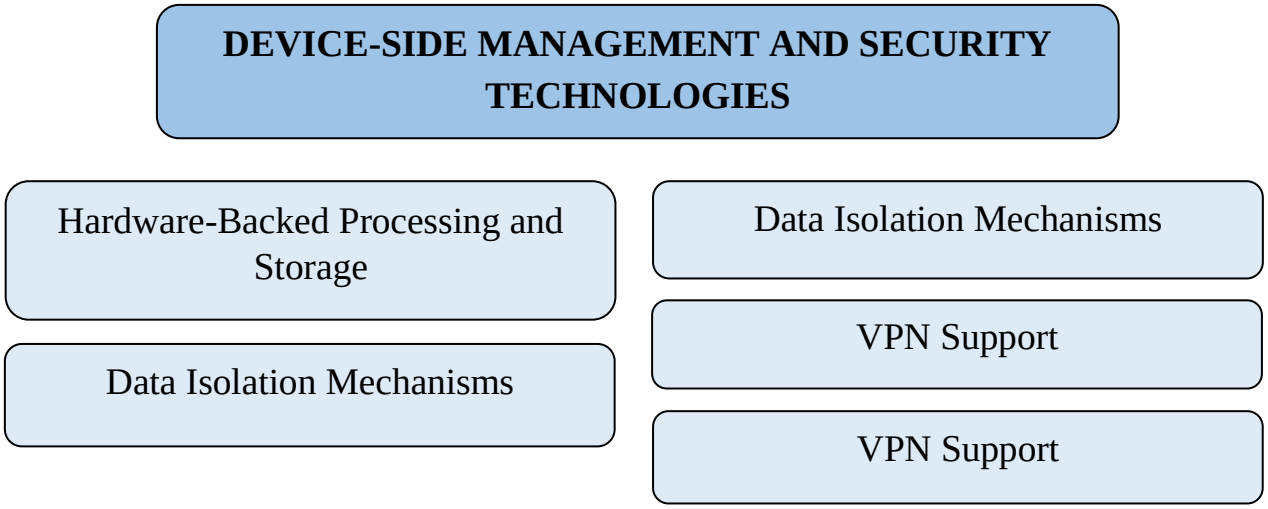

Рис. 2.1. Технології управління та безпеки пристрою

Апаратна підтримка обробки та зберігання даних. Багато мобільних пристроїв містять спеціальні апаратні компоненти для захисту криптографічних

ключів, паролів, цифрових сертифікатів, біометричних шаблонів та іншої конфіденційної інформації. Ці апаратні компоненти також часто використовують для підтримки шифрування даних користувача на мобільних пристроях.

Деякі мобільні пристрої пропонують спеціальні компоненти для виконання конфіденційних операцій, таких як прийняття рішень щодо безпеки (наприклад, надання доступу до привілейованого API) або виконання криптографічних операцій з даними. На деяких платформах безпечне зберігання даних і конфіденційні операції об’єднані в одну SoC (System-on-a-Chip) – материнську плату, що виконує функції цілого пристрою і розміщена на одній інтегральній схемі. Пристрої iOS і Android підтримують апаратну обробку та зберігання [21, 22].

Хоча ці компоненти можуть бути вбудовані в пристрої, вони можуть не використовуватися за замовчуванням. Програми повинні належним чином використовувати правильні API, щоб повністю використовувати функції безпеки, які надає платформа. На деяких платформах API можуть бути доступні не всім розробникам. На інших платформах невеликі програми можна розробляти спеціально для роботи в цих обмежених середовищах безпеки.

Нарешті, пристрої можуть використовувати інші модулі безпеки або елементи, призначені для забезпечення безпечної реалізації конкретних завдань, наприклад, деякі мобільні платіжні рішення використовують чіп, спеціально розроблений для обробки певних транзакцій і шифрування платіжної інформації, що на ньому зберігається.

Механізми ізоляції даних. Мобільні пристрої забезпечують механізми ізоляції даних для запобігання несанкціонованому доступу до даних користувача та пристрою. Приклади механізмів ізоляції даних включають шифрування й ізольоване програмне середовище.

Ізолювання даних за допомогою шифрування розділяє дані на основі авторизованого доступу. Цей механізм означає, що лише користувачі, які мають відповідний криптографічний ключ, можуть отримати доступ до зашифрованих даних на пристрої. Мобільні пристрої шифрують дані

користувача, але дані можуть бути зашифровані за допомогою ключа, яким керує ОС, а не користувач, розробник або компанія.

Ізольоване програмне середовище або пісочниця (Sandbox) на мобільному пристрої може бути реалізована різними способами. Мобільні ОС реалізують ізольоване програмне середовище, яке зазвичай запобігає взаємодії програм одна з одною. Винятки створюються на основі чітко визначених методів, однозначно прийнятих користувачем, наприклад, запитуючи користувача, чи надає він дозвіл програмі на виконання завдання. Крім того, якщо програми створено спільним розробником, їм може бути дозволено обмінюватися інформацією, оскільки вони підписані тим самим ключем розробника. Додаткові пісочниці можуть існувати на рівні користувача або нижче, що забезпечує додатковий рівень сегментації даних [23].

API управління платформою. Основні платформи мобільних ОС пропонують набір API і допоміжних протоколів, які можуть використовуватися сторонніми інструментами керування. API управління пропонують доступ до можливостей, недоступних звичайним розробникам, зокрема управління поведінкою програми, налаштування пристроїв і параметрів безпеки, а також запит конфіденційної інформації про пристрій. Доступ до цих API може бути обмежений підгрупою конкретних розробників, перевірених власниками платформи. Крім того, на доступ до цих API має надати згоду або кінцевий користувач пристрою, або член IT-персоналу компанії. Варто зауважити, що більшість платформ пристроїв дозволяють керувати цими API лише одним рішенням MDM. Можливості управління, що пропонуються власниками платформи, також доповнюються зовнішньою інфраструктурою.

У деяких ситуаціях IT-адміністратори можуть безпосередньо управляти пристроями, тоді як в інших налаштуваннях IT-адміністратори надсилають команди до інфраструктури власника платформи, які згодом передаються на пристрій. Обидва ці сценарії можна розмістити в одній панелі управління і зробити невидимими для користувача.

Підтримка VPN. Мобільні платформи підтримують віртуальні приватні мережі (VPN), які розробники можуть використовувати через API. VPN насамперед забезпечують захист конфіденційності шляхом шифрування даних користувачів.

Існує три типи VPN: VPN на рівні ОС, VPN на рівні додатка та веб-VPN. VPN на рівні ОС можна налаштувати за допомогою платформ управління, а іноді їх можна перевести в стан «завжди ввімкнено». VPN на рівні ОС можуть бути більш енергоефективними й шифрувати великий обсяг трафіку користувачів. Протоколи, які можна використовувати, включають протокол захисту Інтернет-протоколу (IPsec) і протокол тунелювання рівня 2 (L2TP).

На відміну від VPN на рівні ОС, VPN на рівні програми можна налаштувати різними способами, зокрема шляхом використання системних API VPN для захисту даних користувачів або просто захищати дані однієї програми. Більш складні налаштування можуть розгортати VPN для конкретної мобільної програми. Нарешті, користувачам легко скористатися перевагами мереж VPN, часто просто погоджуючись із політикою веб-сторінки. Веб-мережі VPN використовують безпеку транспортного рівня (Transport Layer Security, TLS) і можуть не використовувати ті самі додаткові засоби захисту, які використовуються в інших типах VPN [24].

Механізми автентифікації. Мобільні пристрої пропонують різноманітні датчики, які можуть увімкнути стандартну та біометричну автентифікацію. Біометричну автентифікацію на мобільному пристрої можна використовувати разом із паролями чи PIN-кодами або замість них.

Мобільні апаратні засоби зазвичай не містять і не зберігають необроблені біометричні дані. Натомість біометричні дані трансформуються (наприклад, токенізуються) і можуть безпечно зберігатися, мінімізуючи їх вразливість до зворотного проектування та потенційного впливу зловмисника. Біометричні дані зазвичай зашифровані, зберігаються на пристрої та захищені ключем, доступним лише у спеціальному середовищі безпеки.

Датчики, які використовуються для біометричної автентифікації, включають: датчик відбитків пальців для аутентифікації за відбитками пальців; спеціальні камери та інші датчики для допомоги в розпізнаванні обличчя; гіроскоп, акселерометр або крокомір для аутентифікації на основі ходи; і мікрофон для розпізнавання голосу.

Деякі датчики не доступні безпосередньо розробникам, і рішення про доступ приймаються у власних середовищах безпеки. Хоча ці датчики найчастіше використовуються для локальної автентифікації пристрою, їх також можна використовувати для віддаленої автентифікації на корпоративних ресурсах. Іншим механізмом, який можна використовувати для віддаленої автентифікації, є похідні облікові дані підтвердження особи (PIV). У цьому випадку мобільний пристрій використовує автентифікацію на основі сертифіката за допомогою маркера, пов’язаного з обліковими даними PIV [12].

2.2 Технології мобільної безпеки підприємства

Технології управління мобільною безпекою використовують як для корпоративних, так і особистих мобільних пристроїв і поділяють на: засоби управління конфігурацією пристрою, управління додатками або захисту від мобільних загроз, а також управління мобільними ідентифікаторами, мобільним вмістом і мобільними даними. Загальна схема технологій мобільної безпеки показана на рисунку 2.2 [12].

Розглянемо поточний стан і застосування цих технологій, зосереджуючись на їхніх компонентах і можливостях безпеки. Ці технології є основою для рекомендованих технічних засобів пом’якшення загроз і заходів їх протидії.

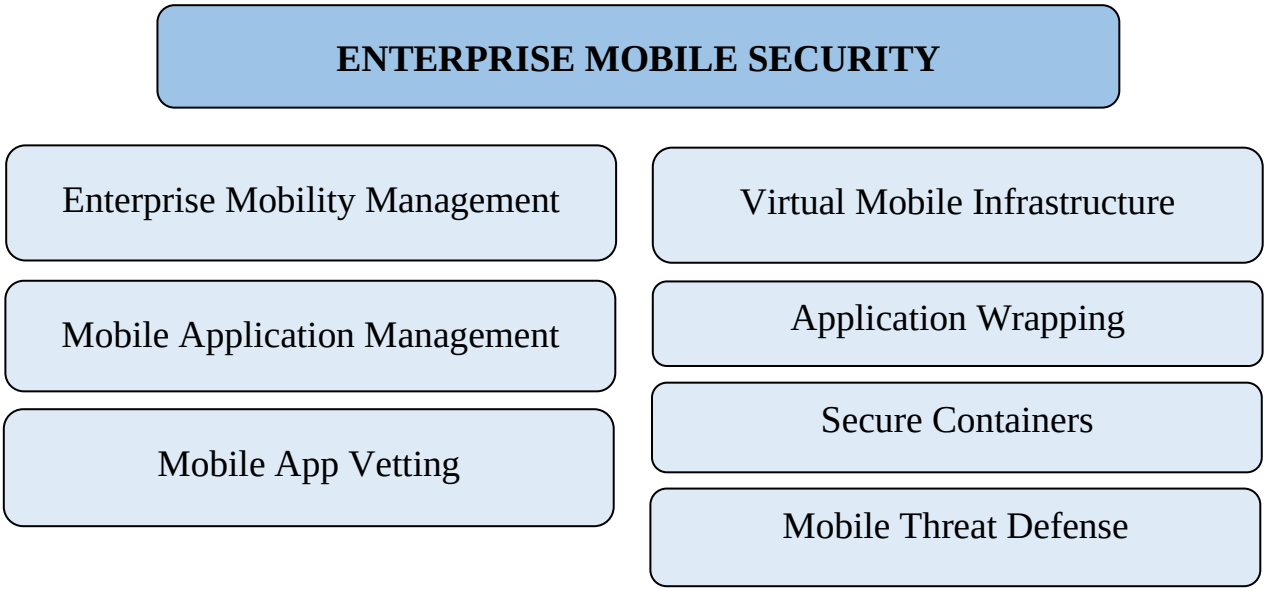

Рис. 2.2. Технології мобільної безпеки підприємства

Управління мобільністю підприємства. Системи EMM, які іноді називають системами уніфікованого управління кінцевими точками (Unified Endpoint Management, UEM) - це рішення, яке використовується для розгортання, налаштування й активного управління мобільними пристроями в корпоративному середовищі.

Набір EMM може охоплювати управління мобільними пристроями (Mobile Device Management, MDM), управління мобільними додатками (Mobile Application Management, MAM), виявлення мобільних загроз MTD й інші технології управління. Ці системи розробляються різними організаціями, зокрема виробниками мобільних пристроїв, розробниками мобільних ОС і незалежними сторонніми організаціями-розробниками. EMM базуються на API і протоколах MDM, використовують технології для моніторингу мобільних пристроїв, розгортання політик і налаштування технологій безпеки на стороні пристрою (наприклад, безпечні контейнери) [25].

Перелік можливостей безпеки, які надаються EMM або будь-якою з їхніх систем підтримки, можуть відрізнятися, а більшості компаній не знадобляться всі передбачені можливості безпеки. Підприємства, які розгортають мобільні пристрої, повинні розглянути переваги кожної можливості безпеки, визначити, які служби потрібні для їхнього середовища, а також розробити і придбати одне або кілька рішень, які разом надають необхідні послуги для їхніх потреб.

Застосування загальної політики. Технологія ЕММ застосовує корпоративні політики безпеки на мобільному пристрої, які можуть налаштовувати або обмежувати використання мобільних функцій і можливостей безпеки. ЕММ може автоматично відстежувати, виявляти й повідомляти про порушення політики та автоматично вживати заходів, коли це можливо й доцільно.

Загальні обмеження політики або параметрів конфігурації для захисту мобільних пристроїв включають:

– управління інтерфейсами бездротової мережі (WiFi, Bluetooth, NFC);

– обмеження доступу користувачів і програм до апаратного забезпечення (наприклад, цифрової камери та знімного носія) і функцій пристрою (наприклад, копіювання та вставлення);

– виявлення змін у затвердженій базовій лінії конфігурації безпеки;

– обмеження або заборона доступу до корпоративних служб на основі версії ОС мобільного пристрою (включно з тим, чи було пристрій зламано), постачальника/бренду, моделі чи версії клієнта ПЗ для управління мобільним пристроєм (якщо застосовно);

– вимкнення режиму налагодження або розробника [12, 26].

Автентифікація користувача та пристрою. Автентифікацію користувача та пристрою визначають і застосовують за допомогою технології ЕММ. Деякі основні параметри та положення включають:

– вимога введення паролю або іншого засобу автентифікації для розблокування пристрою (наприклад, пароль, біометричне сканування).

– вимога введення паролю/коду та/або іншого механізму автентифікації (наприклад, автентифікація на основі маркерів, мережевого пристрою, домену, цифровий сертифікат) для доступу до ресурсів компанії. Сюди входять основні параметри надійності пароля, обмеження на кількість дозволених повторних спроб без негативних наслідків (наприклад, блокування облікового запису, очищення пристрою) і старіння пароля.

