МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ НА ПІДПРИЄМСТВІ ВІДПОВІДНО ДО КОНЦЕПЦІЇ NIST”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Сергій Силко
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Сергій Силко
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна Мужанова
к.держ.упр., доцент Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Силку Сергію Сергійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи управління безпекою мобільних пристроїв на підприємстві відповідно до концепції NIST”,
керівник кваліфікаційної роботи МУЖАНОВА Тетяна, к.держ.упр., доцент,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджена наказом Державного університету інформаційно-комунікаційних технологійвід “27“ лютого 2024 р. № 36.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *безпека мобільних пристроїв, методи управління безпекою мобільних пристроїв підприємства, концепція управління безпекою мобільних пристроїв NIST.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити теоретичні основи управління безпекою мобільних пристроїв підприємства.
4.2. Встановити засади аналізу та оцінки ризиків корпоративній мобільній безпеці.
4.3. Проаналізувати основні аспекти розробки стратегії управління безпекою мобільних пристроїв відповідно до концепції NIST.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Дослідження теоретичних основ управління безпекою мобільних пристроїв підприємства.	08.04.2024	
4.	Встановлення засад аналізу та оцінки ризиків корпоративній мобільній безпеці.	22.04.2024	
5.	Аналіз основних аспектів розробки стратегії управління безпекою мобільних пристроїв відповідно до концепції NIST.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Сергій СИЛКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

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

Направляється здобувач Силко С.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “Розвідка загроз в управлінні інформаційною безпекою підприємства”

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач СИЛКО Сергій у кваліфікаційній роботі дослідив теоретичні основи управління безпекою мобільних пристроїв підприємства; встановив засади аналізу та оцінки ризиків корпоративній мобільній безпеці; проаналізував основні аспекти розробки стратегії управління безпекою мобільних пристроїв відповідно до концепції NIST.

СИЛКО Сергій показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив самостійність у підготовці роботи. Результати дослідження апробовані на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача СИЛКА Сергія на оцінку “відмінно” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

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

“____“_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Силко С.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти СИЛКА Сергія
на тему “Методи управління безпекою мобільних пристроїв на підприємстві відповідно до концепції NIST”

Актуальність. У сучасному високотехнологічному світі безпека мобільних пристроїв стає все більш важливою у контексті корпоративної інформаційної безпеки, оскільки велика кількість бізнес-операцій виконується через мобільні засоби. Безсумнівною є потреба в розробці ефективних методів управління мобільною безпекою, що відповідає сучасним вимогам і стандартам, зокрема рекомендаціям NIST. Це має особливе значення для розбудови вітчизняної системи кібербезпеки, яка інтегрується в глобальний інформаційно-комунікаційний простір.

З огляду на зазначене дослідження методів управління безпекою мобільних пристроїв на підприємстві відповідно до концепції NIST є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено засади аналізу та оцінки ризиків корпоративній мобільній безпеці, проаналізовано основні аспекти розробки стратегії управління безпекою мобільних пристроїв відповідно до концепції NIST.

2. Кваліфікаційна робота оформлена згідно зі встановленими вимогами. Тест викладено логічно й послідовно, згідно з планом, зроблено змістовні висновки. Основні положення роботи представлено у вигляді рисунків і таблиць.

3. Автор ґрунтовно опрацював публікації NIST з питань управління мобільною безпекою, дослідивши зокрема питання оцінювання ефективності системи управління мобільною безпекою підприємства.

4. За результатами дослідження зроблено висновки про необхідність поєднання технологічних інвестицій в мобільну безпеку з аналітичною й освітньою складовою, розвитком корпоративної культури безпеки й адаптації до нових загроз.

Недоліки.

Доцільно було б приділити більше уваги дослідженню конкретних технологій управління мобільною безпекою з елементами порівняння та рекомендаціями для вітчизняних підприємств.

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

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач СИЛКО Сергій заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:

_____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів управління безпекою мобільних пристроїв на підприємстві відповідно до концепції NIST. Робота складається зі вступу, трьох розділів, що містять 11 рисунків, висновків і списку використаних джерел із 44 найменувань. Загальний обсяг роботи становить 67 аркушів, з яких 5 аркушів займають перелік умовних скорочень і список використаних джерел.

Метою роботи є дослідження методів управління безпекою мобільних пристроїв на підприємстві відповідно до концепції NIST.

Об'єктом дослідження є безпека мобільних пристроїв на підприємстві.

Предмет дослідження – методи управління безпекою мобільних пристроїв на підприємстві відповідно до концепції NIST.

Методи дослідження. Для вирішення вищезгаданого наукового завдання в роботі були використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки та системного підходу до управління інформаційною безпекою.

Як результат у роботі досліджено теоретичні основи управління безпекою мобільних пристроїв підприємства; встановлено засади аналізу та оцінки ризиків корпоративній мобільній безпеці; проаналізовано основні аспекти розробки стратегії управління безпекою мобільних пристроїв відповідно до концепції NIST.

Галузь застосування. Розроблені підходи можуть бути використані при виборі і впровадженні ефективних методів управління безпекою мобільних пристроїв з метою досягнення цілей управління інформаційною безпекою підприємства.

Ключові слова: БЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ, МЕТОДИ УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ ПІДПРИЄМСТВА, КОНЦЕПЦІЯ УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ NIST.

ABSTRACT

The qualification work is dedicated to the study of methods for managing the security of mobile devices in enterprises according to the NIST framework. The work consists of an introduction, three chapters containing 11 figures, conclusions, and a list of 44 references. The total volume of the work is 67 pages, of which 5 pages are taken up by the list of abbreviations and references.

The aim of the work is to study methods for managing the security of mobile devices in enterprises according to the NIST framework.

The object of the research is the security of mobile devices in enterprises.

The subject of the research - is methods for managing the security of mobile devices in enterprises according to the NIST framework.

Research Methods. To solve the aforementioned scientific task, methods of analysis and synthesis, comparison, classification, expert evaluation, and a systematic approach to information security management were used.

As a result, the work investigates the theoretical foundations of managing the security of mobile devices in enterprises; establishes the principles for risk analysis and assessment in corporate mobile security; and analyzes the main aspects of developing a security management strategy for mobile devices according to the NIST framework.

Field of Application. The developed approaches can be used in the selection and implementation of effective methods for managing the security of mobile devices to achieve the information security management goals of the enterprise.

Keywords: METHODS OF ENTERPRISE MOBILE DEVICE SECURITY MANAGEMENT, NIST FRAMEWORK FOR MOBILE DEVICE SECURITY MANAGEMENT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

BYOD	Bring Your Own Device
iOS	Операційна система для мобільних пристроїв від Apple
Java ME	Java Platform, Micro Edition
MAM	Mobile Application Management
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
SIEM	Security Information and Event Management
SSL/TLS	Secure Sockets Layer / Transport Layer Security
SWOT	Strengths, Weaknesses, Opportunities, Threats
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VPN	Virtual Private Network

ВСТУП

Актуальність дослідження. У сучасному світі, де технологічні інновації стрімко впроваджуються у всі сфери нашого життя, питання кібербезпеки набуває особливої актуальності. Зокрема, безпека мобільних пристроїв стає все більш важливою у контексті корпоративної інформаційної безпеки, оскільки велика кількість сучасних бізнес-операцій виконується саме через мобільні засоби.

Актуальність дослідження полягає у необхідності розроблення ефективних методів управління безпекою мобільних пристроїв, що відповідають сучасним вимогам і стандартам, зокрема рекомендаціям Національного інституту стандартів та технологій США. Це має особливе значення для України, яка перебуває на шляху інтеграції в глобальні технологічні та інформаційні простори, зокрема, у контексті розбудови національної системи кібербезпеки.

З огляду на зазначене дослідження методів управління безпекою мобільних пристроїв на підприємстві відповідно до концепції NIST є актуальним науковим завданням.

Мета роботи полягає у дослідженні методів управління безпекою мобільних пристроїв на підприємстві відповідно до концепції NIST.

Об'єкт дослідження – безпека мобільних пристроїв на підприємстві.

Предмет дослідження – методи управління безпекою мобільних пристроїв на підприємстві відповідно до концепції NIST.

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

1. Дослідити теоретичні основи управління безпекою мобільних пристроїв підприємства.

2. Встановити засади аналізу та оцінки ризиків корпоративній мобільній безпеці.

3. Проаналізувати основні аспекти розробки стратегії управління безпекою мобільних пристроїв відповідно до концепції NIST.

Методи дослідження. Для вирішення вищезгаданого наукового завдання в роботі були використані методи аналізу та синтезу, порівняння, класифікації,

експертної оцінки та системного підходу до управління інформаційною безпекою.

Практичне значення отриманих результатів. Використання напрацювань дозволить здійснити обґрунтований вибір методів і інструментів управління безпекою мобільних пристроїв на підприємстві з урахуванням кращих практик NIST.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ

1.1 Поняття мобільного пристрою та його безпеки

У розділі розглянуто сутність мобільних пристроїв та основні аспекти їхньої безпеки, що є ключовим елементом для забезпечення надійності та захищеності інформаційних ресурсів в сучасному цифровому світі.

Мобільний пристрій - це портативний електронний прилад, що дозволяє користувачу виконувати широкий спектр функцій, включаючи зберігання даних, доступ до Інтернету, комунікацію, роботу з додатками тощо. Мобільні пристрої включають смартфони, планшети, переносні медіаплеєри, ноутбуки та інші носії, які можуть бути підключені до мережі або використовувати бездротові технології, такі як Bluetooth та Wi-Fi (Рис. 1.1) [1].

Рис. 1.1. Види мобільних пристроїв

Мобільні пристрої відкривають нові можливості для людей у всьому світі, дозволяють отримувати доступ до даних і пошти, спілкуватись на відстані у реальному часі та зберігати інформацію на віртуальних носіях, але разом з цим викликають появу нових викликів у сфері інформаційної безпеки.

Мобільні пристрої з'явилися в кінці 1970-х років, але перші мобільні телефони мають мало спільного з сучасними мобільними пристроями, крім того, що вони надавали можливості здійснювати телефонні дзвінки. Згодом мобільні пристрої перестали бути просто засобами голосового зв'язку.

У 2005 році Рот виділив п'ять категорій мобільних пристроїв: мобільні стандартні комп'ютери (наприклад, ноутбуки, планшети), вбудовані комп'ютери (наприклад, комп'ютери в автомобілях), кишенькові пристрої (наприклад, особисті цифрові помічники та смартфони), годинники-браслети та чіп-карти (наприклад, смарт-карти). Однак через подальший розвиток мобільних пристроїв важко провести чітку межу між цими категоріями. Тому у 2012 році Керстен і Клетт описали нові категорії мобільних пристроїв таким чином: ноутбуки та нетбуки, планшетні комп'ютери, смартфони та планшети [29, с. 23].

Останнім часом поширення мобільних пристроїв значно зросло. За даними Gartner, у четвертому кварталі 2015 року глобальний обсяг продажів смартфонів для кінцевих користувачів склав 403 мільйони одиниць, що на 9,7% більше, ніж за той ж період 2014 року.

У контексті безпеки мобільних пристроїв, що зазнала величезних змін упродовж останніх років, стає все більш актуальним розуміння сучасних викликів та ризиків. Розглянемо дані на 2023 рік, які вказують на збільшення обсягу мобільного інтернет-трафіку, що очікується досягти понад 500 мільйонів терабайт. Це зростання трафіку підкреслює не тільки підвищене використання мобільних технологій у повсякденному житті, але й велику залежність від них у корпоративних системах. Сьогодні, більше ніж будь-коли, мобільні пристрої є важливими інструментами в руках співробітників, що дозволяють здійснювати швидкий обмін даними, ефективну взаємодію між командами, та доступ до корпоративних ресурсів з будь-якої точки світу. Однак ці переваги також несуть ризики, як-от загрози втрати даних через втручання сторонніх програм або через загублені чи вкрадені пристрої.

Враховуючи ці фактори, корпорації мають приділяти особливу увагу розробці та впровадженню стратегій безпеки, які включають: шифрування

даних, двофакторну аутентифікацію та регулярне оновлення безпеки. Такі заходи не тільки зменшують можливість несанкціонованого доступу до корпоративної інформації, але й забезпечують відновлення даних у випадку їхньої втрати. Набуває значення постійний моніторинг та аналіз патернів використання мобільних пристроїв серед співробітників. Це дозволяє виявляти незвичайну активність, яка може бути індикатором безпекових інцидентів. Такі системи аналітики, вбудовані в корпоративні мережі, можуть надавати цінну інформацію для превентивних заходів і реагування на інциденти.

У сучасному світі, де технології швидко змінюються, мобільна безпека має стати не просто частиною корпоративної культури, а ключовим елементом стратегічного планування в будь-якій організації. Це вимагає не тільки технологічної освіти і тренінгів для співробітників, але й залучення керівництва на всіх рівнях для забезпечення надійності та безпеки мобільних комунікацій.

Використання мобільних пристроїв і технологій хмарних обчислень вимагає підвищеної уваги до безпеки, збереження і захисту даних від несанкціонованого доступу та розповсюдження. У разі втрати мобільного пристрою важливо забезпечити захист або знищення конфіденційних даних. Для захисту трафіку мобільних пристроїв рекомендується використовувати послуги віртуальної приватної мережі VPN, що дозволяє передавати дані закритими каналами.

З метою забезпечення інформаційної безпеки пропонуються рішення для обмеження можливості витоку інформації, захищену взаємодію співробітників компанії, віртуальне робоче місце з централізованим управлінням його безпекою та використання сертифікованих засобів захисту [2, с. 271].

