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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо управління мобільними пристроями в інформаційній системі організації»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Михайло СМІРНОВ
(підпис)

Виконав: здобувач вищої освіти групи БСД-44
СМІРНОВ Михайло
(прізвище, ім'я)

Керівник phD(доктор філософії)
СОБЧУК Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ВСТУП

Актуальність дослідження. У зв'язку з масовим поширенням мобільних технологій, організації все активніше впроваджують мобільні пристрої у внутрішні інформаційні системи для забезпечення мобільності персоналу. Проте разом із цим зростають і ризики, пов'язані з інформаційною безпекою. Мобільні пристрої найчастіше є слабкою ланкою в ІС, оскільки можуть бути втрачені, скомпрометовані або піддані атакам через незахищені бездротові канали, фішингові програми, шкідливі додатки чи неправильне конфігурування.

Проблема ускладнюється відсутністю чітких процедур управління мобільними пристроями, обмеженим контролем над ними, а також недостатньою кваліфікацією персоналу в питаннях мобільної безпеки. Внаслідок цього зростає кількість інцидентів, пов'язаних із витоком конфіденційних даних, несанкціонованим доступом до ІС, порушенням законодавства про захист персональних даних.

Тому тема розробки рекомендацій щодо управління мобільними пристроями є надзвичайно актуальною в умовах гібридної роботи, поширення віддаленого доступу та необхідності дотримання вимог інформаційної безпеки. Ефективне управління цими пристроями є не лише технічним завданням, а й стратегічним кроком до забезпечення цілісності, конфіденційності та доступності даних, що обробляються в інформаційній системі організації.*Об'єкт дослідження – управління мобільними пристроями в інформаційній системі організації.*

Предмет дослідження – методи та засоби управління мобільними пристроями в інформаційній системі організації.

Мета роботи – розробка рекомендацій щодо управління мобільними пристроями в інформаційній системі організації.

Наукові завдання:

дослідити сутність проблеми управління мобільними пристроями в інформаційній системі організації;

проаналізувати сучасні рішення та міжнародні стандарти в цій сфері;

розробити рекомендації щодо управління мобільними пристроями в інформаційній системі організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: розроблено рекомендації щодо формування політики управління мобільними пристроями (на базі MDM), а також рекомендації щодо супроводу, моніторингу та вдосконалення політики.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

1.1 Поняття та роль мобільних пристроїв в інформаційній системі організації

Визначення мобільного пристрою

Згідно з публікацією NIST SP 800-124 Rev. 2, мобільний пристрій – це портативний обчислювальний пристрій, що має малий форм-фактор, автономне живлення, локальне сховище даних, бездротові інтерфейси для передачі інформації, а також можливість встановлення сторонніх додатків і використання повноцінної операційної системи [1].

Основні характеристики

У публікації, NIST SP 800-124 Rev. 2 [1], наведено загальні характеристики , що дозволяють визначити їх відмінність від інших типів пристроїв, зокрема пристроїв Інтернету речей.

Насамперед, мобільні пристрої оснащені багатофункціональною операційною системою, що забезпечує гнучкість у використанні та підтримку широкого спектра додатків. Ця особливість відрізняє їх від пристроїв IoT, які зазвичай не мають повноцінної ОС і мають обмежену функціональність.

Характерною ознакою мобільних пристроїв є компактний розмір, що забезпечує високу портативність, а також наявність автономного джерела живлення, яке дозволяє пристрою працювати незалежно від стаціонарних джерел електроенергії. Можливість зарядки реалізується як через фізичні порти, так і за допомогою бездротових технологій.

Мобільні пристрої мають принаймні один бездротовий мережевий інтерфейс, що дозволяє підключення до Інтернету або інших мереж для передачі даних. Вони також містять вбудоване сховище даних, зазвичай незнімне, що забезпечує збереження інформації та налаштувань. Окрім вбудованих додатків, більшість

сучасних мобільних пристроїв підтримують встановлення стороннього програмного забезпечення, що значно розширює їх функціональні можливості.

Керування мобільними пристроями здійснюється за допомогою інтерфейсів прикладного програмування (API) або пропрієтарних механізмів, що дозволяє організаціям реалізовувати політику безпеки та централізоване адміністрування. Крім того, пристрої можуть підтримувати різні мережеві служби, зокрема Bluetooth, Wi-Fi, NFC, а також мобільні мережі передачі голосу та даних (наприклад, 4G LTE або 5G).

Додаткові апаратні можливості включають наявність однієї або кількох цифрових камер, динаміків, мікрофонів, а також різноманітних сенсорів, як-от гіроскопи, акселерометри, біометричні зчитувачі, барометри та інші. Камери, зокрема, можуть виконувати як традиційні функції зйомки, так і слугувати інструментами біометричної автентифікації або зчитування QR-кодів.

Деякі мобільні пристрої підтримують використання знімних носіїв, як-от картки SD, для розширення пам’яті або обміну даними між пристроями. Також поширеною є підтримка синхронізації та резервного копіювання даних із зовнішніми системами, включно з хмарними сервісами чи корпоративною інфраструктурою. Для забезпечення безпеки даних мобільні пристрої можуть містити апаратні модулі безпеки, які відповідають за виконання криптографічних операцій і зберігання ключової інформації.

Класифікація мобільних пристроїв

Мобільні пристрої можна класифікувати за декількома ознаками, залежно від мети використання та функціональних можливостей. Основні класифікаційні критерії включають:

тип пристрою: смартфони, планшети, ноутбуки, носимі пристрої;

операційна система: Android, iOS, Windows, HarmonyOS та інші, менш поширені платформи;

функціональне призначення: пристрої для комунікації, для навігації, для роботи з документами, для аналітики або управління підприємством.

Кожен тип мобільного пристрою може бути інтегрований у корпоративну ІС з урахуванням специфіки бізнес-процесів підприємства. Наприклад, у логістиці широко використовуються планшети зі спеціалізованим ПЗ для сканування товарів, а в офісному середовищі – ноутбуки або смартфони для роботи з поштою, документами, CRM/ERP-системами.

Роль мобільних пристроїв

Мобільні пристрої виконують низку критично важливих функцій у сучасній організаційній структурі, оскільки дозволяють реалізувати концепцію мобільного офісу та віддаленого доступу до інформації. Серед ключових ролей можна виділити наступні:

мобільний доступ до корпоративних систем – за допомогою мобільних додатків працівники мають змогу працювати з внутрішніми базами даних, електронною поштою, календарями, системами управління проєктами, бухгалтерськими платформами тощо;

підвищення ефективності праці – згідно з дослідженням, 85% компаній зафіксували зростання продуктивності працівників завдяки впровадженню мобільних пристроїв у робочі процеси [2]. Це зростання обумовлене можливістю працівників виконувати завдання без жорсткої прив'язки до робочого місця, що особливо актуально для співробітників, які часто перебувають у відрядженнях або працюють дистанційно;

комунікація та оперативне реагування – смартфони та планшети дозволяють не лише оперативно передавати повідомлення чи дзвінки, але й організовувати відеоконференції, групову роботу над документами, обмін файлами. Це сприяє кращій координації між підрозділами та підвищує загальну динаміку управлінських процесів;

автоматизація процесів – у багатьох сферах (торгівля, логістика, виробництво) мобільні пристрої забезпечують швидкий доступ до інформації про залишковий товар, маршрути доставки, кількість запасів, що дозволяє зменшити обсяг ручної праці та підвищити точність обліку;

реалізація концепції цифрової трансформації – через мобільні пристрої реалізується більшість цифрових сервісів, включаючи електронні документообіги, хмарні рішення, цифрову ідентифікацію працівників.

1.2 Загрози, ризики та проблеми, пов'язані з використанням та управлінням мобільними пристроями

Основні загрози безпеки

Мобільні пристрої, незважаючи на свою зручність, мобільність та ефективність, створюють нові вектори атак для зловмисників. Їх широке використання у корпоративному середовищі супроводжується низкою типових загроз ІБ. Нижче наведено основні з них:

фішинг та соціальна інженерія – найпоширеніші загрози для користувачів мобільних пристроїв. Зловмисники імітують легітимні джерела за допомогою електронної пошти, текстових повідомлень або месенджерів, з метою викрадення особистих даних чи іншої конфіденційної інформації користувача. Соціальна інженерія, як інструмент психологічного впливу, використовується для маніпуляції діями користувача з метою обходу технічних засобів захисту;

шкідливе ПЗ – мобільні пристрої вразливі до шкідливого ПЗ різного типу таких як троянські програми, шпигунське ПЗ, руткіти та інші. Таке ПЗ зазвичай проникає на пристрої через встановлення додатків або перехід за посиланням та здатне виконувати несанкціоноване збирання даних, моніторинг дії користувача перехоплення комунікацій та отримання повного контролю над пристроєм;

витік даних через уразливі або ненадійні додатки – деякі мобільні застосунки, навіть офіційно розповсюджені через магазини додатків, можуть містити вразливості або навмисно збирати та передавати конфіденційні дані без відома користувача. Це може призвести до витоку критично важливої корпоративної інформації, що становить значну загрозу для організації;

вразливості бездротових мереж – підключення до відкритих та/або недостатньо захищених Wi-Fi мереж, особливо в громадських місцях, підвищує

ймовірність реалізації атак типу "людина посередині" (Man-in-the-Middle), під час яких зловмисники можуть перехопити, змінити або перенаправити мережевий трафік. Це створює ризик компрометації автентифікаційних даних, службової інформації та інших конфіденційних даних.

Основні ризики безпеки

Окрім загроз, які походять ззовні, існує низка ризиків, що пов'язані з самим процесом використання мобільних пристроїв у рамках ІС організації. Вони можуть спричинити порушення конфіденційності, цілісності та доступності даних. Нижче розглянуто ключові з них:

втрата або крадіжка пристрою – мобільні пристрої компактні, часто використовуються в публічних місцях і можуть бути легко втрачені або викрадені. У випадку, якщо на пристрої зберігаються корпоративні дані або є незахищений доступ до внутрішніх систем, втрата фізичного контролю над пристроєм може мати критичні наслідки для безпеки організації. Особливо небезпечна ситуація, коли пристрій не має засобів шифрування, складної аутентифікації або можливості дистанційного блокування [4];

несанкціонований доступ – у випадку слабких механізмів автентифікації (наприклад, використання простих PIN-кодів або відсутності біометричних методів), існує ризик отримання доступу до пристрою сторонніми особами. Це особливо важливо у випадках, коли пристрій синхронізовано з корпоративною поштою, хмарними сервісами або внутрішніми CRM/ERP-системами [4];

застаріле ПЗ – мобільні пристрої часто залишаються з застарілими версіями операційної системи або додатків через несвоєчасне оновлення. Це створює умови для експлуатації відомих вразливостей, які вже усунуті у новіших версіях. Проблема особливо актуальна для Android пристроїв, де оновлення залежить від виробника апарату, і користувачі можуть роками працювати на застарілих прошивках [5];

відсутність розмежування особистих і корпоративних даних – у разі використання одного пристрою для особистих і робочих цілей без належної сегментації даних (наприклад, за допомогою контейнеризації або віртуалізації),

інформаційна система організації піддається ризику витоку, змішування або випадкового видалення важливих даних. Наявність одночасного доступу до особистих соціальних мереж, хмарних сховищ та корпоративних сервісів підвищує імовірність як ненавмисних, так і зловмисних дій [4];

BYOD без контролю – політика BYOD дозволяє працівникам використовувати особисті пристрої в робочих цілях. Згідно з інформацією зі звіту Іванті про стан кібербезпеки за 2024 рік, яка була опублікована на LinkedIn, BYOD практикується у 84% організацій по всьому світу, незважаючи на те, що лише 52% фактично дозволяють це. Серед організацій, які не дозволяють BYOD, 78% сказали, що співробітники використовують свої особисті пристрої на роботі, навіть якщо це абсолютно заборонено політикою компанії [6]. Така практика дозволяє організації скоротити витрати на технічне забезпечення, однак значно ускладнює контроль і моніторинг безпеки. ІТ-відділ часто не має повноважень встановлювати обмеження або політики безпеки на особистих пристроях, що призводить до підвищеного ризику витоку, саботажу або зараження внутрішньої мережі [4].