– автоматичне блокування пристрою після того, як він деякий час не використовується (наприклад, 45 секунд, 5 хвилин).

– дистанційне блокування пристрою під керівництвом адміністратора, якщо є підозра, що він загублений або залишений у розблокованому стані в незахищеному місці.

– очищення пристрою після певної кількості неправильних спроб автентифікації або через заздалегідь визначений проміжок часу без реєстрації в ЕММ [12]. Водночас, варто пам’ятати, що можливість відновлення даних через ЕММ після видалення обмежена.

Передача та зберігання даних. Захист для передачі і зберігання даних на пристрої можна визначити й застосувати за допомогою технології ЕММ. Положення щодо цих засобів захисту даних включають:

– надійне шифрування передачі даних між мобільним пристроєм і компанією. Таке шифрування найчастіше виконується за допомогою VPN, хоча його можна встановити за допомогою інших видів використання безпечних протоколів і шифрування;

– надійне шифрування даних, що зберігаються як у вбудованому сховищі, так і на знімному носії. Знімний носій також можна «прив’язати» до певних пристроїв, щоб зашифровану інформацію можна було розшифрувати лише тоді, коли знімний носій під’єднано до певного пристрою, тим самим зменшуючи ризик офлайн-атак на носій;

– очищення пристрою, перш ніж передавати його іншому користувачеві, виводити з експлуатації тощо;

– дистанційно очищення пристрою (витирання збережених даних), якщо є підозри, що пристрій було втрачено, викрадено чи він іншим чином потрапив у ненадійні руки, і є ризик відновлення даних ненадійною стороною [25].

Управління мобільними додатками. Деякі системи ЕММ містять функцію управління мобільними додатками МАМ, яка дає змогу управляти

різними програмами на одному керованому пристрої. Хоча MAM може також пропонуватися й окреме стороннє рішення.

Системи MAM призначені для забезпечення корпоративного контролю над мобільними програмами, які отримують доступ до корпоративних служб і/або даних. Ці додатки можуть бути приватними й загальнодоступними. На відміну від MDM, системи MAM не вимагають від власника пристрою реєструвати пристрій під управлінням підприємства, а також власник не повинен погоджуватися на встановлення корпоративного профілю на пристрої. Ця різниця є важливою для додатків, розроблених, зокрема, для підтримки транзакцій між компаніями (B2B) (наприклад, програма, що надається постачальникам для доступу до бази даних корпоративних замовлень). У таких випадках мобільний користувач не є працівником компанії, яка пропонує додаток. Підприємствам із політикою використання власного пристрою працівника (Bring Your Own Device, BYOD) використання функції MAM замість MDM допоможе вирішити проблеми конфіденційності користувачів щодо їхніх особистих пристроїв.

Додатками, які використовуються на мобільних пристроях, можна управляти за допомогою технології EMM. Залежно від того, як пристрій управляється і зареєстрований у рішенні EMM, застосовують такі обмеження:

– обмеження переліку магазинів програм, дозволених для використання (наприклад, обмеження щодо доступу до офіційних магазинів програм чи стороннього завантаження програм);

– обмеження списку дозволених для встановлення програм, додавши дозволені програми в білий список або заблокувавши заборонені програми;

– обмеження дозволів (наприклад, доступу до камери, місцезнаходження), призначених кожній програмі. Може використовуватися технологія запаковування додатків;

– реалізація механізмів захисту для встановлення, оновлення та видалення програм на мобільному пристрої;

– обмеження використання служб синхронізації та спільного доступу до ОС і програм (наприклад, синхронізації локального пристрою, служб віддаленої синхронізації та веб-сайтів);

– поширення додатків зі спеціального корпоративного магазину мобільних додатків, наданих за допомогою технології EMM;

– поширення додатків компанії з офіційного магазину додатків [12].

Варто відзначити, що деякі з перелічених можливостей залежать від платформи і можуть бути доступними не на всіх системах.

Рішення MAM дозволяють підприємствам контролювати доступ до корпоративних додатків та інтегрувати власний корпоративний каталог додатків із магазином додатків постачальника мобільних пристроїв (наприклад, Apple App Store, Google Play), щоб мобільні користувачі могли легко встановлювати корпоративний додаток.

Системні адміністратори можуть розгортати програми або надсилати оновлення мобільним користувачам бездротовими каналами. Вони також можуть обмежити функції програми, не впливаючи на весь пристрій, підхід, якому віддають перевагу користувачі BYOD.

Визначення й застосування політики безпеки і конфіденційності - ключова функція систем MAM, яка часто включає в себе політику на основі користувачів або ролей для доступу до певних програм та інтеграцію з дистанційним очищенням для працівників, які звільняються або змінюють посади.

Шифрування або контейнеризацію використовують для розділення середовищ виконання програм або їх зв’язку з корпоративними службами. Нарешті, системи MAM надає можливість системним адміністраторам підприємства контролювати поведінку програм, відповідність конфігурації або наявність неавторизованих програм на пристрої користувача [27].

Мобільний захист від загроз. Системи захисту від мобільних загроз MTD призначені для виявлення наявності шкідливих програм, мережевих атак, фішингових атак, неправильних конфігурацій і відомих уразливостей у мобільних програмах або самій мобільній ОС. Хоча MTD є переважаючим

терміном, використовують також терміни захист від мобільних загроз (Mobile Threat Protection, MTP) і захист кінцевої точки UEM. MTD - це категорія технологій, яка захищає пристрої від різноманітних загроз, які створюють самі пристрої та будь-які підключені мережі.

Ці системи часто запускають на пристрої агента - як правило, мобільний додаток, та ініціюють аналіз і навчання на зовнішніх хмарних платформах. MTD забезпечують постійний моніторинг у режимі реального часу для оцінки програм після розгортання на мобільному пристрої та під час їх виконання.

Системи MTD знаходяться на мобільному пристрої й не залежать від підключення до мережі, що дає змогу виявляти і захищати від мобільних загроз, навіть якщо мережеве підключення пристрою заблоковано або зламано. У корпоративному контексті система MTD може бути інтегрована з EMM, щоб увімкнути сповіщення користувача або адміністратора або автоматизовану відповідь для усунення виявлених уразливостей, карантинних програм або пристроїв. Деякі мобільні платформи включають вбудовані можливості, схожі на можливості системи MTD, якими не управляє користувач або адміністратор.

MTD може виявляти й захищати мобільний пристрій, програми та кінцевого користувача від фішингових атак або атак типу MitM через бездротову мережу. Системи MTD також можуть виявляти атаки на програму або ОС. Наприклад, системи MTD можуть спостерігати за сторонніми програмами, завантаженими з несхвалених джерел.

Системи MTD відстежують поведінку мобільних програм з ходу в поточному мобільному середовищі, наприклад, коли програма переходить до відомих шкідливих URL-адрес або фішингових сайтів. Наприклад, системи MTD можуть виявляти зв’язок із службою з блокованого списку або нездатність додатка зашифрувати зв’язок із серверною службою підприємства. Несподівана взаємодія між програмами або використання даних на пристрої користувача (наприклад, програма отримує доступ до контактів або місцезнаходження власника пристрою) також може попередити систему MTD про потенційно зловмисну або ризиковану поведінку [28].

Перевірка мобільних додатків. Метою перевірки програм (App Vetting) є виявлення недоліків у ПЗ чи конфігурації, які можуть створювати вразливості або порушувати політику безпеки/конфіденційності підприємства.

Система перевірки програм зазвичай використовується системними адміністраторами перед розгортанням програми на мобільному пристрої користувача, на відміну від системи MTD, яка може аналізувати завантажені та встановлені програми. Перевірку також можна використати для перевірки додатків, які встановлені користувачами поза управлінням адміністраторів.

Перевірка додатків включає послідовність дій, які зазвичай виконуються за допомогою автоматизованих інструментів тестування й аналізу, що можуть взаємодіяти із зовнішніми службами перевірки. Системи перевірки програм аналізують вихідний код програми, двійкові файли програми або загальну поведінку програми, виявляють критично важливі для безпеки проблеми, наприклад, пов’язані з використанням криптографії, збором і обробкою конфіденційних даних або залежністю ПЗ від ненадійних хмарних служб. Системи перевірки також можуть виявити, що програма збирає конфіденційні корпоративні дані або ідентифікаційну інформацію мобільного користувача.

Системи перевірки мобільних додатків можуть виявляти такі проблеми на кількох етапах життєвого циклу додатка: під час розробки, повідомляючи розробникам про проблеми й рекомендовані заходи протидії; перед розгортанням, визначаючи вразливості для аналітиків безпеки додатків або корпоративних системних адміністраторів; після розгортання через інтеграцію з EMM шляхом сповіщення про вразливості в установлених програмах [29].

Віртуальна мобільна інфраструктура. Віртуальна мобільна інфраструктура (Virtual Mobile Infrastructure, VMI) надає альтернативу або супровід технології EMM. Подібно до інфраструктури віртуального робочого столу (Virtual Desktop Infrastructure, VDI), яка містить образ віртуального робочого столу для програм і даних, VMI використовує серверну інфраструктуру для розміщення віртуального мобільного пристрою та мобільних програм. Потім

користувач отримує доступ до свого віртуального пристрою через програму на своєму телефоні, яка надає доступ до віртуальної ОС.

Цей підхід можна розглядати як «обхід» проблем конфіденційності даних шляхом зберігання конфіденційної інформації у зовнішній інфраструктурі, а не на самому мобільному пристрої. Оскільки вся корпоративна інформація буде доступна лише в інфраструктурі, розміщеній у хмарі, корпоративні дані, швидше за все, будуть недоступні, якщо немає підключення до мережі. Рішення VMI може бути розгорнуте також і на пристрої, уже підключеному до EMM.

Обгортання програми. Обгортання програм – це механізм безпеки, який змінює готовий до запуску мобільний виконуваний файл, щоб запобігти функціональності, визначеній мобільним адміністратором. Цей підхід часто розглядається як альтернатива використанню безпечного контейнера.

Обгортка дозволяє застосувати політики до програм сторонніх розробників, які не належать підприємству. Обгортання додатків зазвичай потребує адміністративного доступу до мобільного пристрою, а загорнуті додатки встановлюються на пристрій, не завантажуючись у рідний магазин додатків платформи і не перевіряються ним.

Щоб пом’якшити ці потенційні атаки, функцію зовнішнього завантаження слід вимкнути, якщо вона не використовується для встановлення упакованих програм. Використання упаковки додатків можна розглядати як вигідне з точки зору зручності, оскільки користувачі просто користуються програмами, як зазвичай. З точки зору IT-адміністратора, розгортання оновлень може бути проблематичним і вразливим до помилок.

Захищені контейнери. Захищені контейнери забезпечують програмну ізоляцію даних, призначену для сегментації корпоративних програм та інформації від особистих програм і даних. Контейнери можуть поєднувати кілька користувальницьких інтерфейсів, одним із найпоширеніших є мобільний додаток, який діє як портал до набору бізнес-додатків, таких як електронна пошта, контакти й календар.

Існує кілька архітектур захищених контейнерів, основними з яких є: програмні та ОС. Програмні контейнери можуть не зовсім відрізнятися від інших програм на мобільному пристрої, за винятком використання API управління, наданих розробником ОС. Наприклад, на більшості сучасних мобільних платформ будь-яка інформація, що зберігається в каталозі програми на пристрої, буде зашифрована за замовчанням. Більш розширена реалізація контейнера на рівні програми дозволяє управляти криптографічним ключем, який захищає контейнер. Контейнери на основі ОС забезпечують додаткову сегментацію й ізоляцію даних у порівнянні з контейнерами на основі програм [30].

2.3 Заходи протидії загрозам мобільній безпеці підприємства

Для запобігання і протидії загрозам мобільній безпеці підприємства доцільно застосовувати різноманітні заходи/засоби у комплексі або окремо. У таблиці 2.1 представлені основні загрози безпеці мобільних пристроїв, як корпоративних, так і особистих, які використовуються для виконання робочих завдань, а також заходи/засоби їх запобігання і протидії [12].

Таблиця 2.1

Загрози мобільній безпеці та заходи/засоби їх запобігання і протидії

Загрози	**Заходи/засоби запобігання і протидії**
Використання базових уразливостей пристроїв	– Вибір пристроїв, орієнтованих на безпеку – Ізоляція ОС і програм – Швидке прийняття оновлень ПЗ – Перевірка програм – Захист від мобільних загроз
Втрата або крадіжка пристрою	– Технології EMM – Політики безпеки мобільних пристроїв – Віддалене/захищене очищення пристрою – Сповіщення і скасування корпоративного доступу за порушення політики

	– Надійна автентифікація
Крадіжка облікових даних шляхом фішингу	– Навчання користувачів – Захист від мобільних загроз – Політики безпеки мобільних пристроїв – Надійна автентифікація (напр., багатофакторна) – Віддалене/безпечне стирання
Встановлення шкідливих профілів розробників і ЕММ	– Навчання користувачів – Перевірка додатків – Захист від мобільних загроз
Встановлення неавторизованих сертифікатів	– Мобільний захист від загроз
Доступ до корпоративних ресурсів через неправильно налаштований пристрій	– Технології ЕММ – Політики безпеки мобільних пристроїв – Сповіщення та відкликання корпоративного доступу за порушення політики
Використання ненадійних мобільних пристроїв	– Вибір пристроїв, орієнтованих на безпеку – Технології ЕММ – Захист від мобільних загроз – Сповіщення та скасування корпоративного доступу за порушення політики
Бездротове прослуховування	– Використання безпечних з’єднань з ресурсами (наприклад, VPN) – Захист від мобільних загроз
Зловмисне ПЗ для мобільних пристроїв	– Навчання користувачів – Вибір пристроїв, орієнтованих на безпеку – Швидке прийняття оновлень ПЗ – Перевірка програм – Ізоляція ОС і програм – Захист від мобільних загроз
Втрата інформації через незахищений екран блокування	– Технології ЕММ – Політики безпеки мобільних пристроїв – Навчання користувачів
Порушення конфіденційності користувачів	– Навчання користувачів – Технології ЕММ – Перевірка додатків
Втрата даних внаслідок синхронізації	– Технології ЕММ – Політики безпеки мобільних пристроїв – Навчання користувачів

Продовження табл. 2.1

Тіньове використання IT	– Політики безпеки мобільних пристроїв – Навчання користувачів
Використання вразливостей базової платформи EMM	– Рекомендовані практики кібербезпеки – Навчання користувачів
Крадіжка облікових даних адміністратора EMM	– Додаткова автентифікація для системних адміністраторів
Інсайдерська загроза	– Технології EMM – Політики безпеки мобільних пристроїв – Навчання користувачів

Основні заходи/засоби запобігання і протидії загрозам мобільній безпеці показані на рисунку 2.3.