Загальною метою мобільної безпеки є захист даних на мобільних пристроях. Підприємства повинні враховувати мобільну безпеку, щоб зберігати контроль над чутливою інформацією, яка може бути доступна через мобільні пристрої. З поширенням таких пристроїв, безпека стала надзвичайно важливою функцією при використанні мобільних технологій. Оскільки на мобільних пристроях може бути збережена цінна, чутлива і, можливо, класифікована

інформація, вони стикаються з такими ж або навіть вищими рівнями атак і загроз, які впливають на середовище персональних комп'ютерів.

Порівняно з традиційними областями обчислень, такими як ПК, мобільні пристрої мають відмінні принципи безпеки, які відрізняються від принципів традиційної комп'ютерної безпеки:

1) мобільним пристроям характерна висока рухливість, що збільшує шанси на втрату або фізичні втручання в порівнянні з стаціонарними пристроями;

2) мобільні пристрої мають сильну персоналізацію, і ними зазвичай користується унікальний користувач, їх зазвичай не ділять між декількома користувачами на відміну від комп'ютера;

3) вони мають сильне зв'язування з доступом до різних інтернет-сервісів, підключені до великої кількості інтерфейсів (таких як SD-карти, USB, Bluetooth) та використовують різні типи зв'язку (такі як Wi-Fi, UMTS). Внаслідок різноманіття каналів збільшується їхня вразливість до шкідливого програмного забезпечення;

4) сьогодні мобільні пристрої поєднують численні функціональні можливості (такі як геймінг, обмін відео та даними, перегляд інтернету). Ці функції можуть бути використані зловмисниками для експлуатації різних шляхів для виконання їх атак;

5) порівняно зі стаціонарними пристроями мобільні пристрої мають чотири основні притаманні їм обмеження: обмежений термін служби батареї, обмежена обчислювальна потужність, дуже малий розмір дисплея та дуже маленькі клавіші для введення. Ці обмеження створюють виклики для рішень з мобільної безпеки [11, с. 24].

Безпека мобільних пристроїв стає все більш важливою через їх поширене використання в особистих і корпоративних цілях. Безпека мобільного пристрою передбачає захист інформації, збереженої на пристрої, а також переданої через нього. Основні аспекти безпеки мобільних пристроїв охоплюють (Рис. 1.2):

Рис. 1.2. Ключові аспекти безпеки мобільних пристроїв

1) *фізична безпека*. Фізична безпека мобільних пристроїв поєднує заходи, які захищають пристрій від незаконного доступу, крадіжки, пошкоджень чи втрати, зокрема використання захисних чохлів, блокування пристроїв кабельними замками в громадських місцях та забезпечення відстеження місцезнаходження пристрою через GPS для відновлення після втрати або крадіжки. Також важливим є використання технологій віддаленого стирання даних у разі втрати пристрою, що дозволяє забезпечити конфіденційність інформації навіть після втрати фізичного доступу до пристрою;

2) *захист даних*. Захист даних на мобільних пристроях досягається шляхом шифрування даних, що зберігаються на пристрої, та тих, які передаються. Шифрування перетворює чутливу інформацію в форму, яка не може бути прочитана без спеціального ключа. Сучасні операційні системи мобільних пристроїв, такі як iOS та Android, мають вбудовані можливості шифрування, які можуть бути активовані користувачами або адміністраторами. Крім того, безпечні канали зв'язку, такі як VPN і SSL/TLS, використовуються для захисту даних під час їх передачі;

3) *аутентифікація користувачів*. Ефективна аутентифікація користувачів є критичною для забезпечення доступу до мобільного пристрою та даних на ньому лише для уповноважених осіб. Методи аутентифікації передбачають використання традиційних паролів та PIN-кодів, а також біометричних технологій, таких як відбитки пальців, розпізнавання обличчя і сканування

райдужки. Використання біометрії додає додатковий рівень безпеки, оскільки ці дані унікальні для кожної особи;

4) *управління доступом*. Управління доступом визначає, хто має право доступу до яких ресурсів на мобільному пристрої та які дії вони можуть виконувати. Це включає налаштування політик безпеки, які контролюють встановлення додатків, доступ до мережі та використання даних. Управління правами на доступ може бути сконфігуроване через корпоративні інструменти управління мобільними пристроями, які дозволяють централізовано управляти налаштуваннями безпеки;

5) *захист від шкідливих програм*. Захист мобільних пристроїв від шкідливих програм вимагає використання антивірусних засобів і регулярного оновлення всіх системних компонентів. Антивірусні програми можуть виявляти та видаляти віруси, трояни, шпигунські програми та інші види шкідливого ПЗ. Крім того, важливо забезпечити регулярне оновлення програмного забезпечення та операційної системи, щоб усувати відомі вразливості, які можуть бути використані шкідливими програмами для проникнення у систему.

Безпека мобільних пристроїв вимагає *постійного оновлення та адаптації до нових загроз та викликів*. Особливо це актуально в корпоративному середовищі, де використання мобільних пристроїв для доступу до корпоративних даних і ресурсів ставить під загрозу цілісність та конфіденційність важливої бізнес-інформації. Врахування цих аспектів є критично важливим для розробки ефективних методів управління безпекою на рівні підприємства.

Основними цілями управління безпекою мобільних пристроїв є захист даних, запобігання несанкціонованому доступу, забезпечення цілісності та доступності інформації. Для досягнення цих цілей розроблено низку підходів і технологій, які використовуються у всьому світі.

1) блокування пристрою: у разі втрати пристрою важливо заблокувати його паролем або використовувати інші методи захисту, щоб запобігти несанкціонованому доступу до даних;

2) використання криптографічних засобів: шифрування даних на пристрої та на зовнішніх носіях допомагає захистити інформацію від зловмисників;

3) заборона зберігання паролів у браузері: не слід зберігати паролі в браузері мобільного пристрою, щоб уникнути можливого доступу до облікових записів;

4) заборона використання менеджерів паролів: варто уникати використання менеджерів паролів на мобільних пристроях, оскільки вони можуть бути небезпечними;

5) заборона на установку програмного забезпечення з неперевірених джерел: завантаження програм необхідно здійснювати лише з офіційних джерел, щоб уникнути вірусів та шкідливого програмного забезпечення;

6) використання політик захисту та засобів антивірусного захисту: встановлення антивірусного програмного забезпечення та дотримання політик захисту допоможе захистити корпоративні мобільні пристрої;

7) обмеження передачі даних через хмарні сервіси: слід обережно використовувати хмарні сервіси й обмежувати передачу конфіденційних даних через них [2, с. 273].

1.2 Огляд існуючих підходів до управління безпекою мобільних пристроїв

Розглянемо основні підходи до управління безпекою мобільних пристроїв (Рис. 1.3).

Управління мобільними пристроями (Mobile Device Management, MDM) та підхід *«Принеси свій власний пристрій» (BYOD)* - це важливі підходи до управління та захисту мобільних пристроїв у корпоративному середовищі.

MDM дозволяє забезпечити контроль над пристроями, а BYOD дозволяє співробітникам використовувати власні пристрої для роботи, забезпечуючи при цьому безпеку даних. Перед впровадженням таких технологій важливо ретельно

оцінити потреби і загрози, щоб забезпечити ефективний захист даних на мобільних пристроях.

Рис. 1.3. Основні підходи до управління безпекою мобільних пристроїв

MDM є ключовим компонентом корпоративної стратегії безпеки, який дозволяє IT-відділам централізовано керувати всіма аспектами мобільних пристроїв, що входять до корпоративної мережі. Основна мета MDM полягає в забезпеченні безпеки і контролю над мобільними пристроями, які мають доступ до корпоративних ресурсів, в тому числі конфіденційної інформації [3].

MDM рішення надають широкий спектр функцій, серед яких:

1) у випадку втрати або крадіжки мобільного пристрою адміністратор може віддалено видалити всі дані, щоб запобігти їх потраплянню до рук невповноважених осіб. Ця функція є критично важливою для захисту конфіденційності корпоративної інформації;

2) MDM дозволяє віддалено блокувати мобільні пристрої або обмежувати їх функціональність, що забезпечує додатковий рівень контролю над корпоративними пристроями;

3) централізоване управління дозволяє встановлювати й оновлювати налаштування безпеки на всіх мобільних пристроях в одному місці. Це включає налаштування шифрування, конфігурації паролів, політики використання додатків тощо;

4) MDM дозволяє централізовано встановлювати або видаляти додатки на мобільних пристроях, а також управляти оновленнями програмного

забезпечення, забезпечуючи тим самим, що всі пристрої мають останні версії додатків та операційних систем;

5) моніторинг стану пристроїв: системи MDM забезпечують інструменти для моніторингу стану і використання мобільних пристроїв, допомагаючи виявляти потенційні проблеми з безпекою або неналежне використання корпоративних ресурсів [30, с. 45].

Опишемо деякі з найвідоміших MDM-рішень.

Microsoft Intune: інтегрується з іншими продуктами Microsoft, надаючи широкий спектр функцій для управління мобільними пристроями та додатками, а також інтеграцію з Azure Active Directory для управління ідентичністю та доступом.

VMware Workspace ONE - це комплексне рішення, що поєднує можливості MDM та MAM, забезпечуючи управління пристроями на базі різних операційних систем, включаючи iOS, Android, Windows 10, і MacOS.

MobileIron: забезпечує розширені можливості управління безпекою та мобільними додатками, включаючи шифрування, політики безпеки й управління доступом до даних.

Ці системи дозволяють не лише забезпечувати безпеку і контроль, а й підвищувати ефективність корпоративного використання мобільних пристроїв, забезпечуючи водночас гнучкість і масштабованість для великих і зростаючих організацій.

Управління мобільними додатками (Mobile Application Management, MAM) - це стратегія, що дозволяє більш детально контролювати й управляти мобільними додатками на корпоративних пристроях. Ця стратегія важлива для компаній, які прагнуть забезпечити безпеку своїх даних і забезпечити належний контроль над програмним забезпеченням, яке використовують їх співробітники. MAM може бути імплементовано через різні технічні рішення і підходи, включаючи спеціалізоване програмне забезпечення або як частину комплексного рішення MDM.

Основні аспекти MAM:

1) MAM забезпечує безпеку на рівні додатків, включаючи шифрування даних, що зберігаються і передаються додатками. Це запобігає ризикам витоку даних і несанкціонованому доступу до конфіденційної інформації;

2) за допомогою MAM можна детально налаштувати дозволи для кожного додатка, контролюючи доступ до камери, мікрофона, GPS, контактів та інших системних ресурсів. Це дозволяє мінімізувати ризики, пов’язані з доступом додатків до чутливих функцій пристрою;

3) MAM дозволяє IT-відділам віддалено встановлювати, оновлювати та видаляти додатки на мобільних пристроях. Це забезпечує, що всі корпоративні пристрої використовують актуальні версії програмного забезпечення і додатків, що є важливим для безпеки і функціональності;

4) на додаток до контейнеризації даних MAM може застосовувати контейнеризацію на рівні додатків, ізолюючи корпоративні додатки та їхні дані від особистих додатків користувача. Це забезпечує додатковий рівень безпеки та приватності;

5) хоча MAM може використовуватись окремо, його ефективність збільшується при інтеграції з MDM-рішеннями. Це дозволяє організаціям забезпечувати комплексний контроль та управління всіма аспектами мобільних пристроїв: від фізичної безпеки до додатків і налаштувань.

Практичні переваги MAM: можливість тонкого налаштування політик для кожного додатка окремо; отримання персоналом безпечного доступу до корпоративних ресурсів зі своїх мобільних пристроїв, що підвищує їхню мобільність і продуктивність; інтеграція з MDM дозволяє забезпечити всебічний контроль над корпоративними мобільними ресурсами [4].

Таким чином, MAM становить невід'ємну частину стратегії кібербезпеки будь-якої організації, що прагне захистити свої дані та забезпечити безперервну роботу в умовах ризику втрати інформації через мобільні пристрої.

Контейнеризація - це технологія, що забезпечує відокремлення корпоративних даних і додатків від особистої інформації на мобільних пристроях, створюючи зашифровані "контейнери". Це дозволяє ефективно

балансувати між безпекою та зручністю для користувачів, водночас забезпечуючи строгий контроль над корпоративною інформацією.

Основні аспекти й переваги контейнеризації:

1) ізоляція даних: корпоративні додатки та дані функціонують у відокремленому середовищі, що забезпечує їх захист від несанкціонованого доступу через особисті додатки або в разі компрометації особистих даних користувача;

2) шифрування: всі дані, збережені в контейнері, автоматично зашифровані, що знижує ризики пов'язані з втратою або крадіжкою пристрою;

3) управління доступом: адміністратори можуть детально контролювати, як користувачі взаємодіють з корпоративними додатками та даними, без обмеження особистого користування пристроєм;

4) легкість управління: IT-відділ може легко впроваджувати політики безпеки, оновлювати додатки й видаляти корпоративні дані без впливу на особисті файли та додатки користувача;

5) сумісність з BYOD політиками: технологія дозволяє безпечно імплементувати політики "принеси свій власний пристрій", забезпечуючи безпеку корпоративних даних на особистих пристроях співробітників;

6) збереження приватності: контейнеризація дозволяє співробітникам зберігати особисту інформацію на своїх пристроях, не розкриваючи її адміністрації в рамках корпоративної політики безпеки.