Основні проблеми в управлінні

Незважаючи на розвиток технологій, управління мобільними пристроями залишається викликом для багатьох організацій через низку системних проблем:

Гетерогенність мобільного середовища

Використання співробітниками пристроїв, з різними ОС (наприклад Android, iOS, Windows, Linux), створює проблеми для організацій у контексті формування та впровадження уніфікованої політики управління. Така гетерогенність середовища обумовлює низку технічних і організаційних проблем.

По-перше, спостерігається несумісність механізмів безпеки між різними платформами. Кожна операційна система реалізує засоби захисту даних та контролю доступу за власною архітектурою, що унеможливлює впровадження єдиних стандартів безпеки.

По-друге, виникає складність уніфікації політик управління. Через відмінності у функціональних можливостях ОС та обмеження в реалізації

адміністративних інструментів, застосування однакових правил на всіх пристроях є технічно неможливим або неефективним.

По-третє, гетерогенність істотно обмежує можливості автоматизації процесів управління. Для кожного типу операційної системи необхідно розробляти окремі сценарії, налаштування та засоби контролю, що потребує додаткових ресурсів та ускладнює адміністрування, особливо у великих організаціях з розгалуженою IT-інфраструктурою.

Крім того, актуальною проблемою залишається часта несумісність MDM-рішень з оновленими версіями мобільних операційних систем. Зміни у політиках конфіденційності або архітектурі безпеки, які регулярно впроваджуються виробниками, можуть призводити до порушення функціональності вже реалізованих систем управління або вимагати повторної конфігурації без гарантії стабільної роботи.

Людський фактор

Навіть за наявності належно реалізованих технічних засобів та політик безпеки, людський фактор часто є причиною інцидентів ІБ, які ставлять під загрозу всю ІС організації. Співробітники не завжди дотримуються політик безпеки, нехтують оновленнями, використовують небезпечні програми, використовувати незахищені з'єднання. Як наслідок це призводить до підвищення ризику порушення конфіденційності, цілісності та доступності даних та/або облікового запису. Проблему ще й ускладнює психологічна втома від постійних попереджень з боку систем безпеки, що призводить до ігнорування попереджень або вимкнення захисту.

Обмежені ресурси: фінанси та кадровий дефіцит

Ефективне управління мобільними пристроями передбачає не лише наявність відповідного ПЗ, але й достатню кількість кваліфікованого персоналу та фінансових ресурсів. Витрати на придбання ліцензованого ПЗ, навчання персоналу, оновлення політики безпеки, постійний моніторинг та аудит системи можуть виявитися занадто високими для малого чи середнього бізнесу.

Через обмежені ресурси, організації змушені використовувати базові інструменти управління, які не забезпечують належний рівень захисту корпоративної інформації. Також обмеженість впливає на своєчасність оновлення інфраструктури. Наприклад, застарілі пристрої продовжують використовуватись у корпоративному середовищі, незважаючи на те, що вони вже не підтримують сучасні стандарти безпеки.

Технічні обмеження застарілих пристроїв

Мобільні пристрої мають обмежений життєвий цикл, однак на практиці вони часто використовуються значно довше, ніж це рекомендовано виробником. Це пов’язано з економічними міркуваннями, але це створює серйозні проблеми безпеки. Старі пристрої можуть не підтримувати сучасні методи шифрування, багатофакторну автентифікацію або оновлення системи безпеки. Відсутність підтримки нових версій ОС унеможливлює впровадження сучасних MDM-рішень або політик безпеки.

Застарілі пристрої часто є джерелом вразливостей, які не можуть бути усунуті без повної заміни апаратного забезпечення. Також вони можуть бути несумісними з новими версіями корпоративного програмного забезпечення, що ускладнює інтеграцію та адміністрування таких пристроїв у загальній IT-інфраструктурі.

Невизначеність нормативно-правової бази

Однією з проблем для ефективного управління мобільними пристроями в організаціях також є недосконалість та неоднозначність нормативно-правового регулювання. Хоча багато країн вже розробили нормативні акти у сфері кібербезпеки та захисту персональних даних, ці положення часто не враховують специфіку використання мобільних пристроїв у корпоративному середовищі.

Особливо складною є ситуація для транснаціональних компаній, які змушені враховувати вимоги одразу кількох юрисдикцій. Наприклад, у країнах Європейського Союзу діє Загальний регламент про захист даних (GDPR), який накладає суворі обмеження на обробку персональної інформації. Згідно з цим регламентом, за серйозні порушення можуть бути накладені штрафи до 20 мільйонів євро або до 4% від загального світового обороту компанії за попередній

фінансовий рік, залежно від того, яка сума є більшою [8]. Невиконання таких вимог може мати серйозні фінансові наслідки. Наприклад, у 2025 році компанія TikTok була оштрафована на 530 мільйонів євро за незаконну передачу персональних даних користувачів з Європейського економічного простору до Китаю без належного забезпечення їх захисту [9].

1.3 Сучасні тенденції та проблеми управління мобільними пристроями

Сучасні тенденції в управлінні мобільними пристроями

Управління мобільними пристроями стрімко еволюціонує відповідно до розвитку технологій, зростання кіберзагроз та зміни підходів до організації праці. Серед провідних тенденцій можна виділити наступні:

Архітектура Zero Trust

Архітектура "нульової довіри" (Zero Trust) є однією з провідних тенденцій в управлінні мобільними пристроями. Вона базується на принципі, що жоден пристрій або користувач за замовчуванням, не вважається безпечним, навіть якщо він є частиною корпоративної мережі. Кожен запит доступу розглядається як потенційно небезпечний, і тому має проходити повну перевірку згідно з політиками безпеки організації.

У сфері управління мобільними пристроями це означає, що пристрої повинні постійно підтверджувати свою автентичність, бути відповідно налаштованими, оновленими, шифрованими та контрольованими. ZTA передбачає інтеграцію з системами багатофакторної автентифікації (MFA), аналіз відповідності, інструментами виявлення аномальної поведінки та службами оцінки ризиків. Особливо актуальною архітектура Zero Trust стає в умовах гібридної або віддаленої роботи, коли пристрої отримують доступ до корпоративних ресурсів з поза меж організації. Реалізація даного підходу дозволяє знизити ризики компрометації облікових даних, витоку інформації та проникнення шкідливого ПЗ на кінцеві точки [27].

Хмарні MDM-рішення

Перехід від локальних до хмарних платформ управління (наприклад Microsoft Intune, VMware Workspace ONE) дозволяє централізовано керувати мобільними пристроями, безпековими політиками, спростити адміністрування та інтеграцію з іншими системами. Такі сервіси підтримують централізоване впровадження політик безпеки, віддалене блокування пристроїв, моніторинг відповідності та автоматичне оновлення налаштувань.

Основною перевагою таких рішень є масштабованість, оперативність впровадження, зменшення витрат на обслуговування локальної інфраструктури та висока ступінь інтеграції з іншими хмарними сервісами. Також хмарні рішення дозволяють адміністраторам виконувати політики умовного доступу, дистанційно стирати дані з втрачених пристроїв, контролювати відповідність і забезпечувати безпечний доступ до корпоративних даних у режимі реального часу.

Інтеграція MDM з аналітичними системами та ШІ

Іншою перспективною тенденцією є посилення ролі аналітики та штучного інтелекту в управлінні мобільними пристроями. Завдяки інтеграції з модулями машинного навчання сучасні MDM/EMM/UEM-системи здатні виконувати глибоку поведінкову аналітику, виявляти відхилення від звичних шаблонів використання та автоматично реагувати на потенційні загрози. У разі виявлення аномалії система може автоматично змінити політику доступу, ініціювати додаткову автентифікацію, повідомити адміністратора або заблокувати пристрій. Таким чином, ШІ виступає інструментом проактивної безпеки, що підвищує ефективність реагування на кіберзагрози у режимі реального часу.

Умовний доступ (Conditional Access)

Технологія "умовного доступу" Conditional Access забезпечує надання доступу до даних або систем лише за умови відповідності пристрою ряду визначених політик безпеки. Ці політики можуть враховувати широкий спектр параметрів: стан пристрою (наявність шифрування, наявність антивірусного ПЗ, відсутність рут-доступу), геолокацію користувача, мережеву активність, роль в організації, тип пристрою тощо.

Принцип мінімальних привілеїв (Least Privilege Access)

Реалізація принципу "мінімальних привілеїв" (Least Privilege Access) полягає у тому, що кожному користувачу або пристрою надаються лише ті повноваження, які необхідні для виконання його функціональних обов’язків. Це дозволяє суттєво обмежити ризики у разі компрометації облікового запису або втрати пристрою.

У практичній реалізації це означає впровадження контролю доступу на основі ролей, ізоляцію ресурсів, обмеження привілеїв адміністратора, а також поділ службових і особистих даних.

Впровадження цього принципу є вимогою міжнародних стандартів, зокрема ISO/IEC 27001, та рекомендованою практикою в більшості галузевих рекомендацій з кібербезпеки. Це також важливий компонент загальної стратегії Zero Trust, що посилює стійкість до атак з боку як зовнішніх, так і внутрішніх зловмисників.

Модель Privacy-first

Модель Privacy-first передбачає побудову політик управління мобільними пристроями з урахуванням пріоритетності конфіденційності особистої інформації працівника. Вона полягає у логічному та технічному розмежуванні службових і персональних даних на одному пристрої. Це забезпечується, зокрема, використанням контейнеризації, коли корпоративні дані ізолюються в окремому середовищі, недоступному для сторонніх додатків. У системах на базі Android така ізоляція реалізується через профілі роботи, тоді як в екосистемі Apple доступні політики керування програмами без повного контролю над пристроєм.

Крім технічної реалізації, Privacy-first модель передбачає прозорість політик з боку організації, тобто обов’язкове інформування користувача про те, які саме дані контролюються, з якою метою та в якому обсязі. Впровадження подібних політик дозволяє підвищити рівень довіри співробітників до засобів управління мобільними пристроями, знизити ймовірність несанкціонованих дій або свідомого порушення політик ІБ.

Модель Zero Touch Enrollment

Це стратегія автоматизованого налаштування кінцевих пристроїв, яка дозволяє організаціям впроваджувати безпечну та контрольовану конфігурацію з

мінімальним або повністю відсутнім фізичним втручанням з боку IT-персоналу. Згідно з рекомендаціями NCSC (національного центру кібербезпеки Великої Британії), Zero Touch Enrollment слід розглядати як ключовий елемент у забезпеченні безпечного життєвого циклу пристроїв в організаціях, які впроваджують політику масового або віддаленого розгортання [3].

Основна перевага цього підходу полягає у забезпеченні довіри до пристрою з моменту першого увімкнення, до того як кінцевий користувач отримає до нього доступ. Це досягається шляхом попереднього зв’язування пристрою з інфраструктурою керування (наприклад, через платформу MDM або UEM). У такому сценарії пристрій, підключившись до мережі, автоматично проходить автентифікацію, завантажує потрібні політики безпеки, ПЗ і накладає обмеження згідно з вимогами організації. Крім того, використання Zero Touch Enrollment виключає ситуації, за яких користувачі або сторонні особи можуть втручатись у процес налаштування пристрою або змінювати критичні параметри без погодження з IT-відділом.