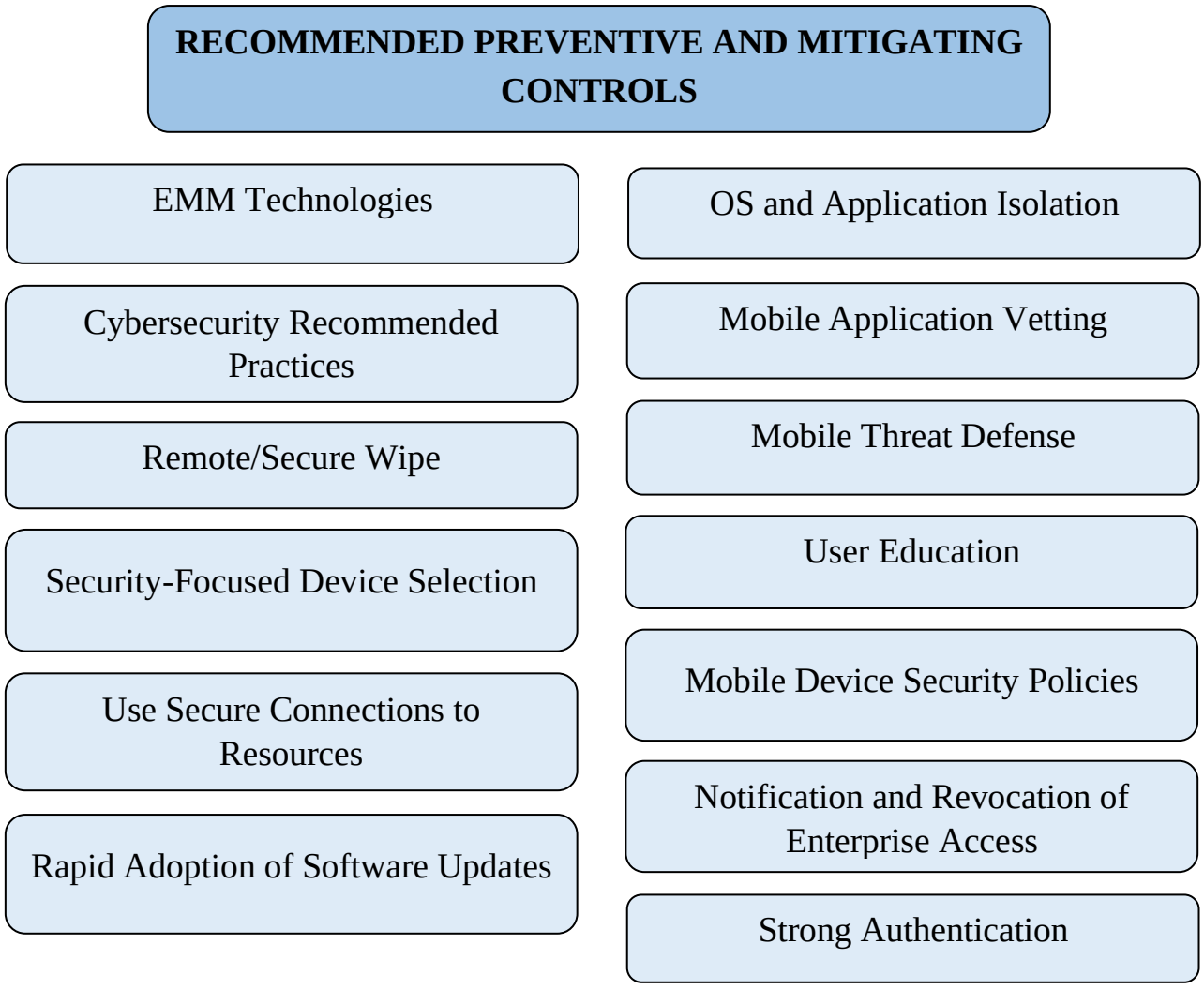

Рис. 2.3. Заходи /засоби запобігання і протидії загрозам мобільній безпеці

Розглянемо кожен із перелічених заходів/засобів детальніше.

Технології ЕММ. ЕММ і допоміжні технології можуть пом’якшити деякі загрози, поширені в мобільній екосистемі, зокрема:

– запобігти підключенню неправильно налаштованого пристрою до підприємства шляхом безпечного налаштування параметрів пристрою перед наданням доступу до корпоративних ресурсів;

– активно забороняти пристрою доступ до корпоративних даних, якщо він перебуває в незахищеному стані;

– стерти корпоративні дані на пристрої у разі втрати бо крадіжки пристрою;

– управляти інформацією, яка надана на екрані блокування пристрою тощо.

Залежно від можливостей ЕММ, список проблем, які можна пом’якшити, може бути набагато більшим, оскільки нерідко ЕММ використовують для управління та налаштування інших технологій, таких як програми MTD і VPN.

Рекомендовані практики кібербезпеки. ЕММ та інша інфраструктура управління мобільністю покладаються на готове комерційне ПЗ (Commercial off-the-shelf, COTS), яке створюється й надається сторонніми постачальниками [31], для виконання функцій управління. Ці базові системи часто працюють на основі ОС загального призначення та стандартного обладнання. Важливо, щоб рекомендовані практики безпеки, включаючи мережеву, фізичну та персональну безпеку, застосовувалися до цих компонентів так само, як вони застосовуються до загальних ІТ-систем у всій галузі.

Механізми захисту, такі як управління виправленнями (Patch Management) [32], управління конфігурацією (Configuration Management) [33] (наприклад, відключення послідовних портів на польовому мережевому обладнанні), управління ідентифікацією та доступом, виявлення шкідливих програм, а також системи виявлення та запобігання вторгнень, можна ретельно спланувати та впровадити по всьому підприємству.

Віддалене/безпечне стирання. Віддалене стирання дозволяє системним адміністраторам видаляти корпоративні дані та програми на мобільних пристроях, що належать підприємству або співробітникам (BYOD). Можливість віддаленого

стирання широко доступна на мобільних пристроях, таких як смартфони та планшети, які підтримують Android або iOS. Варіанти цієї функції також доступні для ОС і програм сторонніх розробників, які встановлюють на цих пристроях.

Щоб увімкнути віддалене стирання, системний адміністратор установлює й налаштовує профіль/агент на пристрої до того, як корпоративні дані або програми стануть доступними для використання. Щоб пізніше виконати віддалене стирання, корпоративний сервер видає команду стирання, яка надсилається через мережу, щоб наказати агенту пристрою EMM видалити дані та/або програми на пристрої. Статус пристрою на консолі EMM оновлюється після стирання, щоб адміністратор міг підтвердити, що стирання виконано.

Віддалене стирання може бути реалізовано на різних рівнях деталізації, починаючи від очищення всього пристрою (наприклад, видалення всього в розділі користувача системи; зазвичай цей рівень використовується для корпоративного пристрою) до корпоративного стирання (наприклад, видалення лише тих налаштувань пристрою, даних і програм, які раніше були надані користувачу для корпоративного використання; зазвичай цей рівень використовується для видалення робочих даних, які зберігаються на особистому пристрої працівника). Власні можливості віддаленого стирання для пристроїв iOS і Android вимагають, щоб пристрій був увімкнений (з достатнім зарядом) і підключений до мережі. Деякі сторонні системи EMM можуть виконувати віддалене стирання, навіть коли пристрій не підключено до мережі [12].

Організації не повинні розглядати віддалене стирання як єдиний засіб захисту конфіденційних даних, а використовувати його як один рівень багаторівневого підходу до захисту. Саме по собі віддалене стирання є принципово ненадійним засобом безпеки. Наприклад, зловмисник може отримати доступ до інформації на пристрої, перш ніж її буде стерто, або вимкнути пристрій, щоб запобігти отриманню сигналу віддаленого стирання.

Вибір пристрою, орієнтованого на безпеку. Відповідно до початкових налаштувань деякі пристрої можуть мати вбудовані вразливості або шкідливе ПЗ, мікропрограму чи апаратне забезпечення. Зловмисники, які мають доступ

до ланцюгів постачання обладнання, вбудованого ПЗ або додатків, можуть змінювати компоненти пристрою, вихідний код або виконувані файли на етапах проектування чи виробництва. Наприклад, хакер може маніпулювати засобами:

– розробки або інтеграції ПЗ (наприклад, компіляторами, системами тестування програмного забезпечення, системами управління конфігурацією);

– підтримки ПЗ (наприклад, системами оновлення або оновлення);

– адміністрування системи (наприклад, управління встановленням і випуском ПЗ, а також виправленнями);

– MDM, MAM або EMM.

Вибір перевірених пристроїв і ПЗ, а також використання перевіреного системного інтегратора вочевидь не може гарантувати уникнення цілеспрямованої атаки на ланцюг постачання однієї компанії чи групи осіб, але може допомогти зменшити ризик.

Організаціям доцільно використовувати списки перевірених продуктів і перевірених системних інтеграторів, щоб зменшити ризик придбання пристроїв або ПЗ із вбудованими вразливостями. На додаток до цих практик виробники пристроїв і ПЗ також мають дотримуватися відповідних галузевих рекомендацій щодо безпечної розробки програмного забезпечення [12].

Використання безпечного підключення до ресурсів. Шифрування даних під час їх передачі можна досягти за допомогою різних варіантів реалізації. Системні адміністратори розуміють, які дані шифруються, які алгоритми використовуються та як обидві сторони автентифікують один одного через VPN. VPN можуть не шифрувати всі дані, і компаніям потрібен час, щоб повністю зрозуміти, яка інформація справді захищена. Крім того, важливо знати, в які системи та географічний регіон надсилається корпоративна інформація [34].

Ризик від використання ненадійних мереж можна зменшити за допомогою надійних технологій шифрування, таких як VPN, для захисту конфіденційності та цілісності зв’язку, а також за допомогою механізмів взаємної автентифікації для перевірки ідентичності обох кінцевих точок перед

передачею даних. Використання довіреної VPN вимагає від організації належної перевірки безпеки постачальника послуг VPN та інфраструктури.

Іншим можливим засобом пом'якшення загроз є заборона використання незахищених мереж Wi-Fi, особливо тих, які використовують відомі вразливі протоколи. VPN забезпечують упевненість у тому, що всі схвалені підприємством програми на пристрої за замовчуванням покладаються на TLS і не можуть бути переведені на HTTP. Крім того, налаштування DNS для використання TLS може допомогти захистити конфіденційність запитів DNS.

Варто наголосити, що сьогодні доступ до корпоративних ресурсів вийшов за межі встановлення периметрів, які визначають безпечну зону та вільний діапазон доступу до ресурсів «всередині» підприємства. Організаціям слід розглянути інші технології, окрім VPN, щоб реалізувати архітектуру нульової довіри, яка забезпечує більш безпечне підключення до ресурсів. NIST SP 800-207, описує принципи нульової довіри, які слід враховувати, дозволяючи користувачам, пристроям і службам доступ до ресурсів підприємства [35].

Швидке впровадження оновлень програмного забезпечення. Розробники постійно вдосконалюють свої технології не тільки для забезпечення кращої функціональності, але й для виправлення програмних та інших помилок. Ці технологічні вдосконалення й виправлення безпеки є основною причиною для оновлення ПЗ і мікропрограм пристрою. Важливо, щоб мобільний пристрій отримував ці оновлення, інакше він залишатиметься у вразливому стані.

Ці оновлення зазвичай не виконуються автоматично, якщо пристрій належним чином не налаштований. Оновлення ПЗ часто розробляються та надаються користувачеві для ручного завантаження та встановлення на своєму пристрої. Оновлення слід розгортати швидко, оскільки чим довше мобільний пристрій уразливий до експлойтів, тим довше корпоративна й інша інформація є вразливою до компрометації.

ЕММ можуть сповіщати користувача про доступність оновлень ОС і програм. Якщо користувач не вносить відповідних оновлень, адміністратор може застосувати дії щодо забезпечення відповідності, зокрема блокування,

обмеження доступу до корпоративної інформації або її повне видалення на мобільному пристрої. Якщо управління програмами ввімкнено, EMM можуть вручну оновлювати програми та надсилати їх на мобільні пристрої.

Вносячи виправлення або оновлюючи ОС або програму, адміністратори мають врахувати багато проблем, які виникають у стандартних IT-середовищах: терміновість оновлення, ймовірність того, що оновлення «зламає» критично важливі функції для користувачів, а також здатність користувача, мобільного пристрою й уражених систем відкатувати невдалі виправлення.

На терміновість оновлення впливає серйозність потенційного впливу використання вразливості (наприклад, критична, важлива, помірна, низька). Наприклад, загальна система оцінки вразливостей (CVSS) - це числова система оцінки, яка використовується для передачі інформації про критичність вразливостей [36].

Оновлення програм для мобільних пристроїв можуть погано взаємодіяти з існуючим ПЗ корпоративної інфраструктури або прикладними програмами і призвести до того, що мобільний додаток або навіть увесь пристрій стане непридатним для використання.

Вибираючи вжиття коригувальних дій і вирішуючи, наскільки сильними мають бути такі дії, адміністратор підприємства повинен враховувати особливі фактори, які впливають на розгортання ПЗ в мобільному середовищі, зокрема пересування користувача, тривале перебування у режимі офлайн або підключення через мережі з низькою пропускною здатністю.

Рекомендації щодо оновлень для мобільних пристроїв включають періодичне надсилання оновлень, щоб привчити користувачів до регулярних виправлень і запобігти надмірному застаріванню програм; надсилання оновлень відносно толерантним користувачам (наприклад, системним адміністраторам) і тільки після цього виправлення решти мобільних пристроїв компанії. Використовуючи цей підхід, проблеми з оновленнями можуть бути виявлені та вирішені до того, як вони вплинуть на більшу кількість користувачів [37].

Ізолювання ОС і програм. Використання захищеного контейнера для ізоляції корпоративних даних є звичайною стратегією запобігання компрометації даних, яка використовує різноманітні базові технології для розділення даних підприємства та користувачів. Захищені контейнери часто діють як агент EMM на стороні пристрою, щоб отримати інформацію про працездатність пристрою, забезпечити дотримання політики підприємства та сповістити адміністраторів про невідповідність. Вони також можуть використовуватися для забезпечення криптографічного захисту конфіденційності даних. Діючи як агент EMM, захищені контейнери можуть працювати в поєднанні з API управлінням для виконання своїх функцій безпеки й управління.

Адміністратори також можуть налаштовувати політику, отримувати сповіщення про її порушення, запобігати викраденню даних та управляти справністю пристрою, вставляючи безпечний набір засобів розробки, утиліт і документації (Software Development Kit, SDK), орієнтований на безпеку, у програму, яка знаходиться на пристрої співробітника. Хоча цей підхід може бути плідним, він вимагає від підприємства певного рівня досвіду для розробки SDK. Інший підхід до ізоляції передбачає упаковування додатків. Усе це може працювати разом, щоб забезпечити бажаний ступінь ізоляції [38].

Підприємствам може знадобитися застосувати кілька механізмів ізоляції в рамках мобільного розгортання. Точна комбінація технологій є відображенням унікальних вимог до забезпечення безпеки і функціонування підприємства. Запровадження всіх перелічених механізмів ізоляції може бути неадекватною відповіддю на загрози, а також може бути занадто дорогим для впровадження на підприємстві. Тому керівництво компаній має добре розуміти, які переваги безпеки насправді забезпечує механізм ізоляції, а які функції є просто побічним продуктом основної ОС. Крім того, організації мають переконатися, що механізми ізоляції активовані та правильно налаштовані.