Для впровадження контейнеризації використовуються спеціалізовані програмні рішення, які інтегруються з операційною системою мобільного пристрою. Ці програми створюють безпечний, керований контейнер, де можна ізолювати і захистити корпоративні додатки та дані. Вони також надають інструменти для моніторингу й управління цими контейнерами, що дозволяє компаніям ефективно забезпечувати безпеку без порушення приватності персоналу.

Контейнеризація є важливим елементом сучасних стратегій кібербезпеки, особливо в умовах зростання мобільності й поширення політик BYOD у бізнес-

середовищах. Вона не тільки забезпечує захист корпоративних даних, але й дозволяє зберегти гнучкість та зручність використання мобільних пристроїв [31, с. 78].

Шифрування є одним із основних засобів захисту даних на мобільних пристроях. Воно використовується для конвертації чутливої інформації у зашифровану форму, яка не може бути прочитана без відповідного ключа розшифрування. Шифрування може бути застосоване як до даних, що зберігаються на пристрої (шифрування на диску), так і до даних, що передаються (шифрування в каналі).

Опишемо основні аспекти шифрування на мобільних пристроях. Це захищає дані на фізичному носії пристрою. Найпоширеніші технології включають BitLocker для Windows пристроїв, FileVault для macOS [12], та вбудоване шифрування в Android і iOS. Шифрування на диску забезпечує, що дані залишаються недоступними без відповідного пароля або шифрувального ключа, навіть якщо зловмисник отримає фізичний доступ до пристрою.

Дані, що передаються між мобільним пристроєм та іншими системами, також повинні бути захищені. Шифрування в каналі, таке як SSL/TLS для захищених веб-з'єднань, VPN для забезпечення безпечного доступу до корпоративної мережі, і end-to-end шифрування в месенджерах, забезпечує, що передані дані залишаються конфіденційними та захищеними від перехоплення.

Переваги шифрування:

1) захист чутливих даних від несанкціонованого доступу, зокрема в разі втрати або крадіжки пристрою;

2) запобігання порушенню конфіденційності у випадку перехоплення даних під час їх передачі;

3) відповідність нормативним вимогам, як-от GDPR у Європі та іншим регулятивним документам, що встановлюють вимоги щодо захисту персональних даних;

4) підвищення довіри споживачів та бізнес-партнерів, демонструючи серйозне ставлення до захисту даних.

Виклики шифрування включають необхідність забезпечити безпечне зберігання та доступ до шифрувальних ключів без ризику їх втрати або компрометації, шифрування може сповільнити пристрої, особливо старші моделі, оскільки вимагає додаткових обчислювальних ресурсів, а також налаштування і управління шифруванням може бути технічно складним, особливо в розгалужених організаційних структурах.

Ефективне використання шифрування на мобільних пристроях є важливою складовою комплексної стратегії інформаційної безпеки, що допомагає захистити корпоративні дані і водночас забезпечує дотримання вимог щодо конфіденційності даних.

Багаторівнева аутентифікація (Multi-Factor Authentication, MFA) значно підвищує безпеку доступу до корпоративних даних, оскільки вимагає підтвердження ідентичності користувача за допомогою кількох незалежних критеріїв. Це додатково захищає від ризиків, пов'язаних зі зламом або викраденням пароля, а також від інших форм несанкціонованого доступу.

Компоненти багаторівневої аутентифікації:

1) щось, що користувач знає (знання): найпоширеніший фактор - традиційний пароль або PIN-код. Це може також включати відповіді на секретні питання;

2) щось, що користувач має (володіння): цей фактор може включати фізичні або програмні токени, які генерують одноразовий пароль, смарт-карти, або ключі доступу. Мобільні телефони часто використовуються для отримання SMS з кодом або через спеціалізовані додатки для аутентифікації, які генерують коди безпеки;

3) щось, чим користувач є: біометричні дані включають відбитки пальців, розпізнавання обличчя, сканування сітківки або райдужки ока та голосову ідентифікацію. Ці методи є особливо надійними, оскільки вони унікальні для кожної особи.

Переваги багаторівневої аутентифікації охоплюють:

1) підвищення рівня безпеки, оскільки MFA значно ускладнює зловмисникам доступ до систем, навіть якщо один із факторів (наприклад, пароль) був скомпрометований;

2) зменшення ризиків втрати даних, оскільки використання декількох факторів аутентифікації допомагає запобігти несанкціонованому доступу до чутливих даних і систем;

3) відповідність нормативним вимогам, тому що багато галузевих стандартів і законодавчих актів вимагають використання MFA для захисту інформації.

Виклики багаторівневої аутентифікації у цьому випадку: додаткові кроки аутентифікації можуть сприйматися як незручність, особливо якщо процеси не оптимізовані або занадто складні; налаштування й управління MFA може бути складним, особливо в великих організаціях з різноманітними системами і технологіями; залежність від пристроїв або сервісів, таких як мобільні телефони або мережеві підключення, може призводити до відмов у доступі в разі їхнього збою або втрати [32, с. 33].

Ефективне впровадження багаторівневої аутентифікації може значно знизити ризики кіберзагроз і забезпечити більш високий рівень безпеки для корпоративних даних та систем.

Ці методи і технології управління безпекою мобільних пристроїв допомагають організаціям адаптуватися до змінюваного ландшафту кіберзагроз, забезпечуючи необхідний рівень захисту інформації у мобільному та динамічному бізнес-середовищі.

1.3 Концепція NIST для управління безпекою мобільних пристроїв

Національний інститут стандартів та технологій (NIST) США розробив кілька напрямків і стандартів, спрямованих на підвищення безпеки мобільних пристроїв у корпоративних середовищах. Основна мета цих стандартів - надати

організаціям чіткі вказівки щодо захисту мобільних пристроїв від різних загроз, в тому числі несанкціонованого доступу, шкідливих програм і витоку даних.

NIST публікує ряд документів, які надають детальні вказівки та рекомендації для захисту мобільних пристроїв, зокрема:

– NIST Special Publication 800-124 (SP 800-124) - керівництво з управління безпекою мобільних пристроїв [18, с. 51];

– NIST Cybersecurity Framework - надає структурований підхід до управління кіберризиками, включно з мобільними ризиками [19, с . 223].

Ці стандарти призначені для допомоги організаціям у впровадженні ефективних заходів безпеки, адаптованих до широкого спектру загроз, які впливають на мобільні пристрої та дані. Вони охоплюють різні аспекти безпеки, включаючи аутентифікацію, шифрування, управління пристроями та додатками, а також реагування на інциденти.

Основними напрямками захисту мобільних пристроїв за NIST є:

1) політика безпеки: NIST зазначає важливість розробки чіткої політики безпеки, яка спеціально спрямована на мобільні пристрої. Ця політика повинна охоплювати вимоги до конфігурації пристроїв, управління додатками, безпеку даних і шляхи їх шифрування, а також стандарти для зв'язку та обміну даними;

2) аутентифікація та контроль доступу: стандарти рекомендують використання сильної багаторівневої аутентифікації для забезпечення доступу до мобільних пристроїв і даних. Важливо забезпечити, щоб доступ до корпоративних ресурсів був можливий лише для авторизованих користувачів;

3) захист від шкідливих програм і кіберзагроз: NIST підкреслює необхідність використання антивірусних засобів та інших технологій безпеки для захисту мобільних пристроїв від шкідливого ПЗ та інших кіберзагроз. Особливу увагу слід приділити захисту від програм-вимагачів і шпигунських програм;

4) управління інцидентами: Важливим аспектом стандартів NIST є розробка і впровадження процесів реагування на інциденти. Організації мають бути готові виявляти, реагувати та відновлюватися після безпекових інцидентів, пов'язаних з мобільними пристроями.

5) освіта й навчання: NIST наголошує на важливості проведення регулярних тренінгів з безпеки для всіх користувачів мобільних пристроїв. Навчання має включати тематику про поточні кіберзагрози, безпечне використання мобільних пристроїв, а також процедури у випадку виявлення інциденту безпеки [33, с. 112].

Виконання цих стандартів не тільки допомагає організаціям захистити свої мобільні активи від різноманітних загроз, але й підтримує високий рівень довіри з боку клієнтів і партнерів, забезпечує дотримання галузевих і регулятивних вимог.

Варто зазначити, що кібербезпека є критичним аспектом для будь-якої компанії, але особливо актуальною є вона для підприємств малого та середнього бізнесу. Дослідження показують, що цей сектор стикається зі значно більшими загрозами, ризиками та проблемами у боротьбі з кібератаками порівняно з великими корпораціями. За даними, наведеними у [6], 60% підприємств малого і середнього бізнесу (МСП), які стали жертвами кібератак, не відновилися та закрилися протягом 6 місяців. Це може бути пояснене декількома причинами.

По-перше, більшість МСП не мають можливості дозволити собі критично важливі компоненти безпеки і достатньо кваліфікований ІТ-персонал. На відміну від великих корпорацій, які можуть собі дозволити ефективні ІТ-відділи, для МСП це часто недосяжно. Ця нерівність у персоналі та ресурсах ускладнює розробку та впровадження ефективних стратегій кібербезпеки.

По-друге, відсутність можливості забезпечити безперервне навчання з кібербезпеки ставить МСП у вразливе становище. Постійне навчання та поінформованість про загрози є ключовими аспектами боротьби з кібератаками, але для МСП це може бути фінансово недосяжно.

По-третє, програми-вимагачі є серйозною загрозою для МСП. Для великих компаній вони можуть бути керованим ударом, але для МСП вони можуть мати фатальні наслідки [7].

Крім того, ігнорування поганої репутації в Інтернеті й недооцінка ризиків можуть призвести до серйозних проблем для МСП.

Отже, щоб захистити себе від кібератак, МСП повинні вдосконалювати свої стратегії кібербезпеки, звертаючи особливу увагу на політику безпеки, навчання персоналу та вдосконалення реагування на інциденти. Важливо також бути уважними до нових загроз та приділяти належну увагу забезпеченню безпеки інформації та клієнтських даних. Загалом, причини з яких компаніям варто направляти ресурси на кібербезпеку зображено на рисунку 1.4.

Рис. 1.4. Мотивація направляти ресурси на кібербезпеку підприємств [7]

Мета NIST полягає в тому, щоб змінити ситуацію, коли компаніям малого бізнесу складно самостійно створити ефективну систему кібербезпеки. Вони пропонують фундаментальні методи для захисту малих бізнесів [9].

На сайті NIST є низка ресурсів для малого бізнесу у сфері кібербезпеки, такі як куток кібербезпеки для малого бізнесу. Ресурси включають освновні заходи кібербезпеки, посібники з планування, посібники з різних напрямків, навчальні курси, вебінари та відеоролики. Візуалізацію структури контенту з напрямку кібербезпеки для малого бізнесу на ресурсах NIST зображено на рисунку 1.5.

У контексті безпеки мобільних пристроїв, розуміння та впровадження концепцій Національного інституту стандартів та технологій (NIST) є критично важливими для забезпечення захисту корпоративних інформаційних систем. Основою управління безпекою за NIST є ідентифікація та оцінка ризиків, які мають на меті зрозуміти потенційні загрози для інформаційних ресурсів і бізнес-операцій компанії. Цей підхід включає декілька ключових аспектів, які детально описані нижче.

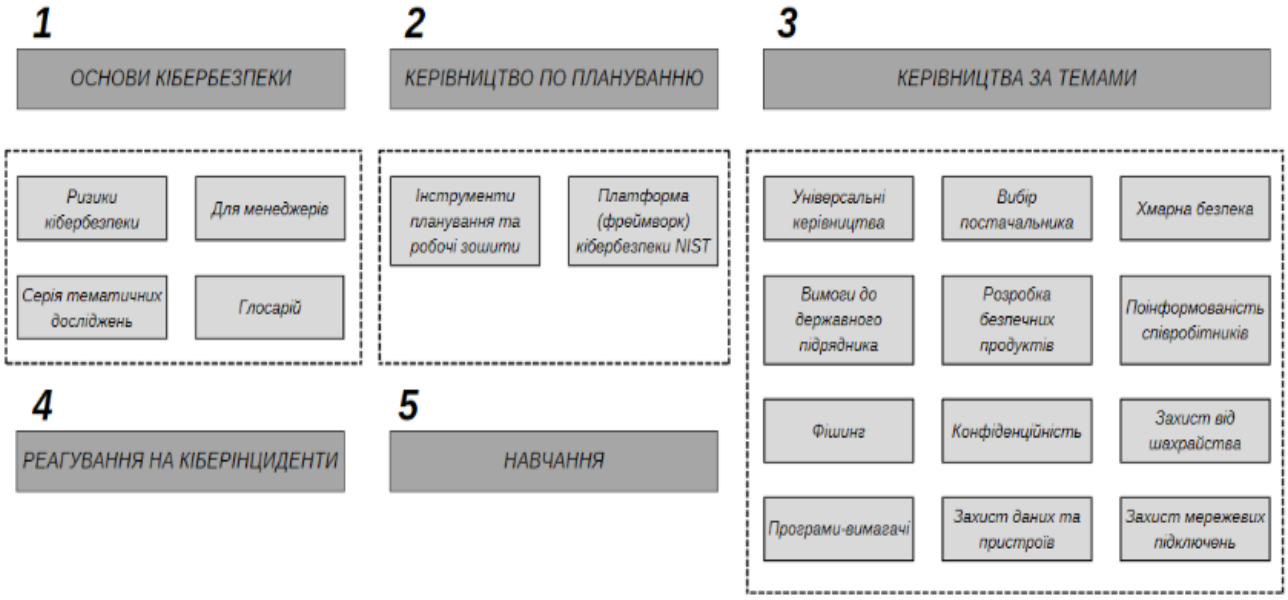

Рис. 1.5. Візуалізація структури контенту з напрямку кібербезпеки для малого бізнесу на ресурсах NIST [7]

У контексті безпеки мобільних пристроїв, розуміння та впровадження концепцій Національного інституту стандартів та технологій (NIST) є критично важливими для забезпечення захисту корпоративних інформаційних систем. Основою управління безпекою за NIST є ідентифікація та оцінка ризиків, які мають на меті зрозуміти потенційні загрози для інформаційних ресурсів і бізнес-операцій компанії. Цей підхід включає декілька ключових аспектів, які детально описані нижче.