2 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА СТАНДАРТІВ УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ

2.1 Міжнародні стандарти з управління мобільними пристроями (ISO/IEC, NIST, CIS)

Стандарти ISO/IEC щодо управління мобільними пристроями

Міжнародна організація зі стандартизації (ISO) у співпраці з Міжнародною електротехнічною комісією (IEC) сформувала низку стандартів серії ISO/IEC 27000, які є фундаментальними у сфері інформаційної безпеки. Особливої уваги заслуговують стандарти ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701 та ISO/IEC 27553-1, які прямо чи опосередковано регулюють питання безпеки мобільних пристроїв.

ISO/IEC 27001 та ISO/IEC 27002

Стандарт ISO/IEC 27001 встановлює вимоги до створення, впровадження та вдосконалення системи управління інформаційною безпекою (ISMS) [10]. Цей підхід дозволяє організаціям ідентифікувати ризики, пов’язані з використанням мобільних пристроїв, та вживати відповідних заходів щодо їх зменшення.

У контексті мобільних пристроїв, ISO/IEC 27002, який надає практичні рекомендації щодо реалізації контролів безпеки, містить положення, що стосуються захисту мобільних пристроїв. Зокрема, контроль 8.1 акцентує увагу на необхідності впровадження політик та технічних заходів для захисту кінцевих пристроїв користувачів, включаючи мобільні телефони та планшети, з метою запобігання несанкціонованому доступу та втраті даних [11].

ISO/IEC 27701

Цей стандарт є розширенням ISO/IEC 27001 та ISO/IEC 27002 і фокусується на управлінні конфіденційною інформацією. Пункт 6.3.2 ISO/IEC 27701 акцентує на необхідності впровадження політик щодо управління мобільними пристроями, особливо в умовах віддаленої роботи. Також підкреслюється важливість

встановлення контролів, які забезпечують захист даних, що передаються або зберігаються на мобільних пристроях, включаючи заходи контролю доступу, шифрування та сегментацію даних [12].

ISO/IEC 27553-1

Стандарт ISO/IEC 27553-1 надає вимоги до захисту біометричних даних при їхньому використанні на мобільних пристроях. Він охоплює принципи забезпечення цілісності біометричних шаблонів, а також вимоги до захищеного зберігання та передачі біометричних даних у мобільному середовищі [13].

Рекомендації NIST щодо безпеки мобільних пристроїв

Національний інститут стандартів і технологій США (NIST) зробив низку публікацій, що надають рекомендації щодо управління та забезпечення безпекою мобільних пристроїв у корпоративному середовищі.

NIST SP 800-124 Rev. 2

Цей документ [1], надає рекомендації щодо управління безпекою мобільних пристроїв в організаціях. Він охоплює такі аспекти:

інвентаризація пристроїв: створення та підтримка актуального реєстру всіх мобільних пристроїв, що мають доступ до корпоративних ресурсів;

контроль доступу: впровадження багатофакторної аутентифікації та обмеження доступу на основі ролей користувачів;

шифрування даних: забезпечення шифрування даних як у стані спокою, так і під час передачі;

управління додатками: встановлення політик щодо дозволених додатків та регулярний моніторинг їх використання;

реагування на інциденти: розробка планів реагування на інциденти, включаючи можливість віддаленого стирання даних з компрометованих пристроїв;

управління життєвим циклом пристроїв: забезпечення безпеки на всіх етапах життєвого циклу пристрою — від впровадження до утилізації;

Ці рекомендації спрямовані на зниження ризиків, пов'язаних з використанням мобільних пристроїв, та забезпечення захисту конфіденційної інформації в організаціях.

NIST SP 1800-21

Публікація NIST SP 1800-21 присвячена моделі COPE (Corporate-Owned, Personally-Enabled) – коли мобільні пристрої належать організації, але використовуються працівниками також у особистих цілях. Вона надає практичні рекомендації щодо конфігурації пристроїв, контролю доступу, сегрегації даних та постійного моніторингу для забезпечення безпеки таких пристроїв [14].

CIS Benchmarks та управління мобільними пристроями

CIS Controls v8 Mobile Companion Guide

Цей посібник [15], є доповненням до основної версії CIS Controls v8, яка включає 18 базових заходів кібербезпеки, та орієнтований виключно на захист мобільних пристроїв. Його ключове призначення – допомогти організаціям впровадити системний та масштабований підхід до безпеки мобільної інфраструктури. Посібник враховує специфіку мобільних платформ, таких як Android та iOS, та описує, як адаптувати кожен із основних CIS Controls до мобільних сценаріїв використання. Наприклад, такі традиційні заходи як інвентаризація пристроїв, контроль доступу, безпечне конфігурування та управління уразливостями, — отримують свою специфічну реалізацію у мобільному контексті.

Основні акценти Mobile Companion Guide:

контроль активів (Control 1–2): Рекомендовано створити окремий мобільний реєстр пристроїв, включаючи BYOD, та застосовувати політики автентифікації при реєстрації пристрою у корпоративній мережі;

захист конфігурацій (Control 4): CIS пропонує мінімально необхідні параметри безпеки для налаштування мобільних ОС, включаючи блокування екрана, шифрування пам’яті та автоматичні оновлення. Важливе місце займає кероване конфігурування через Mobile Device Management (MDM) або Enterprise Mobility Management (EMM) системи;

контроль програмного забезпечення (Control 5): Зазначається необхідність обмеження інсталяції додатків лише з перевірених джерел (App Store, Google Play), блокування сторонніх APK, та впровадження чорних/білих списків програм;

управління даними (Control 13): Рекомендовано впроваджувати контейнеризацію або розмежування корпоративних та персональних даних, особливо у BYOD-сценаріях. Наголошується на використанні механізмів шифрування та політик знищення даних при втраті пристрою або зміні статусу користувача;

моніторинг та реагування (Control 8, 16–17): Посібник радить реалізувати інструменти виявлення аномалій поведінки пристроїв, використання MDM-сповіщень, логування дій користувачів та автоматизовану реакцію на інциденти, включаючи блокування чи віддалене стирання.

Також важливо зазначити, що порівняно з ISO/IEC та NIST, які часто мають більш нормативний або стратегічний характер, CIS Controls v8 Mobile Companion Guide забезпечує практичну реалізацію стандартів безпеки, зосереджену на конфігураціях, інструментах та конкретних сценаріях. Цей документ особливо корисний для малих та середніх організацій, які шукають доступне та конкретне керівництво без необхідності масштабної сертифікації.

2.2 Порівняння технологій MDM, EMM та UEM

Mobile Device Management (MDM) визначення та функції

Mobile Device Management (MDM) – це система, що забезпечує централізоване управління мобільними пристроями в корпоративному середовищі. Основним її призначенням є дистанційне адміністрування смартфонів, планшетів та інших мобільних пристроїв, які використовуються працівниками в межах організації. Завдяки такому підходу IT-адміністратори можуть здійснювати конфігурацію пристроїв, моніторинг їх стану, оновлення програмного забезпечення, а також реалізацію заходів ІБ [16].

Як зазначено у посібнику від 42Gears “The Ultimate Guide to Mobile Device Management” [16], основними функціями MDM є можливість масової реєстрації пристроїв із попереднім завантаженням необхідного програмного забезпечення та налаштувань. Система дозволяє обирати, які саме дані про пристрій отримуватиме

адміністратор: наприклад, стан пристрою або його місцезнаходження. У разі виявлення загроз або підозрілої активності MDM надає можливість оперативного реагування шляхом дистанційного блокування чи повного видалення інформації з пристрою. Додатково реалізовано функції віддаленого технічного супроводу, що дає змогу оперативно вирішувати проблеми користувачів без фізичного доступу до пристрою.

Переваги MDM:

MDM-системи мають низку переваг, які забезпечують їх широку популярність у корпоративному середовищі. По-перше, вирізняється простота впровадження завдяки інтуїтивно зрозумілим інтерфейсам та типовим шаблонам політик безпеки. Це дозволяє швидко розгорнути базове управління без необхідності глибоких технічних знань.

По-друге, реалізується базовий рівень інформаційної безпеки, зокрема шифрування, контроль доступу, а також функція дистанційного видалення даних з пристроїв, що знижує ризики витоку конфіденційної інформації.

Однією з вагомих переваг є централізоване управління, адміністратори можуть керувати усіма пристроями організації через єдину консоль, що значно скорочує потребу в ручному налаштуванні кожного окремого пристрою.

Нарешті, більшість сучасних MDM-рішень підтримують основні мобільні операційні системи (Android, iOS, Windows), що забезпечує їх універсальність та масштабованість.

Недоліки MDM:

Попри численні переваги, використання MDM супроводжується певними обмеженнями. Одним із головних недоліків є обмежений контроль над програмним забезпеченням і даними, оскільки система зосереджена здебільшого на пристроях, а не на керуванні додатками чи вмістом. Це створює ризики у випадках, коли необхідно здійснювати контроль за поширенням або використанням корпоративної інформації. Окрему складність становить підтримка моделі BYOD (Bring Your Own Device), коли працівники використовують власні мобільні пристрої для виконання службових завдань. У таких випадках MDM може надмірно втручатися в особисті

дані користувача, що викликає невдоволення персоналу, знижує рівень довіри до роботодавця і ускладнює впровадження політик безпеки.

Enterprise Mobility Management (EMM) визначення та функції

Enterprise Mobility Management (EMM) – це розширена концепція управління мобільною інфраструктурою підприємства, а й додаткові функції управління мобільними застосунками (Mobile Application Management), корпоративним контентом (Mobile Content Management) та ідентифікацією й контролем доступу користувачів (Identity and Access Management).

Згідно з статтею Ballejos, L. “Enterprise Mobility Management (EMM)” [17], основними функціями EMM є:

Mobile Device Management (MDM): охоплює розгортання, налаштування та моніторинг мобільних пристроїв. Гарантує, що пристрої відповідають корпоративним політикам та стандартам безпеки. IT-адміністратори використовують інструменти MDM для забезпечення дотримання заходів безпеки, таких як політики паролів, шифрування та можливості віддаленого стирання;

Mobile Application Management (MAM): управління та забезпечення безпеки додатків, що працюють на корпоративних пристроях. Є можливість контролювати, які додатки можна встановлювати та використовувати на корпоративних пристроях. Також дозволяє застосовувати політики безпеки для окремих програм, такі як обмеження обміну даними між програмами. Він також підтримує розгортання корпоративних програм, надаючи доступ до необхідних інструментів без шкоди для безпеки;

Mobile Content Management (MCM): забезпечує контроль доступу до корпоративних даних, дозволяє встановлювати політики доступу, редагування або заборони копіювання;

Identity and Access Management (IAM): відповідає за автентифікацію користувачів, багатофакторний доступ та контроль над дозволами.

Переваги EMM:

Основною перевагою EMM-рішень є їх розширена функціональність, що дозволяє охопити більшість аспектів мобільної безпеки в корпоративному

середовищі.

Як зазначає Krystian, M. [18], система забезпечує глибший рівень контролю не лише за самими пристроями, а й за тим, як саме використовуються додатки, як здійснюється обмін інформацією, і яким чином організовано доступ до внутрішніх ресурсів організації. Це значно підвищує рівень захищеності конфіденційної інформації та дозволяє ефективно реагувати на сучасні кіберзагрози.

EMM також сприяє успішній реалізації стратегії BYOD, завдяки технології контейнеризації, яка дозволяє розмежовувати корпоративні та особисті дані на одному пристрої. Це, у свою чергу, забезпечує кращий баланс між корпоративною безпекою та особистою конфіденційністю, підвищуючи рівень довіри співробітників до IT-політик компанії. Додатково, за рахунок інтеграції з IAM-системами, EMM дозволяє реалізувати більш гнучкі сценарії доступу, забезпечуючи одночасно високий рівень безпеки та зручність для кінцевого користувача.