Перевірка мобільних додатків. Інструменти перевірки мобільних додатків (Mobile Application Vetting, MAV) використовують для виявлення вразливостей і шкідливого коду в мобільних додатках. Деякі мобільні платформи мають

вбудовані можливості MAV, що зобов’язує постачальників мобільних ОС забезпечувати багаторівневу модель безпеки.

Інструменти MAV також можуть інтегруватися з багатьма системами EMM і MTD. Коли виявляється проблема, адміністратор має бути належно поінформованим і автоматично розгортати різні дії з виправлення, доступні через EMM. Вони включають сповіщення адміністраторів, постраждалих користувачів і відділів; автоматичне видалення уражених програм; і заборону доступу до ресурсів підприємства.

Щоб досягти цієї автоматизованої операції, EMM інтегровано з інструментами MAV через API, які координують надсилання одноразових або групових мобільних додатків до служби MAV через інформаційну панель EMM. Ці API часто реалізуються за допомогою веб-служб. Для послуг MAV інтеграція EMM може створити гнучкий канал, через який результати від кількох постачальників MAV можна отримувати та зводити на інформаційній панелі або порталі EMM, не вимагаючи, щоб усі звіти про перевірку додатків відповідали одному формату [25, 27].

Мобільний захист від загроз. Система мобільного захисту від загроз MTD, також відома як Mobile Endpoint Detection and Response (EDR), може бути вбудована в ОС або працювати як окрема ізольована система, що виявляє шкідливі програми та інші загрози. Можливості, вбудовані в ОС, можуть бути недоступними для користувача пристрою або компанії.

Системи MTD можуть виявляти мережеві атаки таких видів:

– MitM, які перехоплюють, перенаправляють чи підслуховують комунікації;

– атаки на основі додатків, наприклад, витік інформації або шкідливі програми, завантажені ззовні;

– атаки на основі платформи, наприклад, руткіти;

– фішингові атаки, що мають на меті викрадення облікових даних, тощо.

У поєднанні з інтегрованим EMM ці системи пропонують кілька підходів до виправлення після спроби атаки, виявленого порушення даних або

скомпрометованого пристрою. Усунення мережевих атак включає відключення пристрою від корпоративної мережі, відновлення надійного з'єднання або блокування спроб підключення до заблокованих мереж. Усунення загрози має виконуватися на пристрої, щоб швидко пом'якшити загрозу й усунути залежність від підключення до мережі/хмари для доступу до дій політики усунення.

Для атак на основі програм інтегрована система EMM і MTD може видаляти шкідливі програми або змінювати дозволи програм, щоб обмежити доступ до конфіденційних корпоративних ресурсів. У випадках, коли інтегрована система EMM і MTD виявляє потенційну атаку на мобільну платформу, вона сповіщає користувача про необхідність застосувати виправлення ОС або, принаймні, дистанційно стерти, тобто скинути заводські налаштування пристрою. Інтегровані системи EMM і MTD зазвичай налаштовані для сповіщення системного адміністратора та користувача мобільного пристрою про виявлену проблему та запущений підхід до її усунення [25, 28].

Навчання користувачів. Говорячи про безпеку, варто пам'ятати що користувач не може покладатися виключно на EMM та інші програми сторонніх розробників для захисту свого пристрою та корпоративних даних. Важливою є обізнаність користувача пристрою, оскільки саме він відіграє центральну роль у забезпеченні безпеки. Розуміння важливості захисту пристрою і способів сприяння цій безпеці важливо як для користувача, так і для підприємства.

Навчання користувачів щодо захисту мобільних пристроїв передбачає формування розуміння важливості механізмів безпеки та способів їх застосування, постійні нагадування про заходи безпеки за допомогою вивісок, проведення інформаційних заходів і роздачі тематично оформлених предметів.

Тематика інформування користувачів мобільних пристроїв має, зокрема, охоплювати питання: ознаки і виявлення фішингових атак; управління обліковими даними автентифікації; політика конфіденційності підприємства й персональних даних; виявлення шкідливих профілів EMM або інших шкідливих програм; вимоги щодо встановлення програм лише з перевірених джерел; вимоги щодо швидкого оновлення ОС і програм.

Якщо користувачі пристроїв не навчені належним чином захищати свої мобільні пристрої, це може поставити під загрозу інформацію підприємства та користувачів. Адміністратори мобільних пристроїв і EMM також потребують належної підготовки з безпеки.

Підприємству доцільно визначити категорії працівників і спеціалізовані сфери з Національної ініціативи з освіти кібербезпеки [39], і розробити програму навчання на основі підходу, який передбачає групування працівників з однаковими ролями і повноваженнями, а потім надання їм необхідного пакету знань, формування вмінь і навичок з мобільної безпеки.

Політики безпеки мобільних пристроїв. Розробка політик безпеки має життєво важливе значення для створення міцної позиції безпеки через чітко визначені процедури та методи управління. Мета політик безпеки полягає в тому, щоб забезпечити чіткий план дій компанії під час розгортання нових технологій і усунення проблем безпеки. Політики безпеки мобільних пристроїв можна встановити, здійснивши моделювання загроз або оцінку ризиків відповідно до конкретних потреб підприємства в безпеці.

Політики безпеки мобільних пристроїв мають охоплювати різноманітні аспекти, зокрема право власності на пристрій, управління пристроями, доступ до пристроїв, безпека і використання пристрою. Наприклад, організації можуть використовувати системи MDM або MAM, щоб налаштовувати й контролювати свої пристрої, а також вимагати паролі, біометричні дані, VPN або сертифікати для автентифікації та шифрування. Крім того, для безпеки пристрою може знадобитися антивірусне ПЗ, брандмауери, резервне копіювання, віддалене стирання і блокування екрана. Нарешті, слід пам’ятати про використання публічних Wi-Fi, завантаження програм, спільний доступ до пристроїв або звітування про інциденти як частину політики використання пристроїв [40]. Важливим є розробка процедури перегляду й оновлення політик, особливо якщо є порушення через впровадження слабкої або застарілої політики.

Оповіщення і скасування корпоративного доступу. На кожному підприємстві мають бути розроблені і впроваджені політики і правила безпеки,

які впливатимуть на дії з усунення проблем у разі мережевих атак або зламів, а також порушень безпеки мобільних пристроїв. Дії з усунення негативних наслідків можуть охоплювати низку можливостей, починаючи зі сповіщень окремих користувачів або груп користувачів, яких це стосується, до скасування доступу до корпоративних даних і служб, видалення даних уражених пристроїв або відновлення їх до початкового стану за замовчуванням.

Повідомлення користувачів про проблему часто є найпростішим і найменш агресивним варіантом усунення. Зазвичай це робиться за допомогою push-повідомлень у центр сповіщень телефону або SMS для подальшої відповіді.

Тимчасове скасування доступу до корпоративних ресурсів розглядається як наступний крок, якщо сповіщення не вирішує проблему. Найпростіше це зробити за допомогою агента EMM, якщо його встановлено на пристрої працівника. Тимчасове відкликання може тривати заздалегідь визначений період часу (наприклад, 24 години), і доступ може бути відновлений автоматично або вручну системними адміністраторами [12].

Видалення додатків або очищення мобільного пристрою є одними з більш агресивних варіантів виправлення, доступних підприємству. Ці більш рішучі дії можуть бути вжиті, якщо мобільний додаток був зламаний, інфікований і став джерелом атак або витоків, які впливають на підприємство.

Надійна автентифікація. Системні адміністратори, які використовують консоль EMM, мають доступ до конфіденційної інформації про мобільні пристрої підприємства. Особи з обліковими даними EMM можуть надавати і скасовувати доступ до корпоративних ресурсів і збирати особисту інформацію про працівників, зокрема місцезнаходження пристрою. Крім того, вони можуть очистити весь пристрій, а не лише корпоративні дані. З цієї причини облікові дані адміністратора EMM мають відповідати стандартним правилам надійності та складності пароля, наведеним у NIST SP 800-63-3 [41]. Якщо підтримується EMM, також слід використовувати багатофакторну автентифікацію, що допоможе запобігти крадіжці облікових даних EMM.

Висновки до розділу 2

Дослідження показало, що за останнє десятиліття технології мобільної безпеки стали повнофункціональними комплексами управління безпекою, а для поглиблення керованості корпоративних мобільних пристроїв додаються нові можливості й функції.

Технології мобільної безпеки поділяють на два види: технології управління й безпеки на стороні пристрою і технології мобільної безпеки підприємства. Технології управління та безпеки на боці пристрою охоплюють такі засоби: апаратну підтримку обробки та зберігання даних; механізми ізоляції даних; прикладний програмний інтерфейс управління платформою API; підтримку захищених мереж VPN; механізми автентифікації.

З'ясовано, що технології мобільної безпеки підприємства включають: управління корпоративною мобільністю EMM; управління мобільними додатками MAM; захист від мобільних загроз MTD; перевірку мобільних додатків; віртуальну мобільну інфраструктуру; обгортання програм і захищені контейнери. Саме перелічені засоби мобільної безпеки є основою для запобігання і протидії загрозам мобільним пристроям.

Для запобігання і протидії загрозам мобільній безпеці підприємства доцільно застосовувати різноманітні заходи і засоби у комплексі або окремо. Аналіз показав, що основними управлінськими заходами і програмно-апаратними засобами пом'якшення загроз мобільній безпеці є: технології EMM; впровадження кращих практик кібербезпеки; віддалене безпечне очищення; вибір пристрою, орієнтованого на безпеку; безпечне підключення до ресурсів; швидке здійснення оновлень ПЗ; ізоляція ОС і програм; перевірка мобільних додатків; мобільний захист від загроз; навчання користувачів; політики безпеки мобільних пристроїв; оповіщення і скасування доступу; надійна автентифікація.

РОЗДІЛ 3.
РОЗГОРТАННЯ Й УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ ВІДПОВІДНО ДО ЇХ ЖИТТЄВОГО ЦИКЛУ

Під час розгортання мобільних пристроїв у корпоративному середовищі слід враховувати багато факторів, зокрема вибір прийнятних технологій і засобів управління, а також належне надання їх користувачам.

Експертною спільнотою розроблені декілька моделей процесів управління мобільним середовищем, які підприємства можуть прийняти або поєднати у відповідності до їхнім потреб і вимог. Одним із прикладів є концепція прийняття рішень у сфері мобільних обчислень (Mobile Computing Decision Framework, MCDF) від Ради директорів з інформаційної безпеки (CIO), американського міжвідомчого форуму для вдосконалення практик проектування, придбання, розробки, модернізації, використання, і забезпечення продуктивності федеральних інформаційних ресурсів [42].

MCDF є комплексним процесом, який допомагає компаніям вибрати відповідне рішення для мобільних обчислень і охоплює чотири ключові етапи [43] (Рис. 3.1):

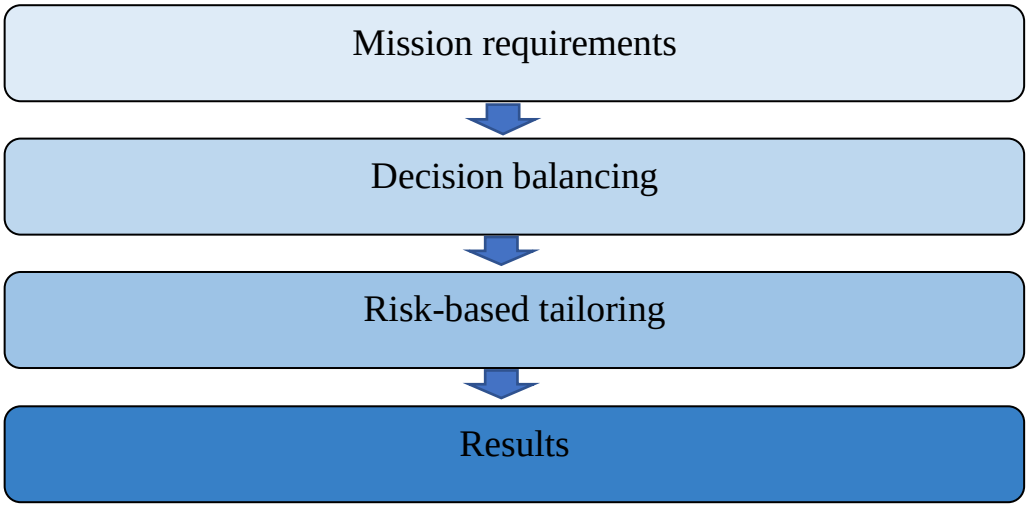

Рис. 3.1. Концепція прийняття рішень у сфері мобільних обчислень (MCDF)

1. Вимоги місії: оцінювання відповідності наявних мобільних технологій місії підприємства з урахуванням користувачів, джерел інформації та необхідних місць розміщення потужностей.

2. Збалансування рішень: аналіз можливостей компанії, вимог безпеки, економічних і фінансових аспектів у їх взаємозв'язку і взаємозалежності.

3. Адаптація на основі ризик-орієнтованого підходу: застосування системи управління ризиками для оцінки юридичних, регуляторних, політичних, конфіденційних і технічних ризиків безпеці мобільним пристроям.

4. Прогнозування результатів: визначення переліку програм, мобільних пристроїв і компонентів інфраструктури, які підлягають, виходячи з вимог місії компанії та результатів аналізу ризиків.

Відповідно до концепції NIST процес розгортання й управління мобільними пристроями протягом їх життєвого циклу включає такі етапи:

- визначення вимог до мобільних пристроїв;
- здійснення оцінювання ризиків;
- впровадження корпоративної стратегії мобільної безпеки;
- експлуатація і підтримка функціонування;
- утилізація та/або повторне використання пристроїв (Рис. 3.2) [12].