Ідентифікація та оцінка ризиків за методологією NIST є важливим компонентом управління безпекою мобільних пристроїв. Цей процес дозволяє організаціям ідентифікувати та оцінити потенційні загрози, які можуть вплинути на їхні інформаційні ресурси та бізнес-операції. Опишемо основні аспекти, які розглядаються в процесі оцінки ризиків.

Аналіз середовища використання допомагає зрозуміти, де і як мобільні пристрої використовуються в рамках організації. Це включає в себе як роботу у внутрішніх мережах організації, так і доступ зі зовнішніх локацій, таких як домашні офіси або публічні місця. Аналіз середовища використання є важливим для визначення специфічних загроз, пов'язаних з різними способами використання технологій.

Визначення видів даних, які обробляються та зберігаються на пристроях, дозволяє зрозуміти рівень чутливості інформації та потенційний вплив її витоку або втрати. Чутливість даних може значно варіюватися від загальної інформації до строго конфіденційних даних, що вимагають особливої уваги до механізмів захисту.

Аналіз способів застосування мобільних пристроїв персоналом включає розгляд того, як співробітники використовують свої пристрої для виконання робочих завдань. Це допомагає виявити можливі "слабкі ланки", де можуть виникнути помилки користувачів або інші вразливості, що можуть бути використані для атак.

Загалом, цей процес вимагає систематичного підходу та постійного перегляду, оскільки нові технології та методи атак постійно розвиваються. Забезпечення безпеки мобільних пристроїв - це неперервний процес, який вимагає регулярного оновлення знань і методів оцінки ризиків.

Застосування політик безпеки за концепцією NIST передбачає розробку та впровадження строгих правил, які регулюють використання мобільних пристроїв та захист корпоративних даних. Ці політики становлять основу захисту інформаційних ресурсів компанії від зовнішніх та внутрішніх загроз. Розробка ефективних політик безпеки вимагає детального аналізу існуючих загроз, потреб компанії та специфіки використання мобільних пристроїв. Основні аспекти, які включаються в політики безпеки:

Аутентифікація становить один із ключових елементів безпеки, вимагаючи від користувачів доводити свою особистість за допомогою надійних методів. Сильна аутентифікація часто включає використання багаторівневих систем, які поєднують декілька форм перевірки особи, зокрема біометричні дані та одноразові паролі.

Шифрування використовується для захисту даних, що зберігаються на пристрої або передаються через незахищені канали. Воно гарантує, що чутливі дані залишаються недоступними для несанкціонованого доступу навіть у випадку втрати чи крадіжки мобільного пристрою.

Управління додатками дозволяє контролювати, які додатки можуть бути встановлені та використовувані на корпоративних мобільних пристроях. Це забезпечує захист від шкідливих або небажаних програм, які можуть становити загрозу безпеці.

Управління переносними носіями інформації. Переносні носії інформації - media зосереджується на тому, як корпоративні дані поширюються через мобільні пристрої, включно з соціальними медіа та іншими платформами. Важливо мати чіткі правила щодо того, як і коли можна ділитися корпоративною інформацією, щоб уникнути витоків даних або репутаційних ризиків.

Ключ до успішного застосування цих політик полягає в тому, щоб вони були не тільки строгими, але й зрозумілими та зручними у використанні для всіх співробітників. Це допомагає забезпечити, що політики будуть ефективно дотримуватися, а системи безпеки - правильно впроваджені. Важливо також забезпечити постійний моніторинг та перегляд цих політик, щоб вони залишалися актуальними в контексті змінних загроз та нових технологій.

Захист мобільних пристроїв від вразливостей і загроз є складним завданням, що вимагає комплексного підходу. Використання технологічних засобів захисту відіграє ключову роль у забезпеченні безпеки цих пристроїв від широкого спектру загроз, включно з шкідливими програмами, кібератаками і несанкціонованим доступом [34, с. 67].

Одним із основних інструментів захисту є *антивірусне програмне забезпечення*, яке сканує мобільні пристрої на наявність вірусів та шкідливих програм, надає захист у реальному часі та допомагає видаляти або блокувати небезпечний контент. Воно важливе не тільки для ідентифікації вже відомих типів шкідливого ПЗ, але й для виявлення нових загроз, що постійно з'являються.

Фаєрволи служать як перша лінія оборони в мережі, контролюючи вхідний і вихідний мережевий трафік. Вони дозволяють блокувати несанкціоновані спроби доступу до пристроїв та даних, а також запобігати спробам кібератак. Важливою їхньою функцією є можливість налаштування правил, які

відповідають політикам безпеки конкретної організації, адаптовані під потреби користувачів та особливості діяльності компанії.

Системи виявлення та запобігання вторгненням активно моніторять мережевий трафік на предмет ознак шкідливої активності, вчасно реагуючи на неї. Вони здатні не тільки ідентифікувати потенційні загрози, але й автоматично вживати заходів для їх нейтралізації, таких як блокування атак або ізоляція інфікованих систем, забезпечуючи тим самим додатковий рівень захисту.

Ці технологічні засоби захисту, коли вони інтегровані та налаштовані правильно, формують міцну оборонну структуру, здатну захистити мобільні пристрої від більшості сучасних загроз. Ефективне впровадження та управління цими системами безпеки вимагають регулярного оновлення й адаптації до нових кіберзагроз, що забезпечує постійний розвиток системи безпеки організації.

Регулярне оновлення й виправлення (патчінг) є однією з ключових рекомендацій NIST для забезпечення безпеки мобільних пристроїв. Цей процес передбачає систематичне встановлення оновлень до операційних систем, додатків та іншого програмного забезпечення, що використовується на пристроях. Оновлення часто містять виправлення помилок, покращення функціоналу та, що найважливіше, патчі для відомих вразливостей.

Актуальність програмного забезпечення є вирішальною, оскільки багато кібератак спрямовані на вразливості, які вже були виявлені та виправлені у новіших версіях ПЗ. Зловмисники постійно шукають застарілі системи, які можна легко скомпрометувати, тому оновлення та патчінг виступають як необхідний бар'єр, що запобігає потенційним атакам.

Однак, процес оновлення й виправлення може бути складним, особливо у великих організаціях з великою кількістю мобільних пристроїв. Вимога до своєчасного та ефективного управління оновленнями вимагає розробки чіткої стратегії. Це включає в себе встановлення процедур для автоматичного розгортання оновлень, що гарантує, що всі пристрої користувачів залишаються захищеними від відомих загроз.

Також важливим аспектом є регулярний моніторинг та аудит інсталювання патчів безпеки. Це забезпечує, що оновлення були встановлені успішно та належним чином. Компанії повинні забезпечити наявність відповідних інструментів та ресурсів для виявлення та усунення будь-яких проблем, що можуть виникнути під час цього процесу.

Застосування цих практик не тільки підвищує рівень безпеки мобільних пристроїв, але й сприяє підтримці довіри та впевненості серед користувачів та клієнтів, оскільки вони можуть бути впевнені, що організація відповідально ставиться до захисту своїх даних і систем.

Навчання та освіта користувачів є життєво важливими аспектами у забезпеченні кібербезпеки, особливо коли мова йде про мобільні пристрої, які часто використовуються в нестабільних або неконтрольованих середовищах. Організації повинні проводити регулярні тренінги та освітні програми, спрямовані на підвищення обізнаності користувачів з питань безпеки. Це допомагає знизити ризики, пов'язані з людським фактором, який часто є найслабшою ланкою в ланцюгу безпеки.

Ефективні програми навчання зосереджуються на забезпеченні користувачів знаннями про те, як визначити та запобігти потенційним загрозам. Це включає інформацію про фішинг, шкідливе програмне забезпечення, втрату даних та інші форми кібератак. Освітні сесії мають охоплювати теми, такі як безпечне використання електронної пошти, безпека в соціальних мережах, важливість регулярного оновлення ПЗ і використання складних паролів [35, с. 67].

Тренінги повинні також включати практичні компоненти, де користувачі можуть відпрацювати навички на практиці, такі як управління паролями та використання двофакторної аутентифікації. Подібні вправи допомагають закріпити теоретичні знання та краще запам'ятати отриману інформацію.

Крім того, освітні програми мають регулярно оновлюватися, щоб відображати нові кіберзагрози та найкращі практики безпеки. Важливо створити

культуру безпеки, де кожен працівник розуміє свою роль у захисті інформації компанії.

Забезпечення регулярних тренінгів та освітніх програм для всіх працівників є фундаментальним кроком у зниженні ризиків, пов'язаних із використанням мобільних пристроїв.

Висновки до розділу 1

У розділі розглянуто ключові аспекти безпеки мобільних пристроїв, а також різні підходи й технології, які можуть бути застосовані для ефективного управління мобільною безпекою в організаціях.

Встановлено, що безпека мобільних пристроїв охоплює здійснення сукупності заходів щодо фізичного захисту пристроїв, захисту даних, які на них зберігаються та передаються, аутентифікації користувачів, управління доступом і захисту від шкідливого програмного забезпечення.

Огляд існуючих підходів до управління безпекою мобільних пристроїв показав, що сучасні стратегії мобільної безпеки передбачають комплексне використання методів і технологій, таких як MDM, MAM, контейнеризація, шифрування і багаторівнева аутентифікація, що дозволяють забезпечувати високий рівень безпеки.

Концепція NIST представляє структурований підхід до управління безпекою мобільних пристроїв, який охоплює оцінку ризиків, розробку і впровадження політик безпеки, які охоплюють всі аспекти використання мобільних пристроїв, і реалізації технологічних заходів. Крім цього, у стандартах NIST підкреслено необхідність регулярного оновлення та виправлень операційних систем, додатків та іншого ПЗ, застосування засобів безпеки (фаєрволи, IDS/IPS, багаторівневої аутентифікації), а також організацію освітніх програм для користувачів, які сприяють підвищенню їхньої обізнаності та відповідальності щодо безпеки.

Підсумовуючи, слід зазначити, що успішне управління мобільною безпекою вимагає не тільки технологічних інвестицій, але й постійної уваги до освітньої складової, розвитку корпоративної культури безпеки й адаптації до нових загроз, що постійно змінюються у глобальному цифровому ландшафті.

Розділ 2 АНАЛІЗ ТА ОЦІНКА РИЗИКІВ КОРПОРАТИВНІЙ МОБІЛЬНІЙ БЕЗПЕЦІ

2.1 Методологія оцінки ризиків за концепцією NIST

Методологія оцінки ризиків за концепцією NIST визначає систематичний підхід до ідентифікації, аналізу й оцінки ризиків безпеки інформації та мобільних пристроїв у корпоративному середовищі. Оцінка ризиків є критично важливим елементом управління інформаційною безпекою, оскільки допомагає організаціям зрозуміти потенційні загрози для їхніх активів та визначити відповідні заходи захисту.

Етапи оцінки ризиків мобільній безпеці відповідно до бачення NIST показані на рис. 2.1 [18].

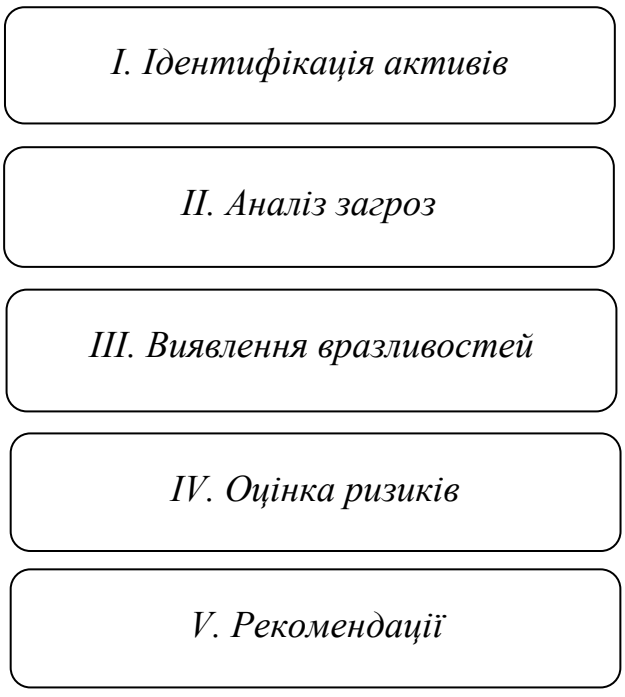

Рис. 2.1. Етапи оцінки ризиків мобільній безпеці NIST

Перший крок цієї методології полягає у *визначенні мобільних пристроїв та інших активів*, які містять або обробляють корпоративну інформацію. Ці активи можуть варіюватися від смартфонів, планшетів до портативних носіїв інформації та навіть до обладнання IoT (Інтернет речей), яке стає дедалі популярнішим у корпоративних мережах. Детальне розуміння, де і як ці активи

використовуються, важливе для визначення потенційних вразливостей, які можуть бути використані зловмисниками. Важливо враховувати не лише фізичне розташування активів, але й спосіб їх використання співробітниками, включно з доступом до корпоративних ресурсів ззовні офісу.