Недоліки EMM:

Незважаючи на функціональні переваги, EMM-системи мають низку суттєвих обмежень. Насамперед це стосується складності впровадження. На відміну від базового MDM, EMM включає значно ширший набір налаштувань, що потребує глибоких технічних знань з боку IT-фахівців. Як наслідок, організаціям доводиться інвестувати ресурси у підготовку персоналу або наймання спеціалізованих працівників, що веде до додаткових витрат. Крім того, управління EMM-рішенням потребує значного часу та уваги через багатофункціональність і складність конфігурації окремих модулів.

Ще одним важливим аспектом є вартість. У порівнянні з базовими системами MDM, EMM-рішення передбачають вищі витрати на ліцензії, технічну підтримку та навчання персоналу. Це може бути критичним фактором для малих та середніх підприємств, які не мають достатніх фінансових ресурсів для впровадження повноцінної EMM-інфраструктури [18].

Unified Endpoint Management (UEM) визначення та функції

Unified Endpoint Management (UEM) – це сучасна концепція управління

кінцевими точками, яка є наступним етапом розвитку технологій MDM та EMM. Вона забезпечує єдину інтегровану платформу для централізованого адміністрування всіх типів пристроїв, включаючи мобільні телефони, планшети, ноутбуки, настільні комп'ютери та інші пристрої, підключені до корпоративної мережі [18].

Як зазначає Krystian, M. [18], функціонально UEM забезпечує міжплатформне управління пристроями, синхронізацію політик безпеки, покращену видимість цифрової екосистеми, а також розширені можливості моніторингу та усунення загроз. Інтеграція з системами IAM дозволяє встановлювати єдині механізми доступу незалежно від типу пристрою або операційного середовища. В умовах сучасної гібридної та віддаленої роботи, UEM є ключовим інструментом для забезпечення безперервного доступу користувачів до корпоративних ресурсів при одночасному дотриманні політик конфіденційності та інформаційної безпеки.

Переваги UEM:

Згідно з статтею Krystian,M., "MDM vs. EMM vs. UEM: Key differences for device management." [18] , UEM має низку стратегічних переваг, які дозволяють організаціям ефективно відповідати на виклики цифровізації та зростання кількості різноманітних пристроїв в IT-інфраструктурі. Найважливішою перевагою є централізоване управління, що охоплює всі типи пристроїв та операційних систем через єдину консоль. Такий підхід не лише спрощує адміністративні процеси, а й сприяє уніфікації політик безпеки та їх узгодженому впровадженню на всіх рівнях.

Крім того, UEM забезпечує високий рівень інформаційної безпеки завдяки підтримці сучасних технологій — від поведінкової аналітики до автоматизованих механізмів виявлення та усунення загроз. Це дозволяє своєчасно реагувати на потенційні інциденти безпеки та мінімізувати ризики витоку або втрати корпоративної інформації. Важливою перевагою є також покращений користувацький досвід: інтелектуальні політики дозволяють враховувати контекст роботи користувача, надаючи гнучкий і безпечний доступ до ресурсів з будь-якого пристрою.

Недоліки UEM:

Разом із потужною функціональністю UEM має і суттєві недоліки, зокрема високу вартість впровадження. Вартість ліцензування, обслуговування, навчання персоналу та інтеграції з існуючими IT-системами часто перевищує можливості малих і середніх підприємств. За словами Krystian, M. [18], UEM є найдорожчим рішенням серед систем управління мобільною інфраструктурою, що може обмежувати його використання у невеликих організаціях або тих, що мають обмежений IT-бюджет.

Ще однією проблемою є складність налаштування та інтеграції. Успішне впровадження UEM вимагає ретельного планування, знання наявної IT-інфраструктури та кваліфікованих спеціалістів. Окрему увагу необхідно приділити дотриманню балансу між безпекою та конфіденційністю, особливо в умовах BYOD. Розширені можливості контролю, які реалізуються в UEM, можуть зачіпати особисті дані працівників, що потребує чіткого визначення політик конфіденційності та юридично обґрунтованого врегулювання доступу до приватної інформації.

Порівняльний аналіз MDM, EMM та UEM

З метою узагальнення та систематизації основних характеристик систем управління мобільними пристроями, у табл. 2.1, наведено порівняльний аналіз технологій MDM, EMM та UEM. Порівняння здійснено за низкою ключових параметрів, ключових параметрів, зокрема: основним призначенням системи, функціональними можливостями, охопленням типів підтримуваних пристроїв, здатністю до управління додатками та корпоративним контентом, рівнем забезпечення ІБ, підтримкою моделі BYOD, складністю впровадження, фінансовими витратами, а також цільовими користувачами. Такий підхід дозволяє сформувати цілісне уявлення про функціональні відмінності між зазначеними рішеннями, а також визначити доцільність їх застосування залежно від специфіки завдань, які стоять перед підприємством у сфері управління кінцевими точками та забезпечення їх безпеки.

Таблиця 2.1.

Порівняння технологій управління мобільними пристроями

Критерій	MDM	EMM	UEM
Основне призначення	Управління мобільними пристроями	Розширене управління мобільними пристроями, додатками, контентом і доступом	Єдине управління всіма типами кінцевих пристроїв (мобільні, ПК, IoT)
Функціональність	Конфігурація, моніторинг, оновлення, безпека пристроїв	Включає MDM, MAM (додатки), MCM (контент), IAM (ідентифікація)	Включає всі функції EMM + управління ПК, ноутбуками, ін. пристроями, поведінковий аналіз, виявлення загроз
Управління додатками/контентом	Обмежене	Повноцінне управління корпоративними додатками та даними	Повноцінне, із можливістю узгодження політик на всіх пристроях
Підтримка BYOD	Часткова, можливе втручання в особисті дані користувачів	Підтримується завдяки контейнеризації	Повна підтримка з урахуванням контексту, конфіденційності, безпеки
Платформи, що підтримуються	Android, iOS, Windows	Android, iOS, Windows (в основному мобільні)	Android, iOS, Windows, macOS, Linux, Chrome OS, IoT-пристрої
Рівень ІБ	Базовий (шифрування, контроль доступу, стирання даних)	Підвищений (контроль на рівні додатків, даних, користувача)	Високий (виявлення загроз, поведінковий аналіз, автоматичне реагування)

Продовження таблиці 2.1

Порівняння технологій управління мобільними пристроями

Критерій	MDM	EMM	UEM
Переваги	Простота впровадження, базовий захист, централізоване управління	Комплексність, безпечне BYOD, контроль на рівні додатків і даних	Універсальність, масштабованість, висока безпека, зручність для користувача
Недоліки	Обмежений контроль над програмами та контентом, недосконала підтримка BYOD	Складність налаштування, потреба у кваліфікованих кадрах, вища вартість	Висока складність впровадження та інтеграції, висока вартість, ризик порушення конфіденційності персональних даних
Складність впровадження	Низька – проста конфігурація, не потребує високої кваліфікації	Середня – потребує підготовленого персоналу, складні політики	Висока – складна інтеграція з IT-інфраструктурою, вимагає досвіду
Фінансові витрати	Низькі – базова ліцензія, мінімальні витрати на впровадження	Середні – потреби в навчанні, розширені ліцензії	Високі – дорога ліцензія, висока вартість обслуговування, додаткові витрати на інтеграцію
Цільові користувачі/організації	Малі та середні компанії з базовими потребами управління	Середній та великий бізнес, що працює з корпоративними даними	Великі підприємства з гібридним або віддаленим IT-середовищем

2.3 Аналіз функціоналу провідних рішень (Microsoft Intune та VMware Workspace ONE)

Аналіз функціоналу Microsoft Intune

Загальна характеристика Microsoft Intune

Microsoft Intune – це хмарне рішення для уніфікованого управління кінцевими точками (UEM), що забезпечує централізоване адміністрування мобільних пристроїв, комп'ютерів, додатків та політик безпеки. Завдяки інтеграції з Microsoft Entra ID (раніше Azure Active Directory) та сервісами Microsoft 365 платформа дозволяє створити єдине кероване середовище для пристроїв, що належать організації, а також для пристроїв у моделі Bring Your Own Device (BYOD), що особливо важливо в умовах зростаючої мобільності працівників [19].

Intune підтримує керування пристроями на базі різних операційних систем, зокрема Windows, macOS, iOS, Android і Linux, що дозволяє забезпечити однаковий рівень контролю незалежно від типу пристрою. Крім того, інтеграція з іншими рішеннями Microsoft, зокрема Microsoft Defender та Endpoint Analytics, дозволяє реалізувати цілісний підхід до управління IT-інфраструктурою [19].

Також це рішення надає адміністраторам низку важливих функцій, зокрема можливість керувати пристроями на різних платформах, розгортати та конфігурувати додатки, застосовувати політики безпеки та відповідності, використовувати аналітичні інструменти для моніторингу стану пристроїв і програмного забезпечення, а також інтегруватися з іншими сервісами Microsoft з метою побудови єдиного керованого середовища. Завдяки такому функціональному наповненню Microsoft Intune є потужним інструментом для забезпечення контролю, безпеки та ефективного адміністрування IT-інфраструктури в організаціях.

Управління пристроями

Microsoft Intune охоплює повний життєвий цикл управління пристроями – від реєстрації до виведення з експлуатації. Наприклад, для пристроїв з ОС Windows реалізована підтримка автоматичного налаштування за допомогою Windows Autopilot, тоді як для пристроїв Apple і Android використовуються Apple Business

Manager і Android Enterprise відповідно. Інструменти платформи дозволяють створювати профілі конфігурації для основних параметрів (Wi-Fi, VPN, електронна пошта), реалізовувати політики безпеки (вимоги до паролів, шифрування), керувати оновленням програмного забезпечення, а також здійснювати віддалене блокування чи повне очищення пристрою у разі потреби [20].

Управління додатками

Microsoft Intune пропонує засоби для розгортання та конфігурації корпоративних додатків із внутрішніх джерел, так і використання додатків із офіційних магазинів, зокрема Microsoft Store, Apple App Store та Google Play. За допомогою політик захисту додатків Intune дозволяє обмежити небажану взаємодію між застосунками, наприклад, заборонити копіювання даних або передачу інформації між додатками, що знижує ризики витоку конфіденційної інформації Також платформа підтримує автоматичне оновлення додатків до останніх версій, що забезпечує актуальність ПЗ [21].

Політики відповідності та умовного доступу (Compliance and Conditional Access)

Microsoft Intune дозволяє встановлювати політики відповідності, які визначають, вимоги до пристрою для отримання доступу до корпоративних ресурсів, зокрема актуальність ОС, ввімкнене шифрування та відсутність root/jailbreak-доступу.

Завдяки інтеграції з Microsoft Entra ID реалізується умовний доступ, який обмежує доступ до ресурсів на основі відповідності пристрою. Наприклад, обмеження доступу до корпоративної пошти лише з пристроїв, які відповідають встановленим політикам безпеки [22].

Аналітика та звітність (Analytics and Reporting)

З метою підвищення прозорості в управлінні IT-інфраструктурою Microsoft Intune включає аналітичні інструменти, серед яких Endpoint Analytics. Вони дозволяють виявляти фактори, що знижують продуктивність, а також формувати рекомендацій щодо їх усунення. Крім того, адміністратори мають доступ до

детальних звітів про відповідність пристроїв політикам, журналів аудиту змін, та інформації про вразливості в інтеграції з Microsoft Defender [19].