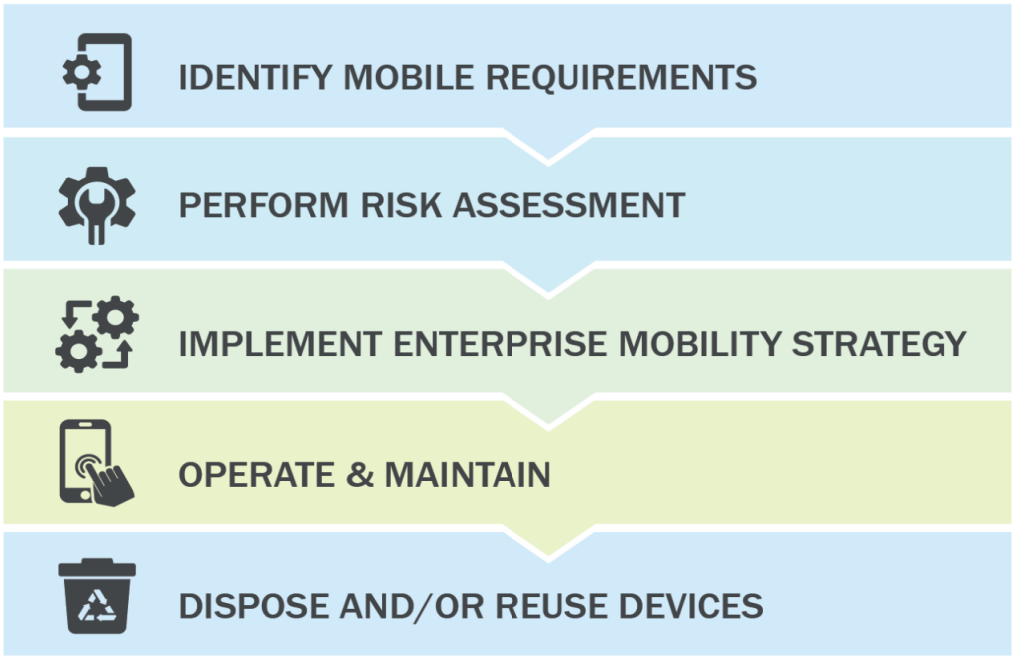

Рис. 3.2. Життєвий цикл розгортання корпоративного мобільного пристрою

3.1 Визначення вимог до мобільних пристроїв

На першому етапі життєвого циклу мобільних пристроїв відповідальні керівники підприємства визначають потреби вимоги до мобільних пристроїв для досягнення корпоративних цілей, проводять інвентаризацію мобільних пристроїв, які вже використовуються, і визначають модель розгортання мобільного середовища, яка підходить компанії.

Це все для того, щоб сформулювати вимоги до управління наявними і майбутніми мобільними пристроями у відповідності з місією компанії та її потребами щодо функціональності, безпеки та конфіденційності. У вирішенні цих завдань беруть участь як посадові особи, які представляють сферу корпоративних IT, так і менеджери основних бізнес-процесів. Таким чином буде забезпечено, що вибір технологій на наступних етапах буде здійснюватися з урахуванням вимог щодо досягнення цілей та місії організації.

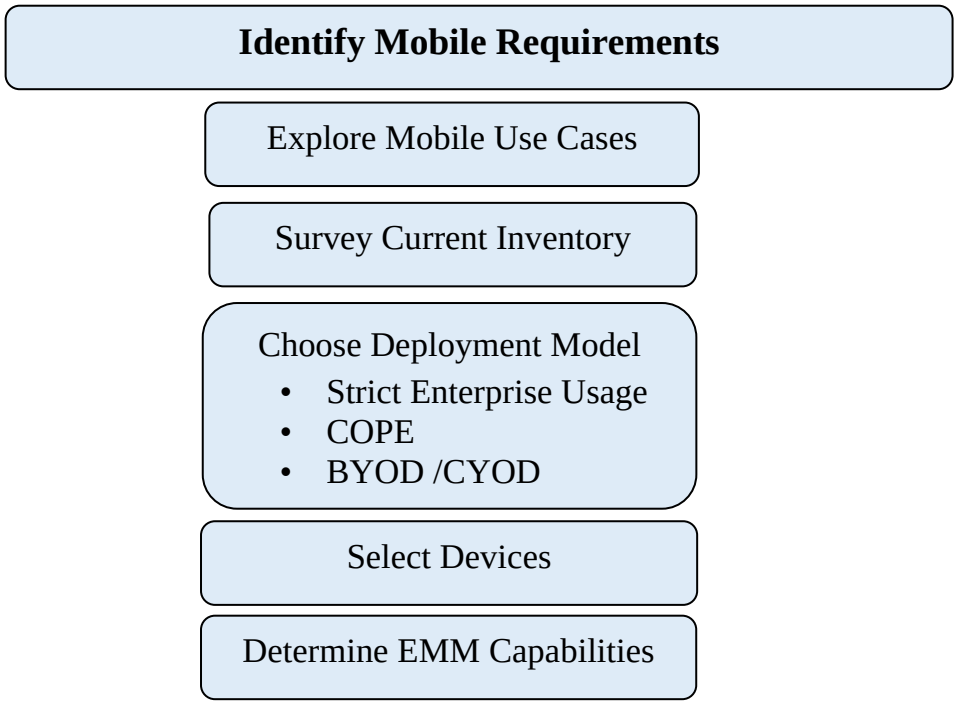

Рис. 3.3. Послідовність дій із визначення вимог до мобільних пристроїв

Вивчення зразків використання мобільних пристроїв. Багато компаній вважають, що мобільні пристрої мають важливе значення для того, щоб їхній персонал міг відповідати динамічним бізнес-вимогам. Для того, щоб завдання,

які раніше могли набагато повільніше виконуватися в офісі, тепер вирішуються «в польових умовах», потрібен доступ до корпоративних даних або додатків і налагоджена взаємодія з колегами і партнерськими організаціями.

Поряд із завданням забезпечення відповідності складним і швидким бізнес-вимогам підприємство має належним чином захищати конфіденційні дані і вирішувати проблеми конфіденційності, фінансових і репутаційних витрат тощо. Вивчення конкретних зразків використання мобільних пристроїв для потреб компанії сприяє визначенню та чіткому опису вимог до розгортання мобільного середовища. Загальні елементи сценаріїв використання включають розуміння того, хто є користувачами, навіщо їм потрібні мобільні пристрої та які програми і функції пристроїв необхідні для досягнення цілей підприємства.

Наприклад, організація з ліквідації наслідків аварій критичної інфраструктури направляє своїх фахівців на підприємства, які постраждали від кібератак або диверсій, спрямованих проти ІТКС, щоб оцінити наслідки й надати допомогу з відновлення потужностей. За таких обставин мобільні пристрої мають важливе значення для зв’язку з корпоративними джерелами даних і надсилання інформації, зібраної на місці. Персонал також може ділитися інформацією з представниками громадськості, місцевими аварійними службами, представниками інших місцевих і державних установ, неурядових організацій.

При вивченні кращих зразків розгортання мобільних пристроїв беруть до уваги аспекти можливої реструктуризації, налаштування необхідних характеристик безпеки (доступність, працездатність), а також урахувати вартість вибраних мобільних пристроїв, щоб переконатися, що весь персонал має необхідне обладнання, яке може забезпечити виконання професійних завдань.

Огляд поточного обладнання. Коли сучасні мобільні пристрої вперше з’явилися на підприємствах, платформи управління були менш зрілими і, зазвичай, без централізованого управління. Тому огляд та інвентаризація мобільних систем поряд з іншими ІС в мережі компанії є доцільною під час розгортання нової мобільної інфраструктури. Варто опитати усіх співробітників щодо мобільних пристроїв, якими вони користуються для виконання робочих

завдань, а також здійснити сканування мережі, щоб виявити пристрої в мережі. Разом ці два джерела інформації дають уявлення про пристрої, які фактично використовуються та потребують захисту або оновлення.

Важливо є виявити всі невідомі мобільні пристрої, які можуть залишити прогалини в інфраструктурі підприємства. Не отримавши необхідних налаштувань безпеки, ці пристрої є потенційними джерелами загроз для їхніх користувачів і підприємства загалом. Проникнення зловмисного ПЗ або несанкціонований доступ до мережі підприємства через неідентифікований мобільний пристрій може мати наслідком, що компанія навіть не буде знати про вразливі атаки через відсутність видимості. Виявлення поточних мобільних активів може здійснюватися за допомогою методології управління активами [44].

Вибір моделі розгортання. Керівники можуть вибирати з багатьох моделей розгортання мобільних пристроїв, які будуть використовуватися на їхньому підприємстві. Модель розгортання фіксує альтернативні варіанти відповідальності за конкретний пристрій, а також політику й технологічні елементи управління пристроєм. Вибір варіантів ранжується від пристроїв, придбаних і повністю керованих підприємством, до пристроїв, що належать працівникам, які не майже або взагалі не взаємодіють з корпоративними системами. При виборі моделі розгортання мобільного середовища необхідно враховувати пристрої, що використовуються для дистанційної роботи, віддаленого доступу та власні пристрої працівників, які використовуються в роботі за принципом BYOD [45].

Обмежене використання мобільних пристроїв підприємства. Корпоративні мобільні пристрої належать компанії, і всі користувачі повинні знати, що вся інформація та дані на цих пристроях нею контролюються, а самі пристрої надаються працівникам тільки для корпоративного використання. Особисте використання корпоративних пристроїв суворо обмежується, а для особистих потреб працівники носять окремий персональний пристрій.

Корпоративні мобільні пристрої забезпечують значні переваги безпеки. У такому випадку підприємство може відстежити ланцюжок постачання

потенційних пристроїв, перш ніж вибрати пристрої для покупки, а системні адміністратори IT можуть розробити плани посилення пристроїв до надходження продуктів. Під час розгортання IT-спеціалісти можуть налаштувати обмежувальні параметри політики, щоб суттєво змінити функціональність пристрою, наприклад, видалити функцію обміну текстовими повідомленнями, обмежити доступ Wi-Fi і Bluetooth і забезпечити, щоб зв'язок відбувався через VPN. При розгортанні корпоративних мобільних пристроїв компроміси між безпекою та зручністю використання можуть здійснюватися виключно на розсуд керівників компанії.

Прикладом розгортання виключно для підприємства може слугувати модель GFE (Government-furnished equipment), яка надається кінцевому користувачеві на час дії контракту або період виконання певних повноважень як повністю керований або контрольований пристрій [46]. Технології мобільної безпеки включають реєстрацію пристрою в MDM з використанням MTD для захисту кінцевих точок і доступу до корпоративних ресурсів через веб-інтерфейси або мобільні програми.

Підхід білого списку реалізується для розгортання мобільних додатків, а всі мобільні програми на пристрої перевіряються за допомогою служби перевірки мобільних програм, перш ніж програми будуть надані на пристрій або дозволено завантажувати з керованого корпоративного магазину програм [28]. У цій моделі розгортання доступ до офіційних загальнодоступних або неофіційних магазинів програм обмежено.

Використання персоналом пристроїв підприємства, в т.ч. в особистих цілях (Corporate-Owned Personal Enabled, COPE). Пристрої типу COPE надає компанія, але співробітники можуть використовувати їх також і в особистих цілях. Такий сценарій може бути реалізований через механізм device owner з м'якими політиками або через робочий профіль [47].

Незважаючи на те, що підприємство володіє (або орендує) пристрій і накладає обмеження на його використання персоналом, ці обмеження є більш м'якими, дозволяючи працівникам певну свободу особистого використання

пристрою. Наприклад, працівнику може бути дозволено завантажувати певні програми або отримувати особисті текстові повідомлення на пристрій COPE. Незважаючи на те, що пристрій COPE активовано особисто, сам пристрій і інформація на ньому належать підприємству. Співробітників інформують про корпоративні обмеження та вимоги щодо конфігурацій ПЗ і пристроїв, які впливають на функціональність і конфіденційність.

Прикладом моделі розгортання COPE є керований пристрій GFE. Це може включати повністю контрольований пристрій або окрему реєстрацію для управління пристроєм шляхом завантаження програми EMM з офіційного магазину програм. MTD використовується для захисту кінцевих точок, а для багатьох розгортань COPE реалізовано підхід до блокування.

У рамках моделі COPE персональні програми дозволені на пристрої GFE, і кінцевий користувач має доступ до офіційних загальнодоступних магазинів програм, але використання програм може бути обмежено корпоративним списком блокування. Усі мобільні додатки на пристрої повинні пройти службу перевірки мобільних додатків, завантажені на пристрій програми перевіряються службою перевірки програм під час або після інсталяції, а також зберігаються у списку блокування програм.

Моделі використання персоналом власних мобільних пристроїв BYOD і CYOD. Модель BYOD дозволяє працівникам використовувати свої особисті мобільні пристрої для доступу до корпоративних даних і послуг. У такому випадку працівник може, наприклад, отримати доступ як до особистої електронної пошти, так і до конфіденційної корпоративної електронної пошти через одну програму.

Модель BYOD викликає занепокоєння щодо витоку конфіденційної корпоративної інформації через пристрій до ненадійних сторонніх серверних систем, які контактують з різними програмами на пристрої. Щоб захистити конфіденційність і цілісність корпоративних даних і систем, а також конфіденційність користувача/власника пристрою, IT-спеціалісти можуть використовувати такі інструменти як EMM, щоб запобігати несанкціонованим

діям користувача, застосовуючи обмеження щодо відключення функції копіювання/вставлення на корпоративних програмах. Підприємство також має використовувати технологію MTD, щоб захистити пристрій від мобільних загроз і спроб компрометації [48].

Модель типу «Вибери свій власний пристрій» (Choose Your Own Device, CYOD) передбачає придбання пристрою працівником для особистого користування, але вибирається зі списку пристроїв, наданих підприємством для взаємодії з корпоративними мережами та програмним забезпеченням. Якщо особистий пристрій працівника входить до списку схвалених і він інсталює ПЗ, необхідне підприємству, тоді цей пристрій використовується для доступу до корпоративних даних і послуг. Співробітники з особистими пристроями, яких немає в затвердженому списку, носять інший (корпоративний) пристрій для виконання робочих завдань. Таким чином вибір пристрою із списку дозволяє персоналу уникнути носіння додаткового гаджета.

Проблемою використання пристроїв BYOD і CYOD є відсутність можливостей управління ланцюгом поставок. Підприємство практично нічого не знає про походження пристрою та його модифікацію. Пристрій BYOD/CYOD може бути розблокований або зламаний із використанням встановлених ненадійних програм, заражений шкідливим ПЗ без відома користувача. Відсутність базової інформації про пристрій ставить під загрозу корпоративні дані, оскільки користувач може отримати доступ до них через свій пристрій.

Для підприємства CYOD пропонує можливість обмежити ризик ланцюга постачання пристроїв і контролювати доступ до корпоративних даних і серверних систем за допомогою захисного ПЗ (наприклад, EMM або MTD).

Перевага CYOD над BYOD полягає в тому, що працівників заздалегідь інформують про пристрої, на яких можна запускати необхідне захисне ПЗ, і, таким чином, їм буде дозволено доступ до корпоративних ресурсів. Коли IT-спеціалісти відмовляються надати дозвіл на використання пристрою BYOD через те, що на ньому не можна запустити корпоративну програму EMM, тоді BYOD фактично зрівнюється в можливостях із CYOD [49, 50].

Вибір пристроїв. Особливості бізнес-цілей компанії й такі обмеження як вартість і моделі розгортання, враховуються при виборі мобільних пристроїв. Розуміння впливу мобільних пристроїв на виконання бізнес-завдань може допомогти зосередити процес відбору, звузивши його до невеликого набору пристроїв, які задовольняють вимоги підприємства.

Витрати й питання безпеки мобільних пристроїв можуть вплинути на рішення про придбання таких продуктів. Витрати можна мінімізувати, обмеживши розгортання пристроїв лише користувачами, яким вони потрібні для підтримки цілей підприємства, й обравши пристрої лише з очікуваними функціями. З міркувань безпеки важливо вибирати моделі пристроїв, які є достатньо актуальними, щоб вони підтримувалися виробником і могли підтримувати оновлення та виправлення ОС і програм.