Другий крок полягає в *аналізі можливих загроз*. Ці загрози можуть бути різноманітними, включаючи внутрішні та зовнішні загрози, такі як витік даних через крадіжку або втрату пристрою, атаки шкідливих програм, фішинг або навіть внутрішнє шахрайство. Аналіз загроз вимагає розуміння потенційних мотивів і можливостей зловмисників, а також оцінки того, як ці загрози можуть вплинути на вразливі аспекти мобільної інфраструктури організації.

Третій крок, *визначення вразливостей*, включає аналіз слабких місць у захисті мобільних пристроїв та процедур, що є частиною загальної інформаційної безпеки. Вразливості можуть бути технічними, наприклад, недоліки у програмному забезпеченні, застаріле обладнання, а також організаційними, як-от недостатнє навчання персоналу або неповне дотримання політик безпеки. Розуміння цих вразливостей є важливим для визначення стійкості системи до потенційних атак.

Четвертий крок, *оцінка ризиків*, передбачає аналіз ймовірності виникнення загроз та їх потенційного впливу на організацію. Це включає розрахунок потенційних втрат від різних видів інцидентів та визначення пріоритетів для заходів щодо зменшення ризиків. Важливим аспектом є також оцінка існуючих захисних заходів і визначення їхньої ефективності у запобіганні чи мінімізації впливу інцидентів.

Ще один крок, *формулювання рекомендацій* щодо вжиття заходів безпеки, може включати впровадження нових технологій, зміну процедур, політик, проведення тренінгів для персоналу, і навіть перегляд інфраструктурних рішень. Особливу увагу слід звернути на впровадження заходів, які мінімізують ризики без зайвого обмеження бізнес-процесів.

Задля посилення розуміння ефективності заходів інформаційної безпеки важливо звернути увагу на необхідність адаптації існуючих захисних стратегій

до постійно змінюваних умов зовнішнього середовища. Технологічний прогрес і розвиток нових форм мобільних комунікацій та обчислень змушують організації постійно переглядати та оновлювати свої політики безпеки. В цьому контексті особливу роль відіграє розробка комплексного плану інцидентного реагування, який дозволить швидко і ефективно реагувати на можливі загрози.

Однією з критичних областей є розробка та впровадження систем електронного спостереження та моніторингу, які можуть забезпечувати неперервний контроль за станом інформаційної безпеки мобільних пристроїв. Ці системи допомагають виявляти не тільки зовнішні, але й внутрішні загрози, зокрема, несанкціонований доступ або неавторизоване використання даних. Застосування таких технологій як штучний інтелект і машинне навчання може значно підвищити ефективність систем безпеки шляхом автоматизації процесів аналізу даних та виявлення аномалій. Також не менш важливим є впровадження строгих процедур для обробки та зберігання даних, особливо в умовах, коли організації все частіше вдаються до використання хмарних технологій для зберігання великих обсягів даних. Належне шифрування даних, як у стані спокою, так і під час їх передачі, є обов’язковим для забезпечення конфіденційності та цілісності корпоративної інформації.

Окрім технічних аспектів, велике значення має і корпоративна культура, зокрема підвищення обізнаності серед співробітників щодо принципів інформаційної безпеки та регулярне проведення тренінгів з безпеки. Залучення кожного співробітника в процес забезпечення безпеки є ключовим фактором у побудові ефективної системи захисту. Застосування методології оцінки ризиків за концепцією NIST дозволяє не тільки ідентифікувати й оцінювати потенційні загрози, але й формувати гнучкі, адаптивні стратегії управління ризиками, що є невід’ємною частиною сучасного підходу до інформаційної безпеки в корпоративному середовищі.

Застосування методології оцінки ризиків за концепцією NIST дозволяє організаціям не тільки виявити й ефективно реагувати на потенційні загрози, але й системно підходити до управління безпекою складних мобільних середовищ.

2.2 Ідентифікація та класифікація ризиків для мобільних пристроїв

Ідентифікація та класифікація ризиків є критичними компонентами управління безпекою мобільних пристроїв. Цей процес дозволяє організаціям визначити потенційні загрози та ризики, які можуть вплинути на їх мобільні активи, і відповідно пріоритезувати заходи безпеки. Основні аспекти ідентифікації та класифікації ризиків охоплюють (Рис. 2.2):

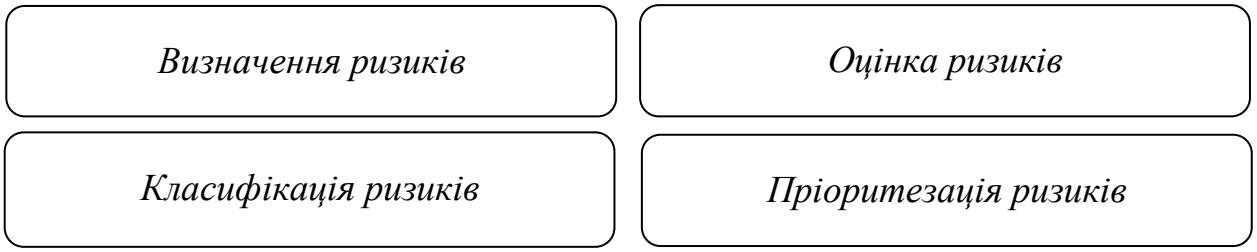

Рис. 2.2. Основні аспекти ідентифікації та класифікації ризиків

Визначення ризиків: перший крок полягає у визначенні всіх можливих ризиків, які можуть вплинути на мобільні пристрої в організації. Це можуть бути технічні ризики, такі як вразливості у програмному забезпеченні й обладнанні, а також ризики, пов'язані з людським фактором, такі як помилки користувачів або зловмисні дії.

Класифікація ризиків: ризики класифікуються за їх потенційним впливом та ймовірністю виникнення. Класифікація допомагає визначити, які ризики потребують негайної уваги та ресурсів для їх мінімізації. Зазвичай, ризики можуть бути категоризовані як високі, середні або низькі залежно від очікуваних наслідків і ймовірності їх виникнення.

Оцінка ризиків: кожен ризик оцінюється за його ймовірністю і потенційним впливом на бізнес. Це оцінювання допомагає організації вирішити, які ризики потребують більше уваги та які заходи безпеки потрібно реалізувати для їх зменшення. Наприклад, ризик втрати даних через втрату пристрою може мати високий вплив на компанію, якщо на пристрої зберігаються чутливі або конфіденційні дані.

Пріоритезація ризиків: після оцінки всіх ризиків, організація розробляє стратегію пріоритезації, яка визначає, які ризики потрібно вирішувати

першочергово. Ризики з високою ймовірністю виникнення та великим потенційним впливом будуть мати найвищий пріоритет для мінімізації [36, с. 44].

Цей процес ідентифікації та класифікації ризиків є основою для розробки комплексної стратегії безпеки, яка включає технічні заходи, політики та процедури, навчання користувачів і реагування на інциденти. Чітке розуміння ризиків дозволяє організаціям ефективно захищати свої мобільні активи і забезпечувати безпеку корпоративної інформації.

Для візуалізації класифікації ризиків за методологією NIST можна створити таблицю, яка розділяє ризики на категорії за їх потенційним впливом і ймовірністю виникнення (табл. 2.1).

Таблиця 2.1

Класифікація ризиків

Категорія ризику	Опис	Ймовірність	Вплив
Високий	Ризики, що можуть призвести до значних фінансових втрат, втрати репутації, або юридичних наслідків.	Висока	Критичний
Середній	Ризики, які можуть спричинити помірні збитки або перешкоджати операційній діяльності.	Середня	Модерний
Низький	Ризики, що мають незначний вплив на діяльність компанії і можуть бути легко вирішені.	Низький	Низький

Ця таблиця допомагає відобразити рівень ризику для різних потенційних загроз, даючи змогу керівництву організації чітко оцінити, які заходи безпеки повинні бути вжиті як найбільш пріоритетні. Вона також служить важливим

інструментом для регулярного перегляду політики та процедур безпеки, що забезпечує їх актуальність і ефективність у захисті мобільних активів організації.

2.3 Аналіз потенційних загроз і вразливостей мобільним пристроям

Аналіз потенційних загроз і вразливостей мобільним пристроям є важливим аспектом управління безпекою. З розвитком технологій і збільшенням залежності від мобільних пристроїв у професійному та особистому використанні, стає критично важливим розуміти та мінімізувати пов'язані з ними ризики.

Загрози для мобільних пристроїв можуть включати, але не обмежуються такими:

1) шкідливе програмне забезпечення;

2) фішинг;

3) втрата або крадіжка пристроїв;

4) несанкціонований доступ;

5) додатки з уразливостями безпеки.

Опишемо ширше кожну з них.

Шкідливе програмне забезпечення охоплює різноманітні типи програм, такі як віруси, трояни та шпигунські програми. Це ПЗ може бути завантажене на мобільний пристрій через інфіковані додатки, приховані у замаскованих під легітимні програмах, або через веб-сайти, що містять шкідливі скрипти. Також, користувачі можуть стати жертвами фішингових атак, які спонукають їх завантажити зловмисне ПЗ через соціоінженерні маніпуляції. Ці програми можуть красти особисті дані, перехоплювати повідомлення, здійснювати несанкціоновані дзвінки або навіть перетворювати пристрій на елемент ботнету.

Фішинг - це вид соціальної інженерії, що має на меті отримати конфіденційні дані користувачів, такі як логіни, паролі та інформацію про банківські рахунки. Зловмисники використовують переконливі електронні листи, SMS або повідомлення в месенджерах, які мімікрують під повідомлення

від надійних організацій, щоб обдурити користувачів і спонукати їх розкрити свої особисті дані.

Мобільні пристрої часто містять значну кількість особистої і корпоративної інформації і є високо вразливими до *втрати або крадіжки*. Сьогодні, коли багато організацій мають кілька місць розташування чи приміщень, а також дозволяють віддалену роботу, мобільні пристрої постійно переносяться з місця на місце. Внаслідок цього збільшується ймовірність їх втрати або викрадення, а наявність на них конфіденційних даних підвищує ризик компрометації для організації [38, с. 56]. Втрата доступу до пристрою може призвести до несанкціонованого доступу до конфіденційної інформації, порушення приватності й потенційних фінансових збитків. Застосування функцій шифрування та віддаленого видалення даних може допомогти зменшити ці ризики.

Слабкі паролі та відсутність двофакторної аутентифікації можуть створити зловмисникам можливості *несанкціонованого доступу* до мобільних пристроїв. Одного вдалого вгадування пароля може бути достатньо, щоб зламати пристрій і отримати доступ до всієї інформації, що на ньому зберігається. Використання складних паролів і впровадження багатофакторної аутентифікації є критично важливими заходами для захисту пристроїв.

Незахищені додатки, які належним чином не проходять перевірки безпеки або містять вразливості, можуть стати причиною серйозних безпекових проблем. Ці додатки можуть використовуватися зловмисниками для отримання несанкціонованого доступу до мобільних пристроїв, здійснення крадіжки даних або навіть атак на інші системи в межах корпоративної мережі.

Для захисту від цих загроз, організації мають вживати комплексних заходів, включаючи регулярні оновлення програмного забезпечення, аудити безпеки, розробку та дотримання строгих політик безпеки, а також проведення тренінгів для користувачів.

Вразливості мобільних пристроїв часто пов'язані з системою управління пристроєм або її компонентами. Наприклад, операційні системи, що не оновлюються регулярно, можуть містити відомі вразливості, які не виправлені.

Безпека додатків також є значним питанням, оскільки розробники можуть не врахувати всі потенційні загрози, особливо в областях захисту даних.

Для розробки ефективних заходів безпеки, організації повинні використовувати стратегії, засновані на ретельній оцінці загроз і вразливостей, зокрема:

1) регулярні аудити безпеки для виявлення нових загроз і оцінки ефективності існуючих заходів безпеки;

2) систематичне оновлення та патчінг для забезпечення захисту проти відомих вразливостей;

3) навчання персоналу для підвищення обізнаності про загрози та правильного використання мобільних пристроїв.

З урахуванням цих аспектів, організації можуть значно знизити ризики, пов'язані з використанням мобільних пристроїв, і забезпечити більш безпечне та контрольоване середовище.

Результати дослідження [13] вказують на те, що мобільні пристрої стають все більш поширеними у всіх сферах життя, завдяки своїй зручності та унікальним можливостям. Однак збільшення кількості користувачів також призводить до зростання загроз безпеці. У роботі розглянуто загрози для мобільних операційних систем та їхній вплив на мобільні пристрої, досліджено чотири найпопулярніші мобільні операційні системи (Android, Apple OS (iOS), Symbian та Java ME) і надано статистичну інформацію про їх особливості й області застосування.

Основні загрози для мобільних операційних систем включають шкідливе програмне забезпечення, вразливості та атаки. Ці загрози можуть призвести до втрати конфіденційності даних, порушення доступності пристрою та порушення цілісності інформації.

Досліджено основні мобільні операційні системи, такі як Android і iOS. Кожна з цих систем має свої особливості та принципи функціонування, які можуть бути використані зловмисниками для здійснення атак. Для забезпечення безпеки мобільних пристроїв у майбутньому, рекомендується вдосконалення

методів виявлення та захисту від загроз, розвиток стандартів безпеки та посилення контролю над доступом до даних.

Таким чином, підкреслено необхідність вдосконалення систем безпеки мобільних пристроїв та операційних систем для захисту від потенційних загроз.