Додаткові можливості та інтеграції

Microsoft Intune також пропонує додаткові функціональні можливості через Microsoft Intune Suite, серед яких варто відзначити Remote Help — інструмент для віддаленої підтримки користувачів; Endpoint Privilege Management — засіб контролю привілеїв на рівні пристрою; та Advanced Analytics — рішення для поглибленого аналізу ризиків, продуктивності та безпеки [19].

Переваги та обмеження Microsoft Intune

Насамперед серед основних переваг використання Microsoft Intune варто виокремити: хмарну архітектуру, що не вимагає локальної інфраструктури; централізоване управління широким спектром пристроїв і додатків; підтримку мультиплатформного середовища (Windows, macOS, iOS, Android, Linux); масштабованість і адаптивність до потреб організацій різного масштабу. Крім того, платформа дозволяє ефективно впроваджувати сучасні підходи до інформаційної безпеки, зокрема Zero Trust, завдяки механізмам умовного доступу та аналітики стану пристроїв. Також у порівнянні з іншими засобами управління мобільними пристроями, такими як VMware Workspace ONE чи IBM MaaS360, Microsoft Intune демонструє високий рівень інтеграції з корпоративною інфраструктурою Microsoft, що робить його найбільш привабливим для організацій, які вже використовують продукти Microsoft 365 [19][20].

Водночас Intune має і певні обмеження. Зокрема, значною вадою є залежність від стабільного інтернет-з’єднання, яке є критично необхідним для коректного функціонування хмарних сервісів. Окрім цього, первинне налаштування платформи може бути складним для нових користувачів або організацій, які не мають досвіду роботи з екосистемою Microsoft. Також існує обмежена підтримка деяких IoT-пристроїв, які не відповідають стандартним вимогам системи, що може ускладнити впровадження в специфічних середовищах [21].

Аналіз функціоналу VMware Workspace ONE

Загальна характеристика VMware Workspace ONE

VMware Workspace ONE — це комплексна UEM-платформа для уніфікованого управління кінцевими точками, яка забезпечує централізоване управління мобільними пристроями, комп'ютерами, додатками та політиками безпеки. Вона дозволяє організаціям ефективно контролювати доступ до корпоративних ресурсів, забезпечуючи високий рівень безпеки та зручність для користувачів. До основних її компонентів належать Workspace ONE Access для забезпечення єдиного входу та контролю ідентичності, Workspace ONE Intelligence для аналітики й автоматизації, а також Workspace ONE Tunnel для захищеного VPN-доступу до корпоративних ресурсів [23].

Платформа орієнтована на побудову безпечного та адаптивног о середовища доступу, забезпечуючи контроль над усіма аспектами взаємодії користувача з корпоративною інфраструктурою. Завдяки багаторівневій архітектурі Workspace ONE є придатним для реалізації сучасних сценаріїв роботи, включаючи віддалену або гібридну модель.

Управління пристроями та реєстрація

VMware Workspace ONE підтримує різні моделі управління пристроями, що дозволяє організаціям адаптувати підходи до різних сценаріїв використання:

повне управління (UEM Managed) – пристрій повністю контролюється адміністраторами, що дозволяє застосовувати всі політики безпеки та конфігурації;

розділене управління (OS Partitioned) – дозволяє розділити особисті та робочі дані на пристрої, забезпечуючи конфіденційність користувача та контроль над корпоративними даними;

реєстрація через Hub (Hub Registered) – пристрій реєструється в системі без повного управління, що підходить для BYOD-сценаріїв;

управління на рівні додатків (App Level Management) – дозволяє застосовувати політики безпеки до окремих додатків без управління всім пристроєм [24].

Завдяки цим моделям платформа забезпечує високий рівень гнучкості, дозволяючи організаціям самостійно визначати оптимальну стратегію управління залежно від рівня ризиків та очікувань з боку кінцевих користувачів.

Управління додатками та контентом

Платформа VMware Workspace ONE підтримує розгортання різних типів додатків, включаючи публічні, внутрішні та веб-додатки, і дозволяє реалізувати політики безпеки, зокрема шифрування, контроль копіювання та автентифікацію. Крім того, компонент Workspace ONE Content дає змогу організувати безпечний мобільний доступ до корпоративних документів і файлів, підтримуючи принципи захищеного інформаційного обміну [23].

Політики відповідності та умовний доступ

VMware Workspace ONE має гнучкі механізми встановлення політик відповідності пристроїв, що дозволяють перевірити, чи відповідає пристрій встановленим корпоративним стандартам — зокрема наявності шифрування, актуальній версії операційної системи, відсутності root/jailbreak-доступу тощо. Ці перевірки реалізуються у взаємодії з компонентом Workspace ONE Access, який, своєю чергою, забезпечує умовний доступ — механізм, що дозволяє надавати або блокувати доступ до ресурсів залежно від відповідності пристрою встановленим політикам [24][25].

Таким чином, організація може, наприклад, дозволити доступ до пошти чи CRM-системи лише з перевірених і належно захищених пристроїв, що значно підвищує рівень загальної інформаційної безпеки.

Аналітика та автоматизація

Компонент Workspace ONE Intelligence забезпечує розширену функціональність аналітики за допомогою збору й обробки даних з пристроїв, додатків і взаємодії користувачів. Аналітична інформація використовується не лише для формування звітів, але й для запуску автоматизованих сценаріїв реагування. Наприклад, у разі виявлення підозрілої активності пристрій може бути автоматично заблокований або ізольований від мережі, що дозволяє мінімізувати час реагування на інциденти [24].

Інтеграція та додаткові можливості

VMware Workspace ONE підтримує тісну інтеграцію з іншими корпоративними рішеннями. Зокрема, підтримується взаємодія з VMware Horizon для реалізації віртуалізованих робочих столів, Workspace ONE Assist для віддаленої технічної підтримки, а також з рішенням VMware Carbon Black, що забезпечує розширений захист від загроз та поведінкову аналітику. Така інтеграційна екосистема підвищує загальну ефективність платформи та дозволяє комплексно вирішувати завдання IT-безпеки [25].

Переваги та обмеження VMware Workspace ONE

До ключових переваг VMware Workspace ONE належать: універсальність у застосуванні завдяки підтримці різних сценаріїв управління; широка функціональність, що охоплює управління пристроями, додатками, політиками безпеки, аналітикою та автоматизацією; хмарна архітектура, яка дозволяє масштабувати рішення без додаткових витрат на локальну інфраструктуру; інтеграція з потужними захисними інструментами, такими як Carbon Black; а також підтримка політик Zero Trust через умовний доступ і багатофакторну автентифікацію [23][24].

Разом із тим, серед недоліків платформи варто відзначити високу залежність від стабільного інтернет-з’єднання, що ускладнює роботу в офлайн-сценаріях; складність первинного налаштування, що потребує відповідної підготовки IT-фахівців; а також обмеження у підтримці деяких спеціалізованих пристроїв або нішевих платформ, що може вплинути на повноцінне впровадження в специфічних галузях [26].

Порівняльний аналіз Microsoft Intune та VMware Workspace ONE

З метою узагальнення та систематизації ключових функціональних характеристик провідних рішень для уніфікованого управління кінцевими точками, у табл. 2.2 наведено порівняльний аналіз платформ Microsoft Intune та VMware Workspace ONE. Оцінювання здійснюється за такими критеріями, як тип платформи, підтримка операційних систем, моделі управління пристроями, можливості розгортання та захисту додатків, реалізація політик відповідності та

умовного доступу, аналітичні засоби, інтеграційні можливості, а також основні переваги й обмеження. Представлений аналіз дає змогу здійснити обґрунтований вибір найбільш релевантного UEM-рішення відповідно до потреб конкретної організації та рівня вимог до безпеки, масштабованості й функціональності

Таблиця 2.2

Порівняльний аналіз Microsoft Intune та VMware Workspace ONE

Критерій	Microsoft Intune	VMware Workspace ONE
Тип платформи	Хмарна UEM, інтегрована в екосистему Microsoft	Хмарна/гібридна UEM-платформа з багаторівневою архітектурою
Підтримка ОС	Windows, macOS, iOS, Android, Linux	Windows, macOS, iOS, Android, Linux, ChromeOS, певні IoT-пристрої
Управління пристроями	Стандартне UEM-управління з автоконфігурацією (Autopilot, Apple/Android Enrollment)	Підтримка моделей UEM Managed, Hub Registered, App-Level Management
Управління додатками	Розгортання, політики захисту, оновлення	Розгортання, захист і контент-менеджмент через Workspace ONE Content
Політики відповідності	Перевірка ОС, шифрування, root/jailbreak, інтеграція з Entra ID	Перевірка відповідності та умовний доступ через Workspace ONE Access
Умовний доступ	Через Microsoft Entra ID	Через Workspace ONE Access
Аналітика	Endpoint Analytics, звіти, аудит, інтеграція з Microsoft Defende	Workspace ONE Intelligence, автоматизовані сценарії реагування
Інтеграція	Продукти Microsoft: M365, Defender, Entra ID	Horizon, Assist, Carbon Black, зовнішні SIEM/EDR
Переваги	Інтеграція з Microsoft, масштабованість, Zero Trust, аналітика, умовний доступ, мультиплатформність	Гнучкість моделей управління, автоматизація, розширена інтеграція, контент-менеджмент

Продовження таблиці 2.2

Порівняльний аналіз Microsoft Intune та VMware Workspace ONE

Критерій	Microsoft Intune	VMware Workspace ONE
Обмеження	Залежність від інтернету, складність первинного налаштування, обмежена підтримка деяких IoT-пристроїв	Аналогічні: залежність від зв'язку, складне налаштування, обмежена підтримка нішових пристроїв
Фінансові витрати	Низькі – Intune Plan 1 ($8/користувач/міс.) для малого бізнесу; Середні – Intune Suite ($10 додатково для Enterprise); Високі – включення E3/E5 або інтеграції з Defender ($32–57/користувач/міс.)	Низькі – Standard план ($6.18–6.52/користувач/міс.); Середні – Advance/Enterprise ($10–15); Високі – VDI-Enterprise ($20–25/користувач/міс.), плюс додаткові витрати на підтримку й інфраструктуру
Цільові користувачі/організації	Малі та середні компанії з базовими потребами керування (Intune Plan 1); Середні, що потребують розширеного контролю (Suite); Великі підприємства — при інтеграції з M365 E3/E5	Малі та середні компанії — Standard та Advanced; Середні/великі підприємства, що працюють з аналітикою — Enterprise; Великі організації з VDI-середовищем — VDI-Enterprise

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

3.1 Узагальнений алгоритм впровадження системи управління мобільними пристроями (на базі MDM)

Ефективне управління мобільними пристроями в сучасній організації потребує системного підходу. Одним з найоптимальніших рішень є впровадження системи MDM, яка дозволяє централізовано контролювати мобільну інфраструктуру, реалізовувати політики безпеки та мінімізувати ризики витоку конфіденційної інформації. У цьому підрозділі наведено узагальнений алгоритм впровадження MDM-системи, що охоплює всі етапи – від початкового аналізу до повноцінного супроводу.

Оцінка бізнес-потреб та ризиків

Початковим етапом упровадження MDM є глибокий аналіз бізнес-потреб організації. Основною метою цього етапу є визначення функціональних завдань, які має вирішувати система, а також формування чітких цілей впровадження. Необхідно встановити, які підрозділи організації активно використовують мобільні пристрої у своїй діяльності, які саме бізнес-процеси здійснюються з їхньою допомогою, які види інформації обробляються (персональні дані клієнтів, фінансова документація, внутрішні звіти тощо), а також які сервіси та додатки при цьому застосовуються.