Визначення можливостей ЕММ. Визначення можливостей ЕММ, необхідних для ефективного їх застосування на підприємстві, є важливою діяльністю, яку виконують перед придбанням ЕММ-рішень. Як відзначалося, керівники компанії мають попередньо проаналізувати поточний стан корпоративного мобільного середовища.

Іншим варіантом є інтеграція інфраструктури ЕММ в інфраструктуру підприємства. Ці параметри включають «попередні» операції (тобто роботу на серверах, розміщених локально в корпоративному центрі обробки даних), підтримку моделі ПЗ як послуги (SaaS) або сертифікацію/акредитацію продуктів та інтеграцію сторонніх служб. Також є багато інших важливих можливостей для ЕММ та інших корпоративних технологій, призначених для підтримки мобільних обчислень підприємства. Список необхідних можливостей ЕММ підтримуватиме обґрунтований вибір ЕММ для підприємства, гарантуючи, що він забезпечує необхідні функціональні й безпекові можливості [12].

3.2 Оцінювання ризиків і впровадження стратегії корпоративної мобільності

Процес оцінювання ризиків є основоположним компонентом кібербезпеки і використовується для ідентифікації, оцінки та визначення пріоритетності ризиків корпоративним операціям і активам, персоналу та іншим організаціям, які є результатом роботи й використання інформаційних систем. Оцінювання ризиків проводять періодично, оскільки ландшафт загроз постійно змінюється, а системи, які потрібно захистити, розвиваються. Регулярні аудити безпеки оцінюють ефективність засобів управління для захисту підприємства.

Оцінювання ризиків можна проводити на рівні підприємства, бізнес-цілей або інформаційної системи. Усі мобільні пристрої, мобільні програми та будь-які системи, що використовуються для управління мобільною системою, мають бути залучені до процесу оцінювання ризиків. Об’єктом оцінювання ризиків може бути певна група мобільних пристроїв або конкретне розгортання мобільного пристрою.

Існують різноманітні методології оцінювання ризиків, наприклад Настанови щодо проведення оцінювання ризиків від NIST [51] і концепція MCDF [43]. Також розроблені інструкції для мобільних пристроїв щодо виконання оцінки ризиків, наприклад проект NISTIR 8144 [52], який використовується разом із процесом моделювання загроз, таким як проект NIST SP 800-154 [53] і концепцією MITRE щодо зловмисних тактик і методів ATT&CK [54].

Компанії, які не проводять оцінювання ризиків, можуть необґрунтовано вибрати й застосувати неприйнятні, неефективні засоби управління безпекою або витратити занадто багато ресурсів на обробку одних ризиків і недостатньо - на інші. Підприємствам рекомендується переглядати встановлені вимоги після оцінювання ризиків, щоб оновити їх з урахуванням отриманих результатів.

Впровадження стратегії корпоративної мобільності. Рішення щодо варіантів мобільного розгортання, пристроїв і систем управління мобільним середовищем компанії приймаються на основі аналізу наявності ресурсів, бізнес-потреб та інших корпоративних обмежень.

Типові етапи впровадження стратегії корпоративної мобільності показані на рисунку 3.5 [12].

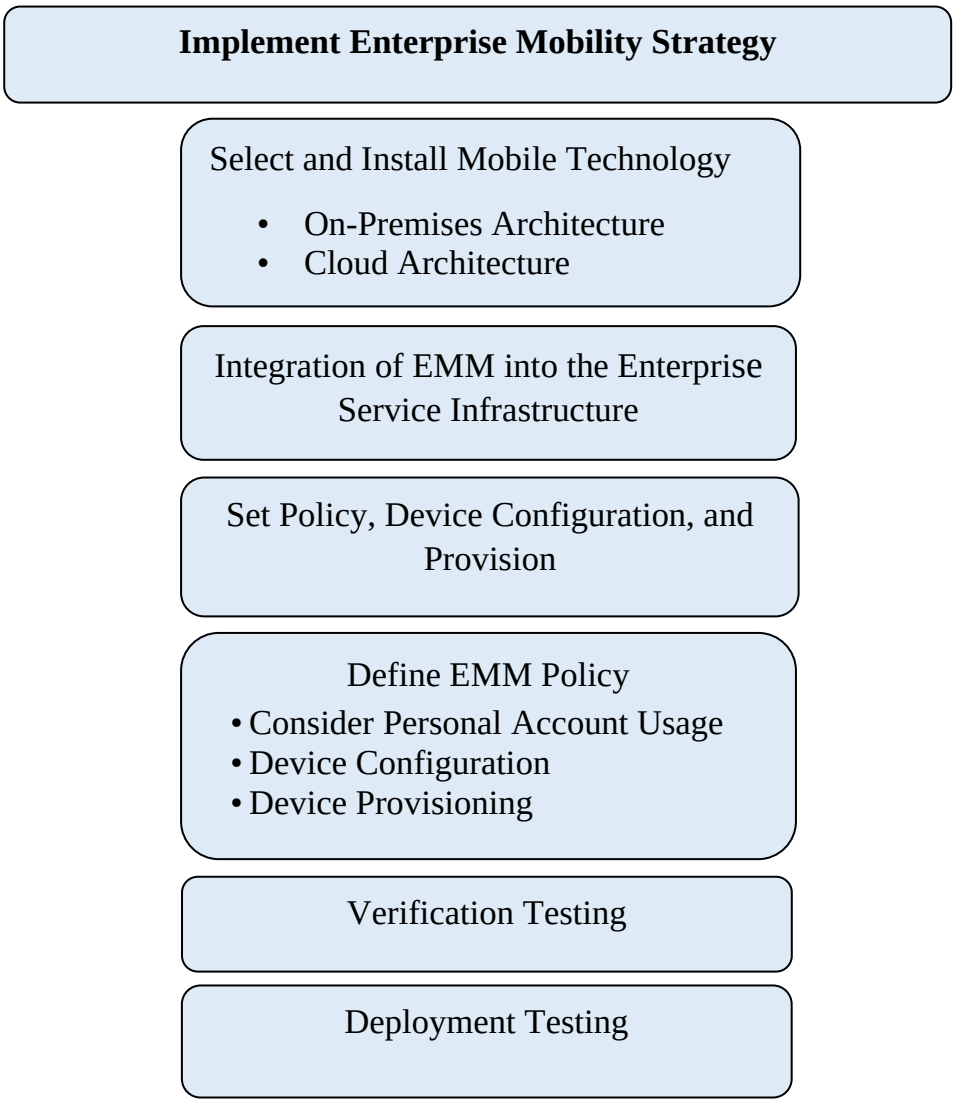

Рис. 3.5. Послідовність дій із впровадження стратегії мобільності

Компанії самі обирають варіанти управління корпоративними мобільними пристроями. Підприємство може мати повний контроль над усіма компонентами корпоративного середовища, тому все мобільне обладнання закуповується компанією й управляється системними адміністраторами через EMM. EMM є класом програмних засобів, що підтримують можливість використання мобільних пристроїв у корпоративних ділових процесах, яке реалізується за

допомогою інтеграції цих апаратних засобів в IT-системи і середовище безпеки на всіх етапах управління життєвим циклом IT [55].

Також можна обрати варіант санкціонованого використання персоналом власних мобільних пристроїв (можливо, зі схваленого списку) для виконання бізнес-завдань. У такому випадку компанія дозволяє працівникам приносити власні пристрої, залишаючи за собою функції управління кількома корпоративними програмами через систему MAM. Отже, керівництво приймає рішення, звужуючи діапазон відповідних варіантів розгортання до найбільш прийнятного варіанту.

Вибір і встановлення мобільних технологій. Для вибору найбільш прийнятних технологій необхідно перелік вимог до мобільних технологій, визначений раніше, порівняти з вимогами EMM. Може не бути ідеального збігу з повним перекриттям вимог і можливостей, особливо коли вибір EMM має здійснюватися з попередньо визначеного списку, який належить зовнішній організації.

Після вибору EMM має бути належним чином реалізовано в межах корпоративної мережі. Це включає правильну конфігурацію продукту, що є ще одним важливим кроком у захисті мобільної інфраструктури підприємства. Неправильно налаштоване рішення EMM може призвести до витоку конфіденційної та службової інформації підприємства, яка може включати власні розроблені внутрішні мобільні програми, дані про персонал і дані, які містять комерційну таємницю.

Адаптований до потреб компанії варіант технології EMM може бути налаштований у різний спосіб і з різною архітектурою. Двома основними методами розташування EMM і пов’язаних технологій є локальні та хмарні. Останні часто називають моделлю SaaS.

Локальна архітектура EMM. Локальні (on-premise) види технології EMM менш поширені, ніж хмарні. У такому разі підприємства самостійно встановлюють і налаштовують EMM, а також оплачують ліцензії на ПЗ для будь-яких базових платформ або компонентів. Деякі постачальники EMM

пропонують зображення та контейнери, які можуть полегшити навантаження щодо їх встановлення та налаштування. Компаніям-споживачам таких рішень рекомендується ретельно перевірити зображення або контейнери на наявність типових уразливостей ПЗ.

Основна перевага цієї моделі полягає в тому, що дані технології зберігаються в компанії, за винятком дозволених пристроїв, які можуть запитувати й отримувати інформацію ззовні. Також компанії можуть відстежувати такий трафік від EMM до інших пристроїв разом із автентифікацією і забезпечити фізичну безпеку EMM.

Нижче наведено зразок архітектури, який демонструє локальну реалізацію технологій мобільної безпеки. Технології MTD зазвичай базуються на хмарі, навіть якщо технологія управління підприємством є локальною. На рис. 3.6 показано MTD як частину хмари, хоча розгортання на практиці може значно відрізнятися.

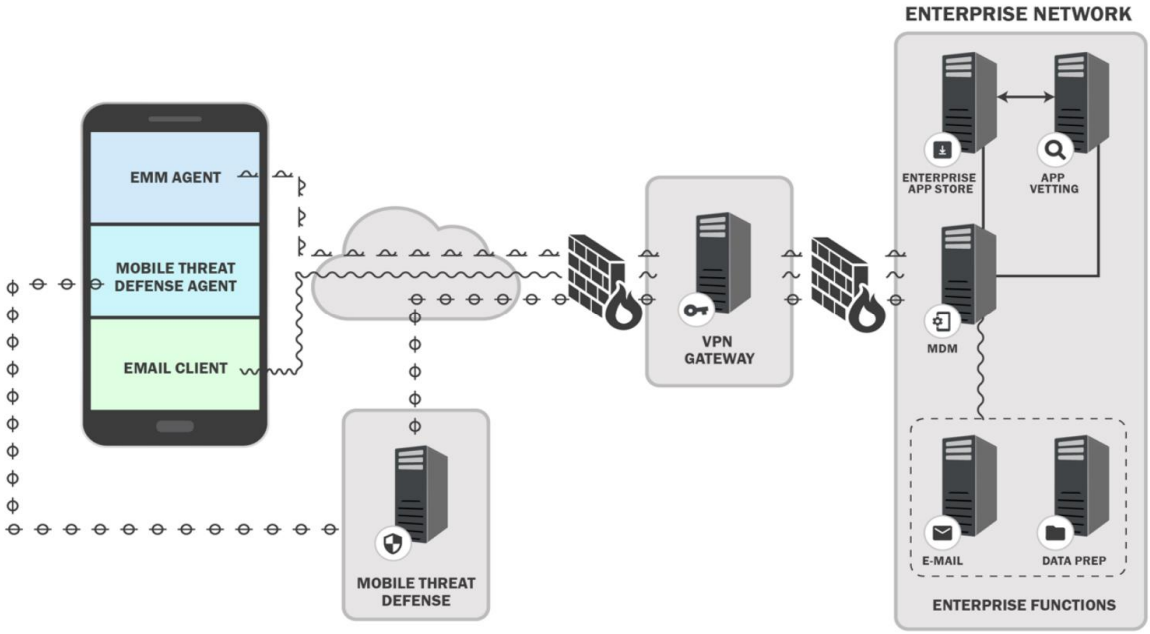

Рис. 3.6. Приклад локальної мобільної архітектури

Компоненти EMM розміщуються на локальних серверах, якими володіє й управляє підприємство. Ця архітектура вимагає прискіпливої уваги до встановлення й обслуговування технологій підприємством, але також забезпечує більший корпоративний контроль над процесом управління й передавання даних.

Хмарна архітектура. Альтернативою локальній архітектурі є хмарне рішення, яке дозволяє розміщувати технології мобільної безпеки за межами локальної корпоративної мережі (Рис. 3.7). При використанні хмарного рішення постачальник технологій мобільної безпеки надає підприємству можливість використовувати свої програми, які працюють у хмарній інфраструктурі. Це рішення широко відоме як SaaS, і мобільні послуги безпеки й управління надаються компанії через Інтернет [56].

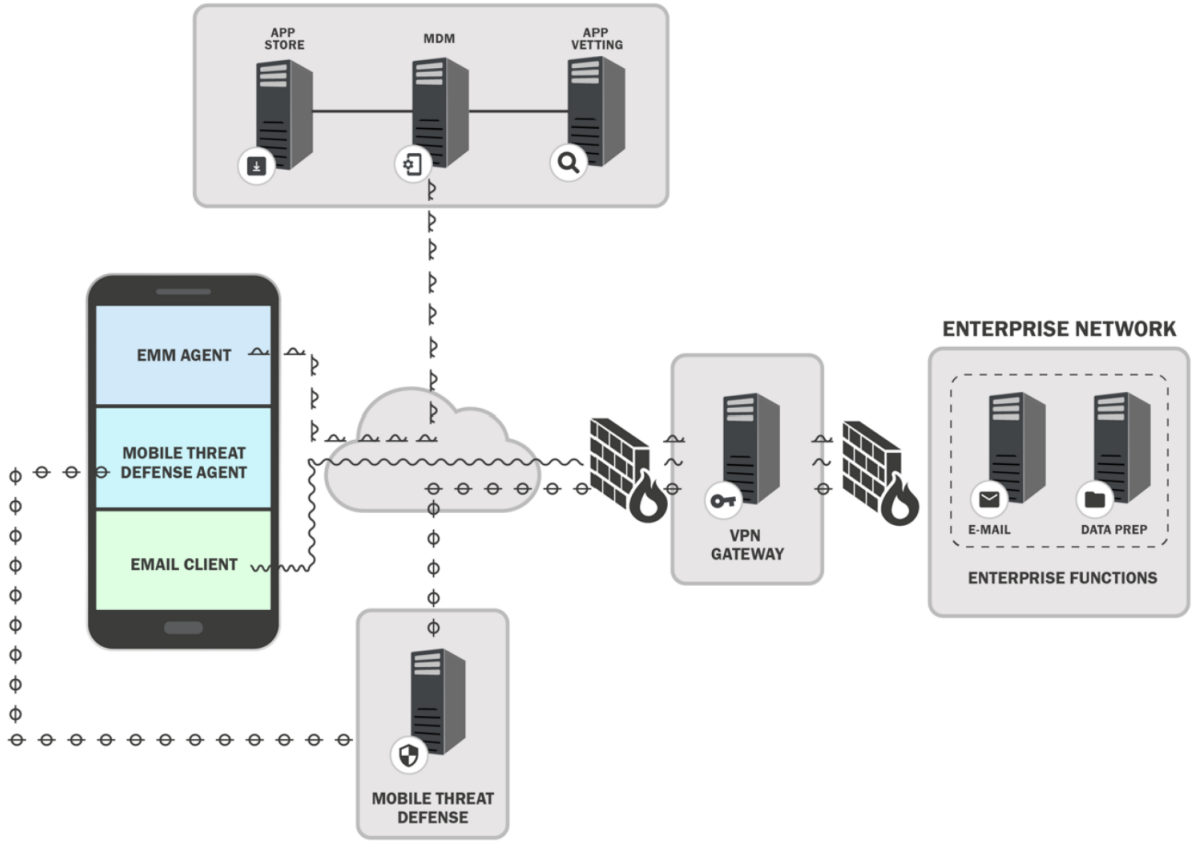

Рис. 3.7. Приклад хмарної мобільної архітектури

Хмарне розгортання EMM часто легше налаштувати й використовувати. Воно включає реєстрацію у веб-сервісах, і користувачі швидко переходять на основну інформаційну панель після покупки. Найважчими аспектами налаштування хмарного рішення є приєднання EMM до служби Active Directory і підтвердження того, що домен електронної пошти, який використовується, дійсно належить компанії. Постачальник EMM часто надає унікальну інформацію, яку потрібно розмістити в DNS і потім перевірити зовні.