Дослідження також виявило, що існує широкий спектр загроз для смарт-пристроїв, що використовують мобільні операційні системи. Розвиток пристроїв, які мають інтернет-з'єднання, сприяє зростанню шкідливого програмного забезпечення як в технологічному, так і в структурному плані. Ці загрози можна розглядати у трьох основних категоріях: шкідливе програмне забезпечення, вразливості та атаки.

Шкідливе ПЗ націлене на конфіденційні дані користувачів, може призвести до збоїв в роботі пристрою та втрати або відмови в доступі до інформації та документів користувача. Трояни, черви, віруси та шпигунське програмне забезпечення є основними видами шкідливого ПЗ. Наприклад, вірус Cabir, створений для операційної системи Symbian у 2004 році, заразив Nokia 60 series і багато смартфонів. Цей хробак пише слово "Cabire" на екрані зараженого телефону та використовує підключення Bluetooth для поширення. Android є більш схильним до атак зловмисного ПЗ через відкриту природу своєї системи.

Вразливості системи безпеки включають недіолки в процедурах безпеки системи, внутрішні контрольні механізми, дизайн та програми. Наприклад, старі пристрої можуть бути вразливі через відсутність підтримки виробників, а також недостатнє захищені порти підключення до мережі чи Інтернету. Вразливості програмного забезпечення також є проблемою, особливо коли використовується застаріла версія операційної системи. Наприклад, деякі атаки можуть бути спрямовані на встановлення старих версій програм.

Атаки представляють собою втручання ззовні, які використовують різноманітні вразливості. Наприклад, атаки можуть бути спрямовані на використання зловмисного ПЗ або вразливостей у пристроях чи операційних системах. Однак, термін "атака" зазвичай використовується для опису вторгнень, які мають на меті отримання конфіденційних даних користувача без його відома.

У майбутньому безпека стане найважливішим фактором у комунікації. З цього приводу очікується, що операційні системи, які пропонують закритий код, такі як iOS, знайдуть собі значне місце. Хоча користувачі цих систем обмежені у виборі додатків, вони мають більшу безпеку порівняно з Android. Windows Phone, інша закрита система, також очікується, що вона покаже успіх у майбутньому, як і в особистих комп'ютерах з Windows. Таким чином, безпека мобільних пристроїв є критично важливою, і вона буде продовжувати зростати важливістю у майбутньому [13].

2.4 Оцінка ризиків та розробка стратегії управління ризиками

Оцінка ризиків і розробка стратегії їх управління є ключовими процесами в управлінні безпекою мобільних пристроїв. Ці процеси допомагають організаціям не тільки ідентифікувати і зрозуміти потенційні ризики, але й розробити ефективні стратегії для їх зниження або уникнення. Розглянемо основні кроки в оцінці ризиків та розробці стратегії управління ними.

Оцінка ризиків - це процес ідентифікації, аналізу й оцінювання потенційних ризиків, які можуть негативно вплинути на активи, проекти або цілі організації. Цей процес є важливим для управління безпекою, оскільки допомагає організаціям зрозуміти ймовірність виникнення певних подій і потенційні наслідки, що можуть виникнути в результаті цих подій. Оцінка ризиків використовується для підготовки і розробки стратегій, які мінімізують або управляють цими ризиками на прийнятному рівні.

Оцінка ризиків зазвичай включає наступні кроки (Рис. 2.3):

1) *визначення потенційних загроз або подій*, які можуть спричинити шкоду організації, її активам, персоналу або клієнтам. До цієї категорії відносять фінансові ризики, технологічні ризики, природні катастрофи, кіберзагрози тощо;

2) *вивчення і аналіз ідентифікованих ризиків* для з'ясування їх природи і того, як вони можуть вплинути на організацію. Ця діяльність охоплює оцінку ймовірності виникнення кожного ризику та його потенційного впливу;

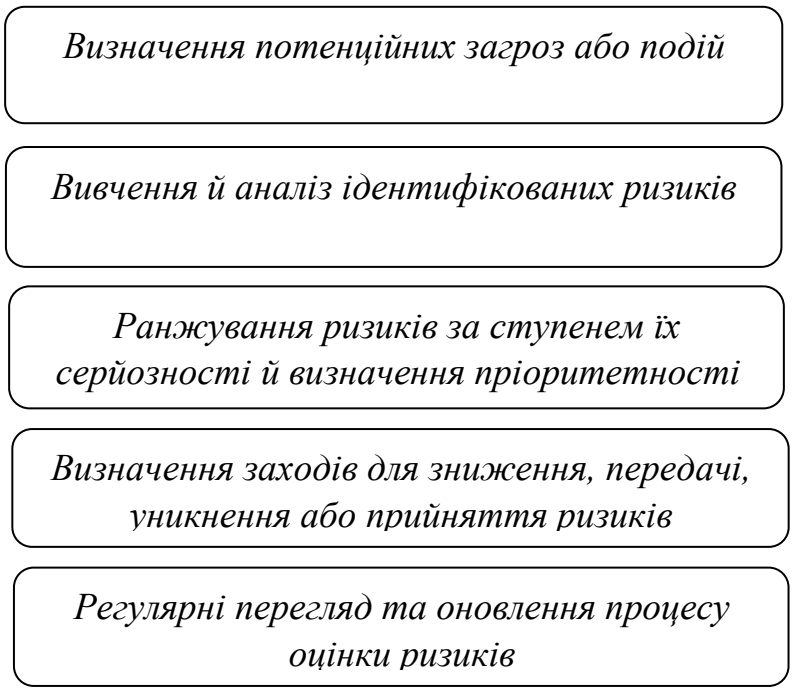

Рис. 2.3. Етапи оцінки ризиків мобільній безпеці

3) *ранжування ризиків за ступенем їх серйозності й визначення пріоритетності для реагування*. Це важливо для того, щоб зосередити ресурси та зусилля на найбільш значущих ризиках;

4) *визначення заходів для зниження, передачі, уникнення або прийняття ризиків* на основі їх оцінки. Цей етап може включати застосування технологічних рішень, зміни в процесах управління, страхування, планування на випадок надзвичайних ситуацій тощо;

5) *регулярні перегляд та оновлення процесу оцінки ризиків* для врахування нових загроз або змін у діловому середовищі. Цей етап забезпечує актуальність та ефективність управління ризиками в організації [39, с. 22].

Оцінка ризиків є фундаментальним елементом у стратегічному плануванні та управлінні будь-якої організації, дозволяючи їй адекватно підготуватися та відповісти на потенційні виклики та загрози.

Розробка стратегії управління ризиками є важливим аспектом у забезпеченні стійкості організації. Цей процес дозволяє системно ідентифікувати, оцінювати, відстежувати й мінімізувати ризики, які можуть негативно вплинути на активи, доходи, репутацію, персонал, клієнтів чи здатність організації досягати своїх цілей.

Основна мета розробки корпоративної стратегії управління ризиками полягає в тому, щоб допомогти компанії адекватно реагувати на загрози, а також забезпечувати її довгострокову стабільність і успіх. Основні етапи розробки стратегії управління ризиками описано в таблиці 2.2 [40, с. 49].

Таблиця 2.2

Етапи розробки стратегії управління ризиками

Етап	Кроки
Визначення контексту	Зовнішній контекст: оцінка зовнішнього середовища, включаючи регуляторні вимоги, ринкові умови, політичні, соціальні та технологічні фактори.
	Внутрішній контекст: аналіз внутрішньої структури, процесів, корпоративної культури та ресурсів.
Ідентифікація ризиків	Визначення потенційних загроз та їх джерел, які можуть завдати шкоди організації.
	Застосування технік як-от мозковий штурм, інтерв'ю з експертами, SWOT-аналіз тощо.
Оцінка ризиків	Оцінка ймовірності та впливу кожного ризику на організацію.
	Класифікація ризиків за пріоритетністю для визначення, які з них потребують негайних дій.
Розробка заходів щодо управління ризиками	Визначення варіантів реагування на ризики, таких як уникнення, зменшення, передача (наприклад, через страхування) або прийняття ризиків.
Впровадження стратегії	Реалізація обраних заходів управління ризиками.
	Включення процесів управління ризиками у загальні бізнес-процеси та процедури.

Продовження таблиці 2.2

Моніторинг та перегляд	Регулярний моніторинг впроваджених стратегій і заходів управління ризиками.
	Перегляд та оновлення стратегії управління ризиками відповідно до нових викликів, змін у бізнесі та зовнішньому середовищі.
Звітність та комунікація	Забезпечення відкритості та прозорості в процесі управління ризиками.
	Комунікація результатів і статусу управління ризиками до стейкхолдерів та вищого керівництва.

Розробка та впровадження ефективної стратегії управління ризиками дозволяє організації не тільки мінімізувати потенційні збитки від несподіваних подій, але й підвищити загальну стійкість та конкурентоспроможність.

Загалом, оцінка ризиків і розробка стратегії управління ними дозволяють організації бути підготовленою до можливих інцидентів безпеки і забезпечити цілісність, конфіденційність та доступність своїх мобільних ресурсів. За допомогою цих процесів можна не тільки мінімізувати потенційні збитки від інцидентів, але й підвищити загальну кіберстійкість організації.

Висновки до розділу 2

Встановлено, що оцінка ризиків є критично важливим елементом управління мобільною безпекою, оскільки допомагає організаціям зрозуміти потенційні загрози для їхніх активів та визначити відповідні заходи захисту. Процес оцінки ризиків є послідовністю таких етапів: визначення мобільних пристроїв та інших активів; визначення загроз і вразливостей мобільної безпеки; аналіз ризиків; розробка рекомендацій щодо вжиття заходів безпеки.

Дослідження показало важливість ідентифікації та класифікації ризиків для мобільних пристроїв за ступенем їх впливу на діяльність підприємства, аналізу потенційних загроз і вразливостей мобільній безпеці як чинника

розробки ефективної стратегії безпеки організації, визначення і впровадження заходів для зниження, передачі, уникнення або прийняття ризиків на основі їх оцінки, оновлення процесу оцінювання ризиків мобільним пристроям з урахуванням нових загроз або змін у бізнес-середовищі.

Розробка стратегії управління ризиками дозволяє системно ідентифікувати, оцінювати, відстежувати й мінімізувати ризики, які можуть негативно вплинути на активи, доходи, репутацію, персонал, клієнтів і здатність організації досягати своїх цілей. Основними етапами розробки стратегії управління ризиками є: визначення внутрішнього і зовнішнього контексту організації; ідентифікація й оцінка ризиків; розробка і впровадження заходів із управління ризиками; моніторинг і перегляд заходів; звітування й інформування зацікавлених сторін.

Розробка та впровадження ефективної стратегії управління ризиками мобільної безпеки дозволяє організації не тільки мінімізувати потенційні збитки від несподіваних подій, але й підвищити загальну конкурентоспроможність і стійкість до чинників негативного впливу на захищеність організації та її активів.

Розділ 3 РОЗРОБКА СТРАТЕГІЇ УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ ВІДПОВІДНО ДО КОНЦЕПЦІЇ NIST

3.1 Визначення політики безпеки мобільних пристроїв

Політика безпеки мобільних пристроїв визначає набір правил, процедур і технологічних заходів, які організація встановлює для захисту даних і мобільних пристроїв, які використовуються персоналом у корпоративних цілях. Ця політика визначає вимоги щодо безпеки, включаючи контроль доступу, шифрування даних, управління додатками, моніторинг і захист від загроз безпеки.

Основними елементами політики безпеки мобільних пристроїв є (Рис. 3.1):

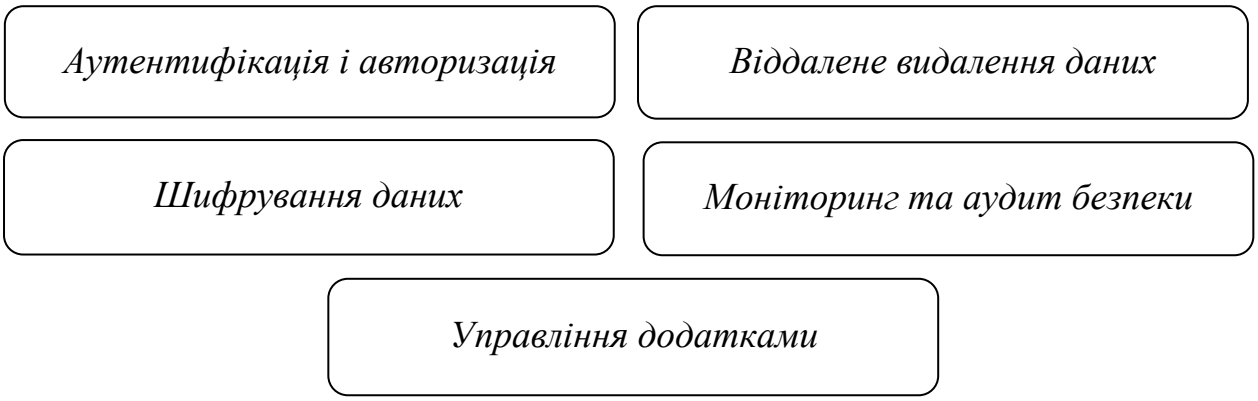

Рис. 3.1. Основні елементи політики безпеки мобільних пристроїв

1) *аутентифікація і авторизація*: вимоги до паролів, використання біометричних методів аутентифікації, двофакторна аутентифікація;

2) *шифрування даних*: вимоги до шифрування даних у спокої та під час передачі;

3) *управління додатками*: список схвалених додатків, обмеження прав доступу додатків;

4) *віддалене видалення даних*: можливість видалення даних на втрачених або викрадених пристроях з віддаленого доступу;

5) *моніторинг та аудит безпеки*: перевірка на використання слабких паролів, реагування на підозрілі дії [41, с. 105].