Паралельно здійснюється оцінка ризиків, яка включає ідентифікацію потенційних загроз, таких як втрата пристроїв, компрометація облікових даних, зараження шкідливим програмним забезпеченням або несанкціонований доступ до корпоративних ресурсів. Ретельний аналіз ризиків дозволяє не лише визначити ймовірність виникнення інцидентів, але й оцінити їх можливі наслідки для

організації. Отримані результати стають підґрунтям для формування вимог до майбутньої MDM-системи.

Аналіз поточного стану мобільної інфраструктури

Другим кроком є детальний аналіз існуючої мобільної інфраструктури. На цьому етапі здійснюється інвентаризація всіх мобільних пристроїв, що перебувають в експлуатації в організації, визначаються їхні технічні характеристики, версії операційних систем, використовувані канали зв'язку (Wi-Fi, VPN, мобільні мережі). Також проводиться класифікація пристроїв за моделями їхнього використання: корпоративні, особисті (BYOD), корпоративні з дозволеним обмеженим особистим використанням (COPE), або персоналізований вибір пристроїв (CYOD).

Важливо оцінити наявність застарілих версій операційних систем, наявність рутованих (root) або джейлбрейкнутих (jailbreak) пристроїв, які є особливо вразливими до атак. Особлива увага приділяється ідентифікації встановлених сторонніх додатків, що можуть нести ризики ІБ.

Формування політик управління пристроями (включно з правовими обмеженнями)

На основі проведеного аналізу формується комплекс внутрішніх політик, які регулюють усі аспекти роботи з мобільними пристроями. Саме на цьому етапі враховуються як внутрішні потреби організації, так і чинне законодавство з питань захисту персональних даних (наприклад, GDPR, ISO 27001, PCI DSS, локальні нормативно-правові акти).

Політика реєстрації та авторизації встановлює правила додавання нових пристроїв до системи, порядок їх автентифікації з використанням багатофакторних механізмів та сертифікатів.

Політика розмежування особистих та корпоративних даних визначає заходи ізоляції корпоративної інформації за допомогою контейнеризації робочого середовища, що дозволяє відокремити корпоративні ресурси від особистих даних співробітника.

Політика управління додатками встановлює перелік дозволених додатків, процедури їх оновлення, а також обмеження на встановлення стороннього програмного забезпечення.

Політика захисту даних передбачає шифрування інформації як на пристрої, так і при її передачі, обов'язкове резервне копіювання та автоматичне блокування пристроїв у разі тривалої бездіяльності.

Політика реагування на інциденти визначає порядок повідомлення про втрату пристрою або підозру на його компрометацію, алгоритми дистанційного стирання (wipe) даних та процедури розслідування інцидентів.

Вибір архітектури MDM-рішення

Наступним кроком є визначення архітектурної моделі MDM-системи з урахуванням масштабів організації, її бізнес-потреб та обмежень інформаційної безпеки. Виділяють три основні моделі:

хмарна – забезпечує швидке розгортання, масштабованість та зниження витрат на інфраструктуру, але потребує ретельного захисту при передачі даних за межі організації;

локальна – забезпечує повний внутрішній контроль, але потребує значних інвестицій у серверне обладнання та обслуговування;

гібридна – дозволяє поєднати переваги обох моделей, забезпечуючи гнучкість налаштувань.

При виборі конкретного рішення обов'язково враховується підтримка різних операційних систем (Android, iOS, Windows), функціональних можливостей системи (управління оновленнями, шифрування, контроль доступу, видалення даних), сумісність з наявною інфраструктурою (Active Directory, Entra ID, VPN, SIEM тощо) та фінансові аспекти володіння системою.

Технічна підготовка інфраструктури до розгортання

Після вибору архітектури проводиться технічна підготовка інфраструктури. Вона включає:

налаштування серверної частини MDM-системи;

підключення до корпоративних служб ідентифікації (Active Directory, IAM);

забезпечення захищених каналів передачі даних (VPN, SSL/TLS);

резервне копіювання конфігураційних даних;

створення тестового середовища для апробації налаштувань і політик.

На цьому етапі важливо закласти технічну основу для стабільної та безпечної роботи системи.

Інтеграція з іншими службами безпеки

Для побудови комплексної системи захисту мобільні пристрої мають стати частиною загальної системи інформаційної безпеки організації. Інтеграція передбачає:

синхронізацію з антивірусними рішеннями та системами моніторингу (SIEM, EDR, XDR, SOAR);

взаємодію з системами аудиту, журналювання дій користувачів та адміністраторів;

централізоване управління правами доступу та обліковими записами.

Таке об'єднання дозволяє забезпечити єдине вікно моніторингу стану безпеки мобільних пристроїв поряд з іншими активами організації.

Підготовка персоналу та внутрішніх процесів

Реалізація MDM-системи потребує не лише технічних налаштувань, а й підготовки людських ресурсів. ІТ-фахівці мають пройти навчання з налаштування, підтримки та оперативного реагування на інциденти в рамках системи MDM. Користувачі повинні бути ознайомлені з новими правилами роботи, пройти навчання з основ кібергігієни, правил безпечного використання мобільних пристроїв та способів повідомлення про інциденти.

Крім того, доцільно створити спеціалізовану групу підтримки, яка оперативно реагуватиме на технічні запити користувачів, допомагатиме у налаштуваннях пристроїв, контролюватиме виконання політик безпеки та супроводжуватиме процеси оновлення системи.

Поетапне розгортання системи (зокрема, реєстрація та налаштування пристроїв)

Впровадження системи управління здійснюється поетапно, щоб мінімізувати можливі ризики та збої. Пілотне впровадження передбачає запуск системи на обмеженій групі пристроїв різних підрозділів з метою перевірки працездатності та ефективності політик.

На основі результатів пілотного запуску проводиться оптимізація налаштувань, після чого відбувається масштабне розгортання системи на всі пристрої організації. Реєстрація пристроїв у MDM-системі може здійснюватися вручну або за допомогою автоматизованих механізмів: QR-кодів, NFC, Apple Business Manager, Android Zero-touch Enrollment, Windows Autopilot.

Після реєстрації пристрої автоматично отримують необхідне програмне забезпечення, профілі безпеки, налаштування мережі, доступу до корпоративних сервісів та застосовуються політики контролю.

Моніторинг та оцінювання відповідності

Після розгортання системи розпочинається постійний моніторинг дотримання встановлених політик. Система MDM проводить перевірку відповідності конфігурацій вимогам безпеки, фіксує підозрілі дії (зміни геолокації, несанкціоновані підключення, модифікації системних файлів), формує звіти для адміністраторів. У разі виявлення порушень застосовуються автоматичні заходи реагування – блокування пристроїв, обмеження доступу, генерація сповіщень відповідальним особам.

Аудит, аналіз ефективності

Регулярне проведення аудитів дозволяє контролювати ефективність функціонування системи. Під час аудитів перевіряється актуальність політик, відповідність конфігурацій нормативним вимогам, аналізуються інциденти, оцінюється результативність прийнятих заходів реагування. Зібраний зворотний зв’язок від користувачів і адміністраторів дає змогу виявити проблемні аспекти та удосконалити політики.

Постійна підтримка та вдосконалення системи

MDM-система потребує постійного розвитку, оскільки змінюються як загрози інформаційній безпеці, так і бізнес-потреби організації. Необхідно

систематично оновлювати програмне забезпечення MDM, адаптувати політики до нових ризиків, проводити підвищення кваліфікації ІТ-персоналу. Перед впровадженням нових функцій і оновлень обов’язковим є їх тестування на відповідність вимогам стабільності роботи та сумісності з новими версіями операційних систем пристроїв.

3.2 Рекомендації щодо формування політики управління мобільними пристроями

Загальні засади формування політики управління

Управління мобільними пристроями потребує формалізованого підходу, заснованого на чітко визначеній політиці безпеки, яка охоплює як технічні, так і організаційні аспекти. Політика управління мобільними пристроями має виконувати кілька взаємопов’язаних функцій. По-перше, вона встановлює вимоги до безпечного використання мобільних пристроїв у середовищі організації. По-друге, визначає механізми захисту даних і контролю доступу. По-третє, вона формує нормативну основу для взаємодії між ІТ-підрозділом та кінцевими користувачами в питаннях відповідальності, реєстрації, інцидентного реагування тощо.

Розробка політики управління мобільними пристроями повинна базуватись на оцінці актуальних ризиків, специфіки бізнес-процесів, типів пристроїв, які використовуються персоналом, та способів їх підключення до корпоративної інфраструктури. Урахування зовнішніх факторів, таких як галузеве регулювання або стандарти безпеки, теж є необхідною умовою. Важливо, щоб політика залишалася адаптивною – вона повинна не лише фіксувати поточні правила, а й передбачати механізми оновлення у відповідь на появу нових технологій, загроз або змін у законодавстві.

Визначення цілей, охоплення та сфери дії політики

Першим етапом формування політики є формалізація її цілей, обсягу охоплення та визначення об'єктів регулювання. Політика має бути спрямована на

забезпечення захисту корпоративної інформації у процесі використання мобільних пристроїв, встановлення правил і процедур контролю над доступом до інформаційних ресурсів, а також регулювання відповідальності користувачів. Важливо визначити, на кого поширюється політика: працівників, підрядників, консультантів, партнерів, які використовують мобільні пристрої для взаємодії з ІС організації. В межах охоплення політики слід також чітко окреслити, які типи пристроїв регулюються: лише корпоративні, або й особисті (у межах BYOD). В останньому випадку політика повинна передбачати заходи сегментації даних, механізми захисту особистої інформації та обов'язковість встановлення керованого ПЗ.

Класифікація мобільних пристроїв і відповідність рівню доступу

Після того як окреслено загальні межі політики, доцільним є перехід до класифікації мобільних пристроїв. Політика управління мобільними пристроями повинна базуватися на системному поділі пристроїв за рядом критеріїв, серед яких тип пристрою (смартфон, планшет, ноутбук, гібридні модулі), тип операційної системи (наприклад, Android, iOS, Windows), модель власності (корпоративна, особиста, змішана) та рівень доступу, необхідний для виконання посадових обов'язків. Зіставлення цих критеріїв дозволить виділити групи пристроїв з різним ступенем критичності.

Залежно від категорії, для кожного пристрою мають бути визначені відповідні обмеження, вимоги, засоби захисту є обов'язковими для конкретного класу пристроїв, а також встановлюється ступінь контролю з боку адміністрації. Наприклад, пристрої, які підключаються до фінансових або адміністративних систем, повинні відповідати найвищим стандартам безпеки, включно з багатофакторною автентифікацією, активним шифруванням, моніторингом активності та регулярною перевіркою відповідності. Натомість пристрої, що мають доступ лише до загальної інформації (наприклад, календар або внутрішній портал), можуть підпадати під менш жорсткі вимоги.

Застосування такого підходу дозволить забезпечити баланс між рівнем безпеки та продуктивністю працівників, а також уникнути надмірного

адміністрування. У майбутньому це також полегшить автоматизацію управління пристроями за допомогою систем MDM, EMM або UEM оскільки класифікація створить логічну структуру для застосування політик керування.

Визначення технічних вимог до безпеки мобільних пристроїв

Після завершення класифікації необхідно сформувати конкретні вимоги до безпеки мобільних пристроїв, які відповідають рівню їхнього ризику та типу доступу до інформаційних ресурсів. Це один із найбільш критичних компонентів політики, оскільки саме технічні засоби забезпечують фактичну реалізацію запланованих заходів контролю.

На цьому етапі формулюються базові параметри конфігурації пристроїв, які мають застосовуватись перед початком їх використання в корпоративному середовищі. До таких параметрів належать: обов’язкове використання засобів автентифікації (складні паролі або біометричні дані), автоматичне блокування пристрою після певного часу бездіяльності, шифрування даних, що зберігаються на пристрої, а також регулярне оновлення операційної системи й критичного програмного забезпечення.