Ще одна перевага моделі SaaS полягає в тому, що проблеми можуть бути легше вирішені постачальником, оскільки він має доступ до примірника EMM і базової платформи. Нарешті, завдяки цій моделі корпоративні дані знаходяться за межами підприємства, так само, як і мобільні пристрої, якими управляє EMM. Це часто є ключовим чинником того, щоб організації вирішують не застосовувати цю модель. Нижче наведено зразок архітектури, яка демонструє хмарну архітектуру мобільного підприємства (наприклад, сервер MDM, сервер перевірки програм, рішення MTD).

Інтеграція EMM в корпоративну сервісну інфраструктуру. Як великі, так і малі підприємства можуть підключити свою систему EMM до існуючих служб корпоративної інфраструктури, щоб покращити управління безпекою мобільних пристроїв. Такі служби підтримують автентифікацію, ідентифікацію та контроль доступу до корпоративних мереж і ресурсів.

Служба віддаленої автентифікації за викликом користувача (RADIUS) - це стандартний протокол служби автентифікації мережі, який забезпечує автентифікацію облікових даних доступу з подальшим призначенням мережевих ресурсів на основі політики (наприклад, адреса Інтернет-протоколу IP, дозволений час підключення до мережі). Служби каталогів, такі як Microsoft Active Directory, відображають мережеві ресурси (наприклад, користувачів, принтери, пристрої) на мережеві адреси. Корпоративні системи використовують полегшений протокол доступу до каталогу (LDAP) для зв’язку зі службами каталогів. Інший набір послуг забезпечує віддалене підключення до корпоративних систем через VPN.

Завдяки інтеграції EMM зі службами серверної інфраструктури підприємства, такими як RADIUS або службами каталогів, компанія може забезпечити більш детальне управління доступом мобільних пристроїв до критично важливих корпоративних ресурсів. Системні адміністратори можуть установлювати конфігурації на основі політики для мобільних пристроїв, щоб обмежити доступ до конфіденційних ресурсів залежно від умов мобільного

пристрою (наприклад, підключення з загальнодоступної мережі Wi-Fi або керованого користувачем пристрою, на якому запущена корпоративна програма).

Якщо підприємства розгортають EMM, не інтегруючи його зі своєю серверною інфраструктурою безпеки, підключенням мобільних пристроїв до корпоративної мережі можна управляти за допомогою глобальних парольних фраз для підключення до корпоративної мережі WiFi [12].

Налаштування політики, конфігурації пристрою і забезпечення відповідності. У деяких моделях розгортання мобільні пристрої слід правильно налаштувати, перш ніж їх можна буде надати корпоративним користувачам. Керівництво компанії, орієнтуючись дотримання вимог IT та власного бізнесу, мають прийняти ефективну політику використання мобільних пристроїв.

Політика використання мобільних пристроїв зазвичай визначає стандартні засоби захисту, які будуть застосовуватися до всіх корпоративних мобільних пристроїв, встановлює дозволи та спеціальні конфігурації, які застосовуються до користувачів з різними ролями. Після цього пристрої можна правильно налаштувати й підготувати для застосування вибраної політики. Для організацій з менш суворою позицією щодо використання пристроїв, таких як BYOD, користувачів ознайомлюють із політикою використання мобільних пристроїв під підпис.

Визначення політики управління корпоративною мобільністю. Політика EMM – це набір правил, які визначають, що користувачеві дозволено (чи заборонено) робити на своєму мобільному пристрої та встановлюють вимоги до конфігурації мобільного пристрою. Політики EMM розробляють, щоб допомогти захистити корпоративні дані на мобільних пристроях. Для цього підприємство має знати типи даних, з якими працює користувач, фактори ризику та правильний спосіб захисту цих даних від випадкових або навмисних загроз. Розуміючи ці ключові фактори, підприємство документує політику EMM і застосовує конфігурації політики в EMM.

Ці політики можуть відрізнятися залежно від користувача чи пристрою, оскільки певна група користувачів або посада на підприємстві можуть мати

різні дозволи для належного виконання своїх обов'язків. Тому політика EMM має бути чітко й однозначно визначена, дозволи користувача мають точно відображати вимоги політики, і користувач має отримати тільки такий доступ до корпоративних даних, який необхідний для виконання його посадових обов'язків. В іншому випадку працівник може отримати несанкціонований доступ до корпоративної інформації. Також у політику EMM варто включити вимоги до пароля, шифрування пристрою, VPN і геозонування [57].

Перевірочне тестування. Щоб захистити робоче корпоративне середовище, а також корпоративні й користувацькі дані, здійснюють перевірку конфігурації мобільних пристроїв, які підключаються до підприємства, і встановленого на них ПЗ. Перед розгортанням, оновленням або виправленням корпоративного ПЗ адміністратори проводять тестування, щоб зрозуміти, як потенційна зміна може вплинути на безпеку й функціональність існуючих корпоративних систем. Для важливого розгортання програмного забезпечення або значних оновлень адміністратори спочатку здійснюють розгортання для обмеженої групи користувачів, щоб оцінити вплив на виробниче середовище.

Очевидно, що надання мобільним пристроям доступу до корпоративних ресурсів може сприяти кращій роботі персоналу для досягнення бізнес-цілей підприємства. Однак мобільні пристрої також несуть ризики для корпоративних систем, даних і користувачів. Перевіряючи прийнятність конфігурації мобільних пристроїв та додатків, підприємство сприяє тому, що переваги мобільного доступу переважають ризики безпеки для корпоративної екосистеми IT.

Конфігурації на рівні мобільних пристроїв або додатків можуть суттєво вплинути на рівень безпеки підприємства. Так, дозволи для пристрою або окремих програм можуть бути надані залежно від конкретних параметрів конфігурації. Конфігурації мережі можуть передбачати обов'язковість автентифікації та використання VPN перед отримання дозволу на підключення до корпоративної бездротової мережі.

Політика геозонування може визначати, які рівні дозволи (часто відмінні для різних регіонів) надаються пристрою, який працює в різних географічних

зонах. Різним користувачам, пристроям або ПЗ можуть надаватися різні дозволи на доступ до серверних служб підприємства (наприклад, бази даних, що містить конфіденційну інформацію), залежно від конфігурації програми або пристрою.

У багатьох випадках функції безпеки мобільного пристрою налаштовані для кращого захисту підприємства на додаток до самого гаджета. Так, можна налаштувати шифрування даних пристрою, тайм-аут блокування екрана, пароль і вимоги до брандмауера програм, що сприятиме забезпеченню безпеки підприємства. Нарешті, корпоративна політика може обмежувати встановлення додатків, вимагати оновлення програм або мобільної ОС, обмежувати доступ до деяких функцій пристрою з метою захисту корпоративних систем або даних.

Тестування розгортання. Корпоративні мережі та програми вимагають оновлення ПЗ, щоб покращити функціональність, виправити вразливості й помилки або розгорнути нове обладнання. Щоб прийняти обґрунтовані рішення щодо розгортання, системні й мережеві адміністратори, перш ніж впровадити нове ПЗ у виробниче середовище, здійснюють тестування розгортання.

Адміністратори розглядають широкий спектр тестових сценаріїв, щоб оцінити оновлення ПЗ й вирішити, які тести будуть використані, щоб переконатися, що оновлення готове до робочого середовища. Для тестування розгортання зазвичай рекомендується поетапний підхід до тестування на рівні компонентів, функцій, мережі та в масштабах підприємства.

Наприклад, при впровадженні нових корпоративних можливостей, таких як керовані мобільні пристрої або перевірка мобільних додатків, адміністратор розглядає можливість розгортання обмеженої пробної версії лише з невеликою групою ретельно відібраних користувачів. Після того, як пробне розгортання задовільно функціонує протягом заздалегідь визначеного періоду часу, і якщо якість взаємодії з користувачем відповідає цільовому рівню, компанія розпочинає розгортання нових схем на рівні підприємства. Дотримання такого підходу не тільки забезпечує мінімальні збої в роботі підприємства і позитивний досвід користувача, але також полегшує виявлення проблем безпеки якомога раніше в процесі розгортання [12].

3.3 Експлуатація, обслуговування й утилізація мобільних пристроїв

Обов’язковим етапом управління мобільним середовищем підприємства є впровадження заходів і засобів безпеки для захисту корпоративних систем, а також даних і користувачів. Однак початкового розгортання засобів управління недостатньо для захисту діючого підприємства. Крім цього, для оцінки ефективності засобів безпеки, виявлення проблем безпеки, модифікації або додавання нових засобів для кращого захисту системи в майбутньому проводять періодичні IT-аудити. Важливим джерелом даних для оцінювання ефективності засобів безпеки в середовищі мобільних комп’ютерів надають журнали використання мобільних пристроїв.

Аудит. Щоб не відставати від динамічної зміни атак і ландшафту кібербезпеки, команда безпеки підприємства має проводити оцінювання безпеки, важливим компонентом якого є періодичний аудит IT-інфраструктури підприємства й мобільної мережевої інфраструктури.

Комплексний аудит має охоплювати такі види діяльності:

– визначення цілей аудиту підприємства;

– встановлення базового рівня безпеки шляхом періодичних аудитів;

– залучення аудиторів зі значним (і підтвердженим) досвідом;

– розробка автоматизованого процесу аудиту для всієї IT-інфраструктури підприємства, включаючи мобільні пристрої;

– проведення детального аналізу даних, отриманих у процесі аудиту;

– залучення стороннього аудитора для звітування про ризики, з якими стикається підприємство.

Періодичні аудити мають охоплювати корпоративну мобільну інфраструктуру й системи управління пристроями, такі компоненти, як EMM/MDM, послуги перевірки мобільних додатків, інтеграцію з серверними

службами, а також мобільні пристрої співробітників і їхні програми. Аудит має допомогти фахівця із безпеки оцінити, чи переваги мобільного доступу переважають ризики безпеці екосистеми підприємства [58].

Використання пристроїв. Обов'язковим кроком в організації заходів безпеки є розробка корпоративної політики безпеки та конфіденційності для використання мобільних пристроїв і програм. Ключовим елементом цієї політики є корпоративний моніторинг використання пристрою/програми. EMM, MAM і багато систем моніторингу мобільних мереж дозволяють адміністраторам відстежувати й контролювати дії користувачів, зокрема щодо:

– ідентифікації всіх програм пристрою,

– шаблонів використання програми (наприклад, завантаження, коли/як часто програма запускається),

– функцій пристрою, які використовуються кожною програмою (наприклад, мікрофон, камера),

– даних, які використовуються програмою (наприклад, місцезнаходження користувача, контакти),

– географічного розташування пристрою/користувача;

– телефонних дзвінків (наприклад, номер телефону, ім'я, тривалість, дата, місце) [59].

Відповідна політика моніторингу для мобільних пристроїв і додатків зазвичай враховує багато факторів, зокрема бізнес-цілі компанії (і те, як мобільний пристрій/додаток підтримує цю місію); характеристики безпеки й конфіденційності корпоративних даних і систем, доступ до яких здійснюється через пристрій; зв'язок користувача з підприємством (наприклад, працівник, підрядник, співробітник партнерської організації, представники широкої громадськості); модель розгортання (наприклад, у власності підприємства, BYOD) і конфіденційність користувача.

Політика моніторингу, яка підходить для корпоративних пристроїв, які використовують працівники в дуже чутливому середовищі, може включати

відстеження місцезнаходження пристрою та користувача, геозонування використання певних програм. Така політика є неприйнятною і, ймовірно, неможливою для реалізації для індивідуальних пристроїв працівників партнерської організації, які перебувають на території підприємства.

Важливим завданням є забезпечення конфіденційності користувачів, оскільки більшість пристроїв міститиме певну особисту інформацію користувача, а певні типи моніторингу (наприклад, геолокація) можуть спричинити конфлікт між інтересами підприємства та положеннями законодавства щодо конфіденційності. Компаніям, які ведуть бізнес у межах ЄС, слід також враховувати, як положення ЄС щодо конфіденційності й захисту даних (наприклад, Загальний регламент захисту даних GDPR [60] обмежують моніторинг використання мобільних пристроїв і додатків.

Утилізація та/або повторне використання пристрою. Мобільні пристрої можуть зберігати конфіденційну інформацію, таку як паролі, номери облікових записів, електронні листи, голосові повідомлення, журнали текстових повідомлень або дані, пов’язані з бізнес-завданнями (наприклад, конфіденційну інформацію правоохоронних органів). Коли мобільний пристрій потрібно утилізувати, важливо вжити належних заходів, щоб конфіденційна інформація не потрапила до чужих рук.

Для очищення носіїв інформації використовують різні методи. Такі методи як розмагнічування, перезапис пам’яті або навіть фізичне шліфування можна використовувати для дезінфекції магнітних носіїв. Однак ці методи є неефективними для очищення твердотільної пам’яті, яка використовується в мобільних пристроях. Більшість мобільних пристроїв тепер зберігають дані користувачів на дисках із самошифруванням (SED), які забезпечують постійне шифрування.

Мобільні ОС використовують шифрування, властиве SED, щоб забезпечити функцію «апаратного скидання» або «скидання до заводських налаштувань», щоб очистити майже всю інформацію з пам’яті пристрою за допомогою техніки «криптографічного видалення» [61]. Криптографічне

видалення здійснюється шляхом дезінфекції ключа шифрування для диска, що робить зашифровані дані користувача нечитабельними. Важливо активувати шифрування всього пристрою перед його розгортанням і виконати операцію скидання до заводських налаштувань, щоб криптографічно стерти всі дані користувача перед утилізацією пристрою.