Ці правила і процедури допомагають забезпечити, що мобільні пристрої використовуються безпечно і зберігають конфіденційні дані в безпеці.

Якщо потрібно розробити стратегію управління ризиками для мобільних пристроїв, основними етапами будуть:

1) *визначення потенційних загроз та вразливостей*. Цей етап передбачає аналіз потенційних загроз безпеці мобільних пристроїв організації. Загрози можуть включати втрату або крадіжку пристроїв, несанкціонований доступ до даних, атаки з використанням шкідливих програм тощо. Також важливо визначити вразливості, які можуть бути використані зловмисниками для атаки на мобільні пристрої;

2) *визначення стратегії*. На цьому етапі визначають цілі безпеки компанії, ролі та відповідальності за забезпечення безпеки мобільних пристроїв, а також ідентифікують заходи безпеки, які необхідно впровадити для зменшення ризиків;

3) *розробка політик*. На цьому етапі створюються політики безпеки, які встановлюють вимоги до захисту даних і пристроїв. Ці політики можуть визначати, зокрема, вимоги до шифрування даних, аутентифікації користувачів, управління додатками та інші аспекти безпеки;

4) *впровадження та навчання*. Етап передбачає впровадження стратегії управління ризиками і проведення навчання для персоналу щодо виконання політик і процедур безпеки, правильного використання мобільних пристроїв та виконання заходів безпеки;

5) *моніторинг і аудит*. На цьому етапі здійснюється постійний моніторинг безпеки мобільних пристроїв і проводиться аудит для виявлення та виправлення вразливостей. Це допомагає вчасно реагувати на можливі загрози безпеці;

6) *постійне вдосконалення*. Цей етап охоплює постійне оновлення та вдосконалення стратегій і політик безпеки на основі нових вимог і загроз. Це дозволяє забезпечити ефективний захист мобільних пристроїв у міру їхнього розвитку та появи нових загроз.

Визначення політики безпеки для мобільних пристроїв є фундаментальним кроком у створенні надійного й ефективного захисту корпоративних даних в

організації. Політика безпеки встановлює чіткі правила і процедури для управління й використання мобільних пристроїв працівниками, що допомагає зменшити ризики та захистити організацію від потенційних загроз.

Основні аспекти політики безпеки мобільних пристроїв представлені в таблиці 3.1.

Таблиця 3.1

Основні аспекти політики безпеки мобільних пристроїв

Категорія	Аспект	Опис
Сфера застосування політики	Визначення пристроїв	Уточнення, які мобільні пристрої входять у сферу застосування політики (службові, особисті пристрої в режимі BYOD тощо).
	Користувачі	Ідентифікація користувачів або груп користувачів, на яких діє політика.
Вимоги до безпеки	Аутентифікація і контроль доступу	Встановлення вимог до аутентифікації користувачів, таких як використання складних паролів, біометричних даних або багаторівневої аутентифікації.
	Шифрування	Вимоги до шифрування даних на пристрої та даних, що передаються.
	Управління додатками	Контроль за додатками, які можуть бути встановлені та використовувані на мобільних пристроях.
Процедури забезпечення безпеки	Заходи щодо запобігання втраті даних	Політики щодо резервного копіювання даних, використання хмарних сервісів, а також заходів у випадку втрати або крадіжки пристрою.
	Моніторинг і реагування на інциденти	Встановлення процедур для моніторингу безпеки та вживання заходів при виявленні інциденту безпеки.

Продовження таблиці 3.1

Обов'язки та відповідальності користувачів	Вимоги до користувачів	Вимоги до користувачів щодо дотримання політик, збереження конфіденційності даних, та повідомлення про будь-які безпекові інциденти або підозрілі дії.
Правила використання пристроїв	Огляд правил	Огляд правил використання мобільних пристроїв, включаючи обмеження на використання пристроїв у певних середовищах або встановлення певних додатків.
Періодичний перегляд політики	Перегляд політики	Політика має регулярно переглядатися та оновлюватися для адаптації до нових технологічних розвитків, змін у регулятивному середовищі, або змін у внутрішній політиці компанії.

Розробка і впровадження ефективної політики безпеки мобільних пристроїв є необхідною для захисту корпоративних даних і ресурсів від сучасних загроз і викликів, які постійно змінюються в динамічному цифровому світі.

3.2 Розробка процедур і заходів управління мобільною безпекою

У сучасному цифровому світі мобільні пристрої відіграють важливу роль у повсякденному житті людей і діяльності підприємств. Відтак, забезпечення безпеки цих пристроїв стає надзвичайно важливим завданням. Розробка процедур і заходів управління безпекою мобільних пристроїв є кроком до забезпечення захисту від різноманітних загроз і вразливостей. У цьому контексті важливо визначити ефективні стратегії та заходи, які дозволять забезпечити безпеку мобільних пристроїв у рамках підприємства (Рис. 3.2).

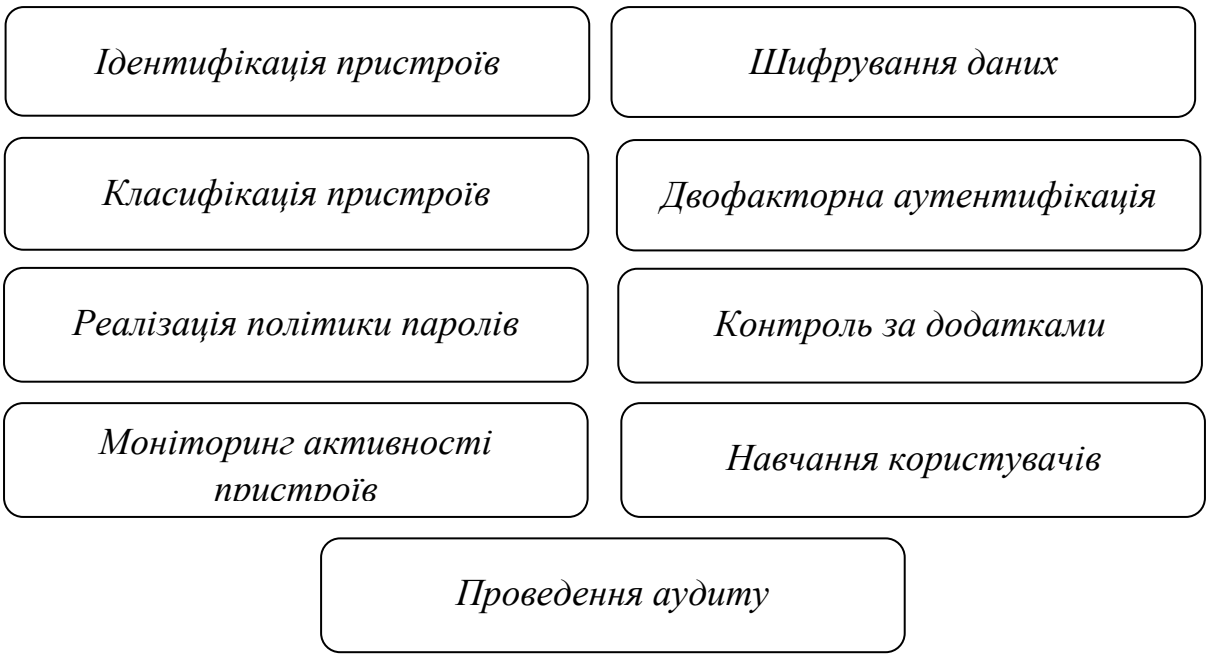

Рис. 3.2. Заходи забезпечення безпеки мобільних пристроїв на підприємстві

Ідентифікація пристроїв може бути здійснена за допомогою унікальних номерів серії та моделі, які можуть бути вбудовані в апаратне забезпечення пристрою або присвоєні під час реєстрації пристрою у системі управління мобільними пристроями. Для забезпечення унікальності ідентифікаційних номерів використовуються криптографічні алгоритми, які гарантують відсутність можливості підробки або дублювання цих номерів.

Класифікація пристроїв за рівнем конфіденційності даних може бути здійснена на основі внутрішніх політик безпеки організації. Наприклад, дані можуть бути класифіковані як високо конфіденційні, середньо конфіденційні та низько конфіденційні в залежності від їх важливості та можливих наслідків в разі втрати або несанкціонованого доступу до них. Кожному рівню конфіденційності можуть бути назначені відповідні заходи безпеки, такі як шифрування даних, обмеження доступу або застосування додаткових методів аутентифікації для забезпечення захисту інформації на мобільних пристроях.

Реалізація *політики паролів* передбачає встановлення вимог до складних паролів, які включають в себе комбінацію різних символів (букви верхнього й нижнього регістрів, цифри, спеціальні символи) і мають достатню довжину.

Паролі повинні періодично змінюватися для зменшення ймовірності їх викрадення або підбору.

Щодо *шифрування даних*, то важливо встановити вимоги до шифрування інформації, яка зберігається на мобільних пристроях, а також під час їх передачі в мережі. Це може бути досягнуто за допомогою вбудованих засобів шифрування в операційних системах мобільних пристроїв або застосування сторонніх програмних рішень.

Контроль за додатками передбачає обмеження на встановлення додатків з неперевірених джерел. Це може бути досягнуто шляхом використання механізмів управління додатками (наприклад, Google Play Protect для Android або App Store для iOS), які дозволяють перевіряти додатки на наявність шкідливого коду та інших загроз перед їх встановленням на пристрій. Також можна встановити політику, що забороняє встановлення додатків з невідомих або ненадійних джерел, що допоможе зменшити ризик встановлення шкідливого програмного забезпечення на мобільний пристрій.

Реалізація *двофакторної аутентифікації* передбачає вимогу до введення двох різних видів ідентифікаційної інформації для доступу до пристрою або даних. Наприклад, це може бути комбінація чогось, що користувач знає (наприклад, пароль), і чогось, що він має (наприклад, код з SMS або додатковий підтверджуючий токен). Це забезпечує більш високий рівень безпеки, оскільки навіть якщо зловмисник дізнається пароль, йому все одно буде важко отримати доступ до пристрою без другого фактору аутентифікації.

Контроль доступу до даних залежно від ролі користувача може бути реалізований шляхом встановлення відповідних прав доступу до окремих функцій або даних на пристрої. Наприклад, адміністратор системи може мати повний доступ до всіх функцій і даних, тоді як звичайні користувачі можуть мати доступ лише до обмеженого набору функцій або даних. Це дозволяє забезпечити, щоб користувачі мали доступ лише до тих даних, які їм потрібні для виконання їхніх робочих обов'язків, що допомагає уникнути несанкціонованого доступу та зменшує ризик витоку конфіденційної інформації.

Моніторинг активності пристроїв може здійснюватися за допомогою спеціалізованих програмних засобів, які аналізують логи, дії користувачів та інші параметри пристроїв для виявлення незвичайних або підозрілих дій. Наприклад, такі програми можуть виявляти спроби неуспішної аутентифікації, незвичайні запити на доступ до даних чи надмірну активність на пристрої.

Моніторинг активності пристроїв передбачає вжиття негайних дій у випадку виявлення або підозри на інцидент безпеки. Це може включати припинення підозрілих процесів або заборону доступу до певних ресурсів, виконання антивірусного сканування пристрою або негайне повідомлення відповідних служб або адміністраторів системи. Важливо мати якісну процедуру реагування на інциденти, яка містить чіткий план дій та визначає відповідальність за їх виконання, щоб уникнути серйозних наслідків в разі виникнення інциденту [42, с. 88].

Навчання користувачів щодо правил користування мобільними пристроями та безпеки інформації може бути реалізоване через різні канали і методи:

1) проведення регулярних тренінгів і семінарів з безпеки інформації для співробітників з аналізом актуальних загроз і способів захисту, демонстрацією практичних прикладів та вправ для засвоєння матеріалу;

2) розроблення навчальних матеріалів, таких як інструкції, відеоуроки, інфографіка, які будуть доступні для співробітників для самостійного вивчення правил користування мобільними пристроями та безпеки інформації;

3) проведення тестів або опитувань для оцінки рівня знань персоналу з питань безпеки інформації та користування мобільними пристроями. Це дозволяє виявити слабкі місця у знаннях та обізнаності щодо правил безпеки;

4) поширення інформації з питань безпеки мобільних пристроїв серед персоналу, включаючи розуміння важливості заходів безпеки та їх вплив на компанію;

5) забезпечення постійного навчання та оновлення інформації про нові загрози та способи захисту [43, с. 71].

Реалізація цих заходів допоможе підвищити рівень усвідомлення безпеки серед користувачів та зменшити ймовірність виникнення інцидентів безпеки.

Важливу роль у забезпеченні безпеки мобільних пристроїв відіграє належна *система аудиту*, яка дозволяє реєструвати дії користувачів і виявляти можливі проблеми безпеки. Розглянемо основні аспекти реалізації системи аудиту.

Система аудиту має здатність реєструвати дії користувачів, такі як вхід в систему, виконання певних операцій, доступ до конфіденційної інформації та інші дії, які можуть бути важливими з точки зору безпеки.

Система аудиту може працювати в режимі реального часу, що дозволяє виявляти незвичайні або підозрілі дії користувачів та негайно реагувати на них.

Варто забезпечити надійне зберігання логів аудиту для подальшого аналізу та виявлення шаблонів поведінки, що можуть свідчити про потенційні загрози.

Система аудиту може автоматично аналізувати логи на предмет незвичайних або підозрілих дій та запускати процедури реагування на потенційні загрози.

Система аудиту може бути інтегрована з іншими системами безпеки, такими як системи виявлення вторгнень або системи управління інформацією та подіями безпеки (SIEM), для більш ефективного виявлення та реагування на загрози [44, с. 66].

Загалом, система аудиту грає важливу роль у забезпеченні безпеки мобільних пристроїв, дозволяючи швидко і ефективно виявляти й реагувати на можливі загрози.

Постійне вдосконалення політик безпеки та процедур є важливою складовою управління безпекою мобільних пристроїв. Основними кроками реалізації цього процесу є:

1) проведення аналізу попередніх інцидентів безпеки для виявлення слабких місць у системі безпеки та розроблення заходів для їх усунення;

2) проведення періодичної оцінки ризиків, пов'язаних з використанням мобільних пристроїв, і внесення змін до політик безпеки для їх зменшення;

3) виявлення нових загроз і технологій, які можуть вплинути на безпеку мобільних пристроїв, і внесення відповідних змін до політик безпеки;

4) регулярне оновлення політик безпеки на основі вищезазначених аналізу й оцінювання, а також з урахуванням змін у законодавстві та стандартах безпеки;

5) навчання й інформування персоналу про зміни в політиках безпеки та процедурах, щоб вони були обізнані та дотримувалися цих політик;

6) проведення регулярних аудитів для перевірки дотримання політик безпеки та відстеження виконання рекомендацій з їх вдосконалення;

7) впровадження нових технологій і рішень безпеки для підвищення ефективності та безпеки мобільних пристроїв.

Ці кроки допоможуть забезпечити постійне вдосконалення політик безпеки та процедур, що використовуються для управління безпекою мобільних пристроїв на підприємстві.

Розробка процедур і контрольних заходів для управління безпекою мобільних пристроїв є важливою складовою стратегії безпеки в сучасних умовах. Запровадження цих заходів дозволяє зменшити ризики втрати конфіденційної інформації, захистити користувачів від шкідливих програм і забезпечити надійний захист даних.

3.3 Реалізація та моніторинг системи управління безпекою

Реалізація системи управління безпекою мобільних пристроїв у компанії вимагає впровадження комплексних технічних і організаційних заходів:

1) встановлення на мобільні пристрої антивірусного програмного забезпечення, шифрувальних засобів, інструментів для управління мобільними пристроями та засобів забезпечення віддаленого доступу та контролю;

2) налаштування політик безпеки на пристроях, включно з політиками доступу, шифрування та ідентифікації/аутентифікації;

3) забезпечення інтеграції мобільних пристроїв з корпоративними системами безпеки для управління ідентифікацією, політиками доступу та моніторингу;

4) проведення брифінгів та навчальних сесій для працівників, щоб вони розуміли та дотримувались встановлених політик безпеки.

Моніторинг та оцінка ефективності системи управління безпекою є критично важливими для забезпечення захисту мобільних пристроїв:

1) регулярний моніторинг через системи MDM, які дозволяють відстежувати стан безпеки мобільних пристроїв і збирати дані про інциденти безпеки;

2) аналіз логів системи та аудит активності користувачів для виявлення можливих зловживань або аномалій у безпеці;

3) виконання регулярних перевірок безпеки та тестувань на проникнення для оцінки працездатності заходів безпеки і виявлення потенційних слабких місць;

4) перевірка реагування на інциденти, аналіз його ефективності;

5) використання результатів моніторингу й аналізу для постійного вдосконалення системи управління безпекою. Це включає оновлення політик безпеки, вдосконалення процедур і впровадження нових технологій і методів захисту;

6) використання штучного інтелекту й аналітики для автоматизації моніторингу та виявлення вразливостей у безпеці мобільних пристроїв;

7) забезпечення взаємодії з постачальниками програмного забезпечення та послуг у галузі безпеки мобільних пристроїв та обміну інформацією про загрози;

8) регулярне звітування про стан безпеки мобільних пристроїв та їх аудит для внутрішнього і зовнішнього використання.

Моніторинг та реалізація цих заходів дозволяють підприємствам ефективно управляти безпекою мобільних пристроїв та забезпечити захист від потенційних загроз інформаційної безпеки.

Розробка та реалізація системи управління безпекою мобільних пристроїв є важливим завданням для будь-якої сучасної організації. Враховуючи швидкий розвиток технологій і збільшення кількості загроз інформаційній безпеці, важливо вживати комплексних заходів для забезпечення захисту даних і пристроїв.

Виконання процедур і заходів, визначених у системі управління безпекою, дозволяє ефективно управляти ризиками та зменшити ймовірність інцидентів безпеки. Важливою складовою є постійне вдосконалення системи, враховуючи нові технології та загрози.

Моніторинг системи управління безпекою допомагає вчасно виявляти потенційні проблеми та реагувати на них, щоб запобігти серйозним наслідкам. Співпраця зі сторонніми постачальниками та постійний аналіз стану безпеки допомагають забезпечити високий рівень захисту.

Отже, ефективна система управління безпекою мобільних пристроїв є важливою складовою успішної діяльності будь-якої організації, що використовує ці пристрої в своїй роботі.

3.4 Оцінка ефективності системи управління безпекою

Для проведення оцінки ефективності системи управління безпекою мобільних пристроїв можна використовувати комплексний підхід, який передбачає оцінку різних аспектів безпеки (Рис. 3.3):

Рис. 3.3. Аспекти оцінювання ефективності системи управління мобільною безпекою

1) *рівень виконання політики безпеки*:

a) оцінка відповідності паролів вимогам безпеки;

b) перевірка наявності й активності антивірусного ПЗ;

c) перевірка наявності й активності програм для виявлення шкідливих програм;

2) *рівень шифрування даних*:

a) перевірка наявності та правильності налаштувань шифрування файлів і папок;

b) перевірка наявності та правильності налаштувань шифрування даних під час їх передачі;

3) *рівень доступу до даних*:

a) перевірка рівня аутентифікації користувачів для доступу до даних;

b) перевірка правильності налаштувань доступу до даних залежно від ролі користувача;

4) *моніторинг та виявлення інцидентів*:

a) перевірка наявності та правильності налаштувань систем моніторингу та виявлення підозрілих активностей;

b) перевірка реакції системи на підозрілі або незвичайні активності;

5) *реагування на інциденти*:

a) оцінка швидкості й ефективності реакції на інциденти безпеки;

b) аналіз вжитих заходів для вирішення інцидентів та їх ефективності;

6) *навчання користувачів*:

a) оцінка доступності й ефективності навчальних матеріалів щодо безпеки мобільних пристроїв;

b) аналіз реакції користувачів на навчання та їх здатність до дотримання правил безпеки;

7) *впровадження оновлень і виправлень (патчів)*:

a) перевірка наявності й ефективності системи впровадження оновлень і патчів;

b) оцінка частоти й регулярності впровадження оновлень.

8) *ступінь відповідності стандартам безпеки*: перевірка відповідності системи управління безпекою встановленим стандартам безпеки (наприклад, NIST [20] або ISO 27001 [29]).

Після проведення оцінки за цими критеріями складають звіт із рекомендаціями для покращення системи управління мобільною безпекою.

Висновки до розділу 3

Встановлено, що політика безпеки мобільних пристроїв визначає набір правил, процедур і технологічних заходів, які організація встановлює для захисту даних і мобільних пристроїв. Основними елементами політики безпеки мобільних пристроїв є: аутентифікація і авторизація, шифрування даних, управління додатками, віддалене видалення даних, моніторинг та аудит безпеки.

Розробка процедур і заходів управління безпекою мобільних пристроїв є кроком до забезпечення захисту від різноманітних загроз і вразливостей. У цьому контексті важливо впроваджувати ефективні заходи, які забезпечать безпеку мобільних пристроїв, зокрема їх ідентифікацію та класифікацію, реалізацію політики паролів, встановлення вимог до шифрування даних, контролю за додатками, двофакторну аутентифікацію, контроль доступу до даних, моніторинг активності пристроїв, навчання користувачів.

Дослідження показало, що важливу роль у забезпеченні мобільної безпеки відіграє система аудиту, яка дозволяє реєструвати дії користувачів і виявляти можливі проблеми безпеки. Обов’язковим є постійне вдосконалення політик безпеки та процедур, яке є важливою складовою управління безпекою мобільних пристроїв. Реалізація та моніторинг системи управління мобільною безпекою має охоплювати впровадження комплексних технічних і організаційних заходів.

Оцінювання ефективності системи управління безпекою мобільних пристроїв включає перевірку виконання політики безпеки, рівнів шифрування та доступу до даних, ефективності моніторингу, виявлення й реагування на інциденти, оновлення та виправлення, навчання користувачів.

ВИСНОВКИ

У кваліфікаційній роботі проведено дослідження проблематики управління безпекою мобільних пристроїв в корпоративному середовищі. Значення мобільних пристроїв у сучасному діловому та особистому спілкуванні не може бути переоцінене, проте це також вносить певні ризики, які вимагають комплексного підходу до їх управління та захисту.

У першому розділі розглянуто теоретичні основи управління безпекою мобільних пристроїв, де основна увага була приділена аналізу сучасного стану мобільних технологій та їх впливу на корпоративну безпеку. Визначення та класифікація мобільних пристроїв допомогла усвідомити різноманітність та специфіку загроз, які вони несуть.

Другий розділ зосереджений на аналізі та оцінці ризиків, асоційованих з використанням мобільних пристроїв в корпоративних системах. Розглянуто методологію оцінки ризиків за концепцією NIST, що дозволило виявити основні вразливі місця та потенційні загрози. Практичне застосування цієї методології в корпоративних умовах демонструє її ефективність у зниженні потенційних ризиків.

Третій розділ присвячений розробці стратегій управління безпекою мобільних пристроїв згідно з рекомендаціями NIST. Він включав визначення політик, розробку процедур, реалізацію та моніторинг систем управління безпекою. Застосування цих стратегій на практиці дозволяє не тільки реагувати на існуючі виклики, але й проактивно адаптуватися до мінливих умов.

Підсумовуючи, слід констатувати, що впровадження комплексного підходу до управління безпекою мобільних пристроїв є критично важливим для забезпечення цілісності та конфіденційності корпоративної інформації. Рекомендації NIST слугують надійним орієнтиром для організацій, що прагнуть оптимізувати свої системи інформаційної безпеки в умовах зростаючої залежності від мобільних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке мобільний пристрій? URL: http://surl.li/uigfs
2. Скіцько О. І. Деякі аспекти системи управління інформаційною безпекою мобільних пристроїв в мережі. С. 271-274.
3. Serdiukov D. Sievierinov O., Sydorenko Z. Особливості розгортання застосунку eset mdm/mdc для забезпечення безпеки мобільних пристроїв. Системи управління, навігації та зв'язку. Збірник наукових праць, 4(74), 2023. С. 102-105.
4. Nechvolod K., Sievierinov O. and Vlasov A. Аналіз безпеки даних в EMM системах. Системи управління, навігації та зв'язку: Збірник наукових праць 3.55, 2019. С. 131-134.
5. Кожедуб Ю. Реалізація процесного підходу до керування ризиками інформаційної безпеки в документах NIST. Information Technology and Security, (5,№ 2), 2017. С. 76-89.
6. 4 main reasons why SMEs and SMBs fail after a major cyberattack. URL: https://www.csoonline.com/article/565034/4-main-reasons-why-smes-and-smbs-fail-after-a-major-cyberattack.html
7. Стайкуца С., Кільдішев В., Гуренко А., Корольов А. Кібербезпека підприємств малого бізнесу на основі рішень та рекомендацій NIST. Scientific Collection «InterConf», (166), 2023. С. 271-279.
8. Small business cybersecurity corner. Корпоративний сайт NIST. 2023. URL: https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics
9. National Institute of Standardsand Technology (NIST). Корпоративний сайт NIST. 2023. URL: https://www.nist.gov/.
10. Башинська І. О. Інноваційно-інформаційні технологій для забезпечення інтелектуально-кадрової складової економічної безпеки підприємства. Херсон: Грінь ДС, 2016. С. 606-635.
11. Hasan B. A conceptual framework for mobile security supporting enterprises in adopting mobility (Doctoral dissertation, Universität Oldenburg), 2019. 206 с.

12. Тимощук В., Стебельський М. Шифрування даних в операційних системах. Матеріали VI Міжнародної студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання “, 2023. С. 183-184.

13. Yesilyurt M., Yalman Y. Security threats on mobile devices and their effects: estimations for the future. International Journal of Security and Its Applications, 10(2), 2016. С. 13-26.

14. Jeon W. R., Kim J. Y., Lee Y. S., Won D. H. Analysis of Threats and Countermeasures on Mobile Smartphone. Journal of The Korea Society of Computer and Information, 16(2), 2011. С. 153-163.

15. Rizvi S., Labrador G., Hernandez W., Karpinski K. Analysis of Mobile Threats and Security Vulnerabilities for Mobile Platforms and Devices. In Security, Privacy and Reliability in Computer Communications and Networks, River Publishers, 2022. С. 139-173.

16. Lopes H., Lopes R. (2013). Comparative analysis of mobile security threats and solution. Int. Journal of Engineering Research and Application, 3(5), 499-502.

17. Seo S. H., Gupta A., Sallam A. M., Bertino E., Yim K. Detecting mobile malware threats to homeland security through static analysis. Journal of Network and Computer Applications, 38, 2014. С. 43-53.

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

19. NIST