Важливим технічним обмеженням є заборона використання пристроїв із модифікованими (рутованими або джейлбрейкнутими) операційними системами. Такі пристрої, навіть за наявності формальних захисних механізмів, фактично не здатні забезпечити належний рівень контролю на рівні ядра системи та стають потенційно небезпечними для всієї корпоративної мережі. У зв’язку з цим політика повинна прямо забороняти використання подібних пристроїв або передбачати їхню автоматичну ізоляцію від внутрішніх ресурсів.

Окрему увагу слід приділити механізмам видаленого керування, зокрема можливості дистанційного стирання корпоративних даних у разі втрати пристрою або виникнення підозри на його компрометацію. Наявність такого функціоналу – важлива передумова динамічного реагування на інциденти безпеки. Технічні вимоги мають бути інтегровані в MDM-систему і відповідати категорії пристрою згідно з попереднім етапом класифікації.

Реєстрація пристроїв і автентифікація користувачів

Після встановлення технічних вимог до мобільних пристроїв важливою складовою політики стає забезпечення їхньої реєстрації в централізованій системі управління. Без належної ідентифікації пристроїв і прив'язки до конкретних користувачів неможливо реалізувати контроль доступу, моніторинг дій та ефективне реагування на інциденти. Цей етап спрямований на формалізацію процесу включення мобільного пристрою до інформаційного середовища організації та перевірку його відповідності вимогам безпеки.

Процес реєстрації передбачає попередню перевірку пристрою на відповідність мінімальним критеріям, описаним у попередньому етапі. У межах цього процесу встановлюються відповідні компоненти керування, зокрема MDM або EMM-клієнти, які забезпечують зв'язок між пристроєм і серверною частиною системи управління мобільністю. Також проводиться фіксація даних про пристрій (модель, серійний номер, ОС, власник) у внутрішньому реєстрі. Кожен мобільний пристрій має бути однозначно асоційований з особою, яка несе за нього відповідальність.

Невід'ємним елементом безпечного підключення є автентифікація користувача. На цьому етапі організація повинна впровадити багатофакторну автентифікацію (MFA) для всіх пристроїв, що отримують доступ до конфіденційної або критичної інформації. Комбінація щонайменше двох факторів – знання (наприклад, пароль), володіння (токен або сертифікат), або біометрії (відбиток пальця, розпізнавання обличчя) – є сучасним стандартом, який суттєво знижує ймовірність несанкціонованого доступу.

Реєстрація та автентифікація виконують не лише технічну, а й правову функцію, оскільки фіксують відповідальну особу за кожен пристрій і створюють основу для аудиту дій у майбутньому. Це, у свою чергу, підсилює цілісність політики управління мобільними пристроями в цілому.

Керування оновленнями та уразливостями

Наявність навіть найсучасніших засобів захисту не гарантує безпеки, якщо ОС або додатки залишаються неоновленими. Саме тому політика управління мобільними пристроями повинна містити положення щодо регулярного оновлення

ПЗ. Цей етап має на меті впровадження циклу керування уразливостями – процесу, за допомогою якого забезпечується оперативне реагування на появу нових загроз через оновлення компонентів системи.

Політика повинна передбачати, що кожен пристрій, який підключається до ІС організації, повинен мати активоване автоматичне оновлення ОС та застосунків. Централізоване керування оновленнями через MDM-рішення дозволяє адміністраторам контролювати статус оновлень, встановлювати обмеження на використання застарілих версій ПЗ та автоматично розгортати патчі на визначену групу пристроїв.

Крім того, слід передбачити механізм ізоляції пристроїв, які не відповідають критичним вимогам до безпеки. Така ізоляція може реалізовуватися шляхом обмеження доступу до ресурсів, блокування VPN-з'єднань або повного тимчасового відключення пристрою від корпоративної інфраструктури. Така тактика є превентивною і дозволяє зменшити ризик компрометації даних через відомі вразливості.

Ефективність цього етапу значною мірою залежить від синхронізації політики управління мобільними пристроями із загальною стратегією управління ІТ-активами в організації. Лише за умови тісної взаємодії між відділом безпеки, системними адміністраторами та кінцевими користувачами можна досягти належного рівня захищеності мобільного середовища.

Контроль за мобільними додатками

У сучасному інформаційному середовищі особливу загрозу становлять не лише пристрої як такі, а й ПЗ, яке на них інсталюється. Велика кількість мобільних додатків має потенційний доступ до конфіденційної інформації, геолокаційних даних, мікрофона, камери та інших чутливих ресурсів. У зв'язку з цим політика повинна чітко регламентувати правила використання мобільного ПЗ, що встановлюється на пристроях, які взаємодіють із корпоративною мережею.

Перш за все, слід визначити перелік дозволених додатків (так званий "білий список"), які схвалені для використання в межах організації. До таких можуть належати офіційні поштові клієнти, VPN-клієнти, засоби комунікації, внутрішні

корпоративні застосунки. Інше ПЗ може бути дозволено за погодженням з IT-відділом або за умови використання в ізольованому середовищі.

У разі використання BYOD-пристроїв політика повинна передбачати ізоляцію корпоративного середовища від особистого через контейнеризацію, віртуалізацію або створення захищених сесій. Такий підхід дозволяє зберігати контроль над службовими даними без доступу до особистої інформації працівника. Забороняється встановлення програм із невідомих джерел, додатків із високим рівнем ризику (наприклад, анонімних месенджерів, сторонніх файлових обмінників), а також софту, який дублює функціональність захищених корпоративних сервісів.

Реалізація політики контролю додатків сприяє зниженню ризику несанкціонованого витоку інформації, підвищенню загального рівня цифрової гігієни користувачів і забезпечує кращу прогнозованість функціонування мобільного середовища. Цей етап є ключовим для запровадження моделі нульової довіри (Zero Trust) у мобільному контексті, яка ґрунтується на постійному контролі кожного елемента – пристрою, користувача, додатку та з'єднання.

Регламентація поведінки користувачів

Жодна система технічних засобів безпеки не є ефективною без належного регламентування поведінки самих користувачів. У політиці управління мобільними пристроями особливе значення набувають правила, що визначають допустимі дії персоналу, обмеження та обов’язки у процесі взаємодії з корпоративними ресурсами. Цей етап передбачає формування комплексу вимог, дотримання яких знижує ризики, пов’язані з необережністю, неуважністю або навмисними діями користувачів.

Поведінкові обмеження мають охоплювати як фізичні, так і цифрові аспекти використання мобільних пристроїв. До них належать заборона на підключення до відкритих Wi-Fi мереж без VPN-захисту, зобов’язання негайно повідомляти відповідальні служби у разі втрати пристрою, виявлення підозрілої активності або спроби несанкціонованого доступу. Також доцільно закріпити заборону на

копіювання службових даних до особистих хмарних сховищ або пересилання через неофіційні месенджери.

Важливо, щоб політика не лише описувала ці правила, а й передбачала процедурну відповідальність користувача. Для цього доцільно впровадити обов'язкове підписання декларації або угоди про ознайомлення з політикою, яка має юридичну силу. Такий підхід формує у працівників чітке усвідомлення меж дозволеного і посилює персональну відповідальність за дотримання вимог.

Крім цього, політика повинна враховувати, що рівень цифрової грамотності працівників може істотно варіюватися. У зв'язку з цим рекомендується передбачити систематичне проведення навчань та інструктажів щодо актуальних вимог до безпечного використання мобільних пристроїв. Особливо ефективними є інтерактивні тренінги, що моделюють реальні сценарії інцидентів.

Реагування на інциденти та засоби дистанційного впливу

Оскільки повністю виключити загрозу інцидентів ІБ в мобільному середовищі неможливо, політика повинна передбачати комплекс заходів, спрямованих на оперативне реагування, локалізацію шкоди та відновлення функціональності. Умовно цей етап можна поділити на три компоненти: технічні засоби, організаційні процедури та система інформування.

Технічні засоби реагування базуються на функціоналі централізованих систем керування мобільними пристроями. Через MDM-рішення організація має забезпечити можливість блокування пристрою, віддаленого видалення корпоративних даних (wipe), відновлення даних із резервних копій, а також автоматичну ізоляцію пристрою від корпоративної мережі у разі порушення політики. Наприклад, при виявленні втрати з'єднання з MDM-сервером або використання застарілої ОС система може самостійно призупинити доступ до критичних ресурсів.

Організаційні процедури передбачають створення чіткого алгоритму дій для ІТ-служби та користувача в разі інциденту. Політика повинна вказувати, хто несе відповідальність за ініціацію реагування, як швидко мають бути виконані ключові

дії, якими є критерії завершення інциденту та які заходи передбачено щодо запобігання подібним ситуаціям у майбутньому.

Інформування є важливою, але часто недооціненою складовою. Користувач повинен знати, як і до кого звертатися у разі виявлення ознак компрометації. Для цього політика має включати контакти відповідальних осіб або підрозділів, описати порядок комунікації та обсяг інформації, що має бути надана. У підсумку, цей етап забезпечує організації здатність до швидкої реакції, мінімізації збитків і підтримання стабільної роботи навіть у критичних ситуаціях.

Моніторинг та аудит

Останній етап у формуванні політики управління мобільними пристроями передбачає запровадження безперервного контролю за її виконанням, періодичного перегляду положень та гнучкої адаптації до змін у технологічному, правовому або організаційному середовищі.

При запровадженні моніторингу, політика має чітко вказувати, які саме дані підлягають журналюванню, з якою метою вони збираються, хто має до них доступ і на який строк зберігаються. Відповідальність за моніторинг повинна покладатись на ІТ-відділ або підрозділ ІБ.

Також варто зазначити, що політика повинна передбачати регулярний її перегляд. Рекомендований період ревізії – щонайменше раз на рік, або раніше, якщо були зафіксовані серйозні інциденти ІБ, зміни у законодавстві, поява нових технологій або виявлено структурні недоліки в реалізації. Доцільно передбачити механізм подання пропозицій від співробітників, що підвищить прозорість політики та сприятиме її прийняттю колективом.

3.3 Рекомендації щодо супроводу, моніторингу та вдосконалення політики

Значення супроводу як безперервного процесу безпеки

Ефективне управління мобільними пристроями в організації не завершується на етапі розробки та впровадження політики. Політика є живим документом, який

потребує постійного супроводу, моніторингу відповідності та адаптації до змін зовнішнього і внутрішнього середовища. Супровід охоплює як технічні, так і організаційні дії: оновлення конфігурацій у системах MDM/UEM, аналіз інцидентів, підтримку користувачів, актуалізацію документації, а також комунікацію між IT-відділом і працівниками.

Ефективна підтримка політики передбачає координацію між кількома компонентами ІБ: управлінням доступом, аудитом, інцидентним реагуванням і навчанням персоналу. Необхідно створити відповідальні ролі або групи – наприклад, координатора з мобільної безпеки чи внутрішній комітет з інформаційної політики, – які забезпечуватимуть узгодженість, прозорість і своєчасність рішень щодо політики управління мобільними пристроями.

Моніторинг мобільного середовища: технічний та поведінковий рівні

Моніторинг є основним інструментом постійного контролю ефективності політики. Він повинен охоплювати як технічні параметри пристроїв, так і поведінкові патерни користувачів. Технічний моніторинг включає спостереження за станом ОС, батареї, пам’яті, оновленнями безпеки, активацією/деактивацією функцій (Bluetooth, GPS, камери), спробами обходу політик або встановлення несанкціонованих додатків.

Водночас поведінковий моніторинг дозволяє виявляти аномалії: наприклад, спроби входу з нових локацій, використання корпоративних сервісів у незвичний час, надмірна активність у внутрішніх системах або нетипове використання додатків. Використання аналітики на основі штучного інтелекту дає змогу не лише виявляти аномалії, а й автоматизувати реагування – через блокування, обмеження доступу або зміну рівня довіри пристрою.

Система моніторингу повинна бути інтегрована в централізовану архітектуру безпеки організації. Це дозволяє централізовано збирати події, реагувати на інциденти та узгоджувати мобільну безпеку з іншими шарами захисту.

Аудит і регулярна адаптація політик

Періодичний аудит політик управління мобільними пристроями є критичним елементом забезпечення їхньої актуальності. Він повинен включати як технічну

перевірку відповідності пристроїв до вимог, так і оцінку організаційної ефективності: зручність застосування політик, рівень обізнаності користувачів, відповідність стандартам. Аудит має поєднувати кількісні показники (кількість порушень, інцидентів, оновлень) з якісним аналізом (зворотний зв'язок від працівників, виявлення прогалин у регламентах або змін у законодавстві).

Результати аудиту слугують підставою для оновлення політик. Це може включати включення нових типів пристроїв, перегляд правил BYOD, зміну вимог до автентифікації, уточнення процедур у разі інцидентів тощо. Усі зміни мають фіксуватись у централізованому журналі версій політики із зазначенням дати, ініціатора та обґрунтування.

Освіта, комунікація та культура безпеки

Жодна політика не буде ефективною без розуміння та підтримки з боку користувачів. Тому супровід політики повинен включати не лише технічне адміністрування, але й постійну роботу з персоналом. Доцільно запровадити регулярні тренінги з безпечного використання мобільних пристроїв, оновлення інструкцій у доступній формі, нотифікації про зміни політик, платформи для зворотного зв'язку.

Важливу роль у формуванні культури безпеки відіграють керівники підрозділів: вони повинні демонструвати приклад дотримання політик, сприяти відповідальному використанню ресурсів і заохочувати відкриту комунікацію про проблеми. Працівники повинні мати можливість безпечно повідомляти про інциденти, порушення або складнощі у застосуванні політики – без страху дисциплінарних наслідків.

Гнучкість і масштабованість політик в умовах змін

Мобільне середовище є динамічним: змінюються моделі роботи (перехід на віддалену зайнятість), з'являються нові категорії пристроїв (IoT, носимі пристрої), посилюються вимоги до приватності. У таких умовах критично важливо, щоб політика була не уніфікованою та жорсткою, а гнучкою та масштабованою.

Рекомендується будувати політики за принципом адаптивної сегментації: різні рівні вимог для різних типів пристроїв, ролей користувачів та ступенів ризику.

Наприклад, адміністратор баз даних і менеджер з продажу не повинні підпадати під однакові обмеження. Для підрозділів, що працюють із конфіденційними даними, політика повинна бути жорсткішою, ніж для допоміжних служб.

Застосування принципу мінімально достатніх привілеїв, контейнеризації середовища BYOD, політик умовного доступу (Conditional Access) дозволяє підвищити безпеку без надмірного ускладнення роботи користувачів. Завдяки цьому політика стає гнучкою, релевантною та прийнятною в очах персоналу.

ВИСНОВКИ

У кваліфікаційної роботи було розроблено узагальнені рекомендації щодо управління мобільними пристроями в інформаційній системі організації. Робота має важливе практичне значення для організацій, які використовують мобільні пристрої в своїй повсякденній діяльності, зокрема в умовах гібридної або повністю дистанційної моделі роботи. Проведене дослідження дало змогу узагальнити теоретичні засади та практичні аспекти організації управління мобільними пристроями в корпоративному середовищі, а також сформувати системний підхід до впровадження захищеної моделі використання таких пристроїв.

У рамках дослідження було проаналізовано поняття, функціональні особливості та роль мобільних пристроїв у сучасній інформаційній системі організації. Встановлено, що попри зручність і мобільність, ці пристрої є потенційним джерелом численних загроз – від витоку конфіденційної інформації до проникнення в корпоративну мережу зловмисного програмного забезпечення.

У другому розділі дослідження розглянуто сучасні міжнародні стандарти та нормативні акти, що регламентують підходи до управління мобільними пристроями. Зокрема, вивчено стандарти ISO/IEC 27001, NIST SP 800-124 Rev. 2, рекомендації CIS Controls, які визначають вимоги до впровадження засобів контролю, автентифікації, шифрування, а також управління оновленнями й моніторингом пристроїв. Важливим етапом стало дослідження технологій MDM (Mobile Device Management), EMM (Enterprise Mobility Management) і UEM (Unified Endpoint Management), які є основними платформами для централізованого управління пристроями. На основі порівняльного аналізу таких рішень, як Microsoft Intune та VMware Workspace ONE, було визначено ключові критерії вибору системи для впровадження: функціональні можливості, масштабованість, відповідність вимогам безпеки, інтеграція з іншими системами організації.

У третьому розділі представлено розроблений узагальнений алгоритм впровадження системи управління мобільними пристроями на базі технологій MDM, який охоплює всі етапи життєвого циклу: від аналізу вимог і ризиків до

постійного вдосконалення політик. Запропоновано конкретні рекомендації щодо формування внутрішньої політики управління мобільними пристроями. Крім того, сформульовано практичні поради щодо супроводу та постійного моніторингу ефективності впроваджених засобів управління, що передбачає регулярний аудит, оцінку нових загроз, оновлення політик відповідно до змін в архітектурі ІС та законодавчих вимог.

Підсумовуючи, варто зазначити, що ефективне управління мобільними пристроями в організації є невід'ємною складовою сучасної системи інформаційної безпеки. Воно повинно реалізовуватись на основі інтеграції технічних, організаційних і адміністративних засобів захисту, відповідно до принципів ризик-орієнтованого підходу. Розроблені в межах кваліфікаційної роботи рекомендації можуть бути використані фахівцями з кібербезпеки при розробці або оновленні внутрішніх політик, при підборі та впровадженні засобів управління мобільними пристроями, а також при підготовці персоналу до роботи в умовах підвищеної мобільності та віддаленого доступу.

ПЕРЕЛІК ПОСИЛАНЬ

1. NIST Special Publication 800-124 Revision 2. Guidelines for Managing the Security of Mobile Devices in the Enterprise. URL: https://doi.org/10.6028/NIST.SP.800-124r2 (дата звернення: 31.05.2025р.)
2. TinyMDM. Impact of Mobile Devices on Productivity in the Workplace. URL: https://www.tinymdm.net/impact-of-mobile-devices-on-productivity-in-the-workplace/?utm_source=chatgpt.com (дата звернення: 31.05.2025р.)
3. National Cyber Security Centre (NCSC). Zero Touch Enrolment. URL: https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/zero-touch-enrolment (дата звернення: 31.05.2025р.)
4. American Public University System (APUS). BYOD Security Risks and the Implications for Organizations. URL: https://www.apu.apus.edu/area-of-study/information-technology/resources/byod-security-risks-and-the-implications-for-organizations (дата звернення: 31.05.2025р.)
5. Glisson, W.B., Storer, T. Investigating Information Security Risks of Mobile Device Use within Organizations. URL: https://arxiv.org/abs/1309.0521 (дата звернення: 31.05.2025р.)
6. Black Hat MEA. BYOD: What do organisations really know? URL: https://www.linkedin.com/pulse/byod-what-do-organisations-really-know-blackhatmea-dl5ff/ (дата звернення: 31.05.2025р.)
7. 42Gears. Top 8 Mobile Device Management Trends To Look Out For in 2025. URL: https://www.42gears.com/blog/top-mobile-device-management-trends (дата звернення: 31.05.2025р.)
8. GDPR. Fines & Penalties. URL: https://gdpr-info.eu/issues/fines-penalties/ (дата звернення: 31.05.2025р.)
9. The Times. TikTok Fined Over EU Users' Information Kept in China. URL: https://www.thetimes.co.uk/article/tiktok-fined-over-eu-users-information-kept-in-china-0xpdhxl28 (дата звернення: 31.05.2025р.)

10. Wikipedia. ISO/IEC 27001. URL: https://en.wikipedia.org/wiki/ISO/IEC_27001 (дата звернення: 31.05.2025р.)
11. ISMS.online. ISO/IEC 27002:2022 - Control 8.1 - User Endpoint Devices. URL: https://www.isms.online/iso-27002/control-8-1-user-endpoint-devices/ (дата звернення: 31.05.2025р.)
12. ISMS.online. ISO 27701 - Clause 6.3.2 - Mobile Devices and Teleworking. URL: https://www.isms.online/iso-27701/clause-6-3-2-mobile-devices-and-teleworking/ (дата звернення: 31.05.2025р.)
13. ISO/IEC 27553-1:2022 Information security, cybersecurity and privacy protection - Security and privacy requirements for authentication using biometrics on mobile devices - Part 1: Local modes. URL:https://cdn.standards.iteh.ai/samples/71671/6c675c88a09047eeb549a6092898a2bf/ISO-IEC-27553-1-2022.pdf (дата звернення: 31.05.2025р.)
14. NIST Special Publication 1800-21. Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD). URL:https://cdn.standards.iteh.ai/samples/71671/6c675c88a09047eeb549a6092898a2bf/ISO-IEC-27553-1-2022.pdf (дата звернення: 31.05.2025р.)
15. Center for Internet Security (CIS). CIS Controls v8 Mobile Companion Guide. URL:https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide (дата звернення: 31.05.2025р.)
16. 42Gears. The Ultimate Mobile Device Management Guide. URL: https://www.42gears.com/guide/the-ultimate-mobile-device-management-guide/ (дата звернення: 31.05.2025р.)
17. Ballejos, L.. Enterprise Mobility Management (EMM). URL: https://www.ninjaone.com/blog/enterprise-mobility-management-emm/ (дата звернення: 31.05.2025р.)
18. Krystian,M. MDM vs. EMM vs. UEM: Key differences for device management. URL: https://www.rippling.com/blog/mdm-vs-emm (дата звернення: 31.05.2025р.)

19. Microsoft. Microsoft Intune - Endpoint Management Solution URL: https://www.microsoft.com/en-us/security/business/endpoint-management/microsoft-intune (дата звернення: 31.05.2025р.)
20. Microsoft Learn. Microsoft Intune Documentation. URL: https://learn.microsoft.com/en-us/intune/intune-service/ (дата звернення: 31.05.2025р.)
21. Stanfield IT. Microsoft Intune Features and Capabilities. URL: https://www.stanfieldit.com/microsoft-intune-features/ (дата звернення: 31.05.2025р.)
22. Recast Software. Microsoft Intune Explained. URL: https://www.recastsoftware.com/resources/microsoft-intune-explained/ (дата звернення: 31.05.2025р.)
23. Omnissa. Workspace ONE Unified Endpoint Management. (UEM) URL: https://www.omnissa.com/products/workspace-one-unified-endpoint-management/ (дата звернення: 31.05.2025р.)
24. ePlus. VMware Workspace ONE Datasheet. URL: https://www.eplus.com/docs/default-source/default-document-library/vmware-workspace-one-datasheet.pdf (дата звернення: 31.05.2025р.)
25. VMware EUC Blog. Introduction to Workspace ONE UEM Device Management Modes. URL:https://blogs.vmware.com/euc/2022/10/introduction-to-workspace-one-uem-device-management-modes.html (дата звернення: 31.05.2025р.)
26. Comparitech. VMware Workspace ONE Review. URL: https://www.comparitech.com/net-admin/vmware-workspace-one/ (дата звернення: 31.05.2025р.)
27. National Institute of Standards and Technology (NIST). Zero Trust Architecture. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (дата звернення: 31.05.2025р.)