Для безпечної утилізації пристрою необхідно враховувати два додаткові аспекти: гарантоване знищення ключа шифрування накопичувача і знищення даних користувача на знімних картах пам’яті (наприклад, картках SIM або Secure Digital). Якщо ключ шифрування пристрою має створену резервну копію або депонований за межами пристрою, цей ключ можна буде використати для відновлення даних користувача на пристрої. Під час розробки процедур санітарної обробки пристроїв компанії слід звернути увагу на наявність і розташування таких резервних копій.

Окрім зберігання такої інформації, як фотографії та завантажені документи, у внутрішній пам’яті пристрою, багато мобільних пристроїв зберігають таку інформацію на зовнішній картці SD. Контакти, голосова пошта та журнали текстових повідомлень можуть зберігатися на SIM-картці, а також у внутрішній пам’яті пристрою. Скидання заводських налаштувань не видалить інформацію, що міститься на SIM- або SD-картах, які використовуються з пристроєм. Щоб видалити всю інформацію з цих карток, їх вилучають і фізично знищують. Ретельний процес утилізації пристрою включає як відновлення заводських налаштувань, так і видалення всіх пов’язаних карт.

Висновки до розділу 3

Встановлено, що для підвищення ефективності управління мобільним середовищем NIST пропонує впровадити процес розгортання й управління мобільними пристроями протягом їх життєвого циклу, який включає етапи:

визначення вимог до мобільних пристроїв; оцінювання ризиків; реалізація корпоративної стратегії мобільної безпеки; експлуатація і підтримка функціонування; утилізація або повторне використання мобільних пристроїв.

На першому етапі життєвого циклу мобільних пристроїв відповідальні особи визначають вимоги до мобільних пристроїв для досягнення цілей компанії, проводять інвентаризацію наявних мобільних пристроїв і визначають найбільш прийнятну модель розгортання мобільного середовища.

Процес оцінювання ризиків є основоположним компонентом кібербезпеки і другим етапом життєвого циклу мобільних пристроїв, який передбачає ідентифікацію, оцінювання й визначення пріоритетності ризиків мобільним операціям і активам на рівні компанії, бізнес-цілей або інформаційної системи.

Рішення щодо впровадження стратегії мобільності підприємства приймається на основі аналізу наявності ресурсів, бізнес-потреб та інших корпоративних вимог і охоплює: вибір і встановлення мобільних технологій; інтеграцію EMM в корпоративну інфраструктуру; налаштування політики, конфігурації пристроїв і забезпечення відповідності; визначення політики управління корпоративною мобільністю; тестування з метою перевірки і перед розгортанням мобільної інфраструктури.

Для забезпечення успішної експлуатації та підтримки функціонування мобільних технологій компанія впроваджує заходи і засоби для захисту корпоративних мобільних пристроїв, даних і користувачів, а також проводить періодичні IT-аудити, які є основою для оцінки ефективності заходів і засобів безпеки та їх подальшого коригування.

Завданням етапу утилізації або підготовки пристрою до повторного використання є очищення носіїв інформації з використанням методів, які забезпечують гарантоване знищення даних на певних видах пристроїв і всіх пов’язаних картах без можливості їх відновлення.

ВИСНОВКИ

У результаті дослідження встановлено, що мобільні пристрої, крім очевидних переваг надання доступу до послуг, додатків і даних у будь-який час і будь-якому місці, створюють унікальні загрози для підприємства, пов’язані з обробкою, зберіганням і передачею конфіденційних даних. З огляду на це визначальну роль відіграє мобільна безпека, яка має на меті захист мобільних пристроїв від загроз несанкціонованого доступу, використання чи модифікації і включає безпеку пристроїв, даних, програм і мереж.

Аналіз показав, що основними вразливостями безпеки мобільних технологій є: відсутність засобів фізичної безпеки; використання ненадійних пристроїв, мереж, програм і контенту, взаємодія з іншими системами, використання GPS. Загрози мобільній безпеці підприємства поділяють на загрози для корпоративного використання мобільних пристроїв і систем їх управління.

З’ясовано, що технології мобільної безпеки поділяють на два види: технології управління й безпеки пристрою (апаратну підтримку обробки та зберігання даних; механізми ізоляції даних; прикладний програмний інтерфейс API; підтримку захищених мереж VPN; механізми автентифікації, і технології мобільної безпеки підприємства (управління корпоративною мобільністю EMM; управління мобільними додатками MAM; захист від мобільних загроз MTD; перевірку мобільних додатків MAV; віртуальну мобільну інфраструктуру VMI; обгортання програм і захищені контейнери).

Для запобігання і протидії загрозам мобільній безпеці підприємству доцільно застосовувати різноманітні заходи і засоби, серед яких технології EMM; впровадження кращих практик кібербезпеки; віддалене безпечне очищення; вибір пристрою з функціями безпеки; безпечне підключення до ресурсів; швидке здійснення оновлень ПЗ; ізоляція ОС і програм; перевірка мобільних додатків; мобільний захист від загроз; навчання користувачів; політики мобільної безпеки; оповіщення і скасування доступу; автентифікація.

Встановлено, що для підвищення ефективності управління мобільним середовищем доцільно впровадити процес розгортання й управління мобільними пристроями протягом їх життєвого циклу, який включає етапи: визначення вимог до мобільних пристроїв; оцінювання ризиків; реалізація корпоративної стратегії мобільної безпеки; експлуатація і підтримка функціонування; утилізація або повторне використання мобільних пристроїв.

ПЕРЕЛІК ПОСИЛАНЬ

1. Why is mobile security important? URL: https://www.ibm.com/topics/ mobile-security

2. Why mobile security is more complicated than ever. URL: https://everphone.com/en/blog/mobile-security/

3. Verizon’s Mobile Security Index 2020. URL: https://www.verizon.com/ business/verizonpartnersolutions/business/resources/reports/2020-msi-financial-services.pdf

4. Verizon’s Mobile Security Index 2023. URL: https://www.verizon.com/ business/resources/reports/mobile-security-index/

5. Сєвєрінов О. В., Федорченко В. М., Перепадя В. І. Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків. Системи озброєння і військова техніка. 2016. № 4 (48). С. 42-45.

6. M. Souppaya, K. Scarfone. Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST SP 800-124r1. June 2013. 21 p.

7. BYOD (Bring Your Own Device). URL: https://www.techtarget.com/ whatis/definition/BYOD-bring-your-own-device

8. NIST Glossary. Information Technology Laboratory. Computer Security Resource Center. URL: https://csrc.nist.gov/glossary (дата звернення: 15.12.2023).

9. ENISA Glossary. URL: https://www.enisa.europa.eu/topics/incident-response/glossary

10. Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53, Rev. 5. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

11. What is GPS? URL: https://www.gps.gov/systems/gps/

12. M. Souppaya, K Scarfone. NIST SP 800-124r2 Guidelines for Managing the Security of Mobile Devices in the Enterprise. May 2023. 51 p.

13. S. McConnell. Code Complete: A Practical Handbook of Software Construction. Microsoft Press, Redmond, WA, 2nd Ed. 2004. URL: https://github.com/media-

lib/prog_lib/blob/master/general/Steve%20McConnell%20-%20Code%20Complete%20(2nd%20edition).pdf

14. Phishing attacks. URL: https://www.imperva.com/learn/application-security/phishing-attack-scam/

15. M. Shacklett, P. Loshin. Digital certificate. URL: https://www.techtarget.com/ searchsecurity/definition/digital-certificate

16. Shadow IT. URL: https://www.proofpoint.com/us/threat-reference/shadow-it

17. J. Minihane. Tethering. URL: https://www.uswitch.com/ mobiles/guides/what-is-tethering/

18. National Vulnerability Database. NIST. URL: https://nvd.nist.gov/vuln/data-feeds

19. Платоненко А. В. Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту. Сучасний захист інформації. 2017. №1. С. 128-132.

20. Mobile threat catalog. NIST. URL: https://pages.nist.gov/mobile-threat-catalogue/categories.html

21. Apple Platform Security Guide. Apple. 2023. URL: https://help.apple.com/ pdf/security/en_US/apple-platform-security-guide.pdf (дата звернення: 15.12.2023).

22. Android Enterprise Security Paper. Android. 2023. URL: https://source.android.com/security/reports/Google_Android_Enterprise_Security_Whitep aper_2020.pdf

23. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.

24. K. Perunicic. Different types of VPNs and when to use them. URL: https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/

25. M. Goad, C. Steele. Enterprise Mobility Management (EMM) URL: https://www.techtarget.com/searchmobilecomputing/definition/enterprise-mobility-management-EMM

26. Толюпа С. В., Пархоменко І. І., Кириленко А. І., Вадис К. А. Захист корпоративної інформації на мобільних пристроях. URL: https://kneu.edu.ua/ userfiles/zb_mise/99/13.pdf.

27. T. Reidt. How does MAM work? URL: https://emteria.com/learn/mobile-application-management

28. Mobile Threat Defense (MTD). URL: https://www.appsealing.com/ mobile-threat-defense/

29. M. Ogata, J. Franklin, J. Voas, V. Sritapan, S. Quirolgico. Vetting the Security of Mobile Applications. NIST SP 800-163, Rev. 1. 2019. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/ NIST.SP.800-163r1.pdf

30. M. Chapple. Mobile security trends: app containers, app wrapping for BYOD. URL: https://www.techtarget.com/searchsecurity/feature/App-container-app-wrapping-and-other-emerging-mobile-security-tactics

31. What is a COTS (Commercial-Off-the-Shelf) Software. URL: https://itechnolabs.ca/commercial-off-the-shelf-software-cots-advantages-and-examples/

32. Patch Management. URL: https://www.intel.com/content/www/us/en/ business/enterprise-computers/resources/patch-management.html

33. Configuration Management. URL: https://www.vmware.com/topics/ glossary/content/configuration-management.html

34. E. Barker, Q. Dang, S. Frankel, K. Scarfone, P. Wouters. Guide to IPsec VPNs. NIST SP 800-77, Rev. 1. 2020. URL: https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-77r1.pdf

35. S. Rose, O. Borchert, S. Mitchell, S. Connelly. Zero Trust Architecture. NIST SP 800-207. 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/ NIST.SP.800-207.pdf

36. National Vulnerability Database: Vulnerability Metrics. NIST. 2023. URL: https://nvd.nist.gov/vuln-metrics/cvss

37. M. Souppaya, K. Scarfone. Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. NIST SP 800-40, Rev. 4. 2022. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

38. Application isolation. URL: https://devopsbootcamp.osuosl.org/ application-isolation.html

39. R. Petersen, D. Santos, K. Wetzel, M. Smith, G. Witte. Workforce Framework for Cybersecurity (NICE Framework)., NIST SP 800-181, Rev. 1. 2017. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

40. R. Chouffani. Why a mobile security policy is a must-have corporate policy. URL: https://www.techtarget.com/searchmobilecomputing/feature/Why-a-mobile-security-policy-is-a-must-have-corporate-policy

41. P. Grassi, M. Garcia, J. Fenton. Digital Identity Guidelines. NIST SP 800-63-3, 2017. updates in 2020. URL: https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-63-3.pdf

42. Purpose and vision CIO. URL: https://www.cio.gov/about/vision/

43. Mobile Security Decision Framework v1.0. Appendix B. URL: https://assets.cio.gov/assets/files/resources/Mobile-Security-Decision-Framework-Appendix-B.pdf

44. K. Dempsey, P. Eavy, G. Moore. Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management. NIST Interagency or Internal Report (IR) 8011, Vol. 2. 2017. URL: https://nvlpubs.nist.gov/nistpubs/ir/2017/ NIST.IR.8011-2.pdf

45. M. Souppaya, K. Scarfone. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. NIST SP 800-46, Rev. 2. 2016. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

46. Government Furnished Equipment (GFE). URL: https://www.bis.doc.gov/ index.php/component/fsj_faqs/faq/317-q-5-what-does-the-term-government-furnished-equipment-gfe-mean-in-paragraph-b-2-iii-e-of-license-exception-gov

47. B. Posey. COPE (Corporate-owned, Personally Enabled). URL: https://www.techtarget.com/searchmobilecomputing/definition/COPE-corporate-owned-personally-enabled

48. J. Franklin, G. Howell, K. Boeckl, N. Lefkovitz, E. Nadeau, B. Shariati, J. Ajmo, C. Brown, S. Dog, F. Javar, M. Peck, K. Sandlin. Mobile Device Security:

Corporate-Owned Personally-Enabled (COPE) NIST SP 1800-21. 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-21.pdf

49. K. Boeckl, N. Grayson, G. Howell, N. Lefkovitz, J. Ajmo, M. McGinnis, K. Sandlin. Mobile Device Security: Bring Your Own Device (BYOD) Second Draft NIST SP 1800-22. 2022. URL: https://www.nccoe.nist.gov/sites/default/files/2022-11/mdse-nist-sp1800-22-draft-2.pdf

50. M. Brodin BYOD vs. CYOD. What is the difference? URL: https://www.diva-portal.org/smash/get/diva2:920380/FULLTEXT01.pdf

51. Joint Task Force Transformation Initiative. Guide for Conducting Risk Assessments. NIST SP 800-30, Rev. 1. 2012. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

52. J. Franklin, C. Brown, S. Dog, N. McNab, S. Voss-Northrop, M. Peck, B. Stidham. Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue. NIST Interagency or Internal Report (IR) 8144. 2016. URL: https://csrc.nist.gov/publications/detail/nistir/8144/draft

53. M. Souppaya, K. Scarfone. Draft NIST SP 800-154, Guide to Data-Centric System Threat Modeling. Draft NIST SP 800-154. 2016. URL: http://csrc.nist.gov/publications/drafts/800-154/sp800_154_draft.pdf

54. The MITRE Corporation. Adversarial Tactics, Techniques & Common Knowledge Mobile Profile (ATT&CK). 2023. URL: https://attack.mitre.org/tactics/mobile/

55. B. Taylor, M. Bhat, T. Cosgrove, C. Silva, R. Smith. Critical Capabilities for Enterprise Mobility Management Suites. 2017. URL: https://www.gartner.com/en/documents/3751864

56. J. Franklin, K. Bowler, C. Brown, S. Dog, S. Edwards, N. McNab, M. Steele. Mobile Device Security: Cloud and Hybrid Builds. NIST SP 1800-4. 2019. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-4.pdf

57. How can you ensure your EMM policies reflect the latest mobile technologies? URL: https://cutt.ly/twSgBQ1b

58. Auditing Mobile Devices ISACA, Securing Mobile Devices, USA, 2012. URL: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2017/volume-6/auditing-mobile-devices_joa_eng_1117

59. How can you effectively monitor mobile devices in your organization? URL: https://www.linkedin.com/advice/1/how-can-you-effectively-monitor-mobile-devices

60. General Data Protection Regulation. GDPR. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

61. R. Kissel, A. Regenscheid, M. Scholl, K. Stine. Guidelines for Media Sanitization. NIST SP 800-88, Rev. 1. 2014. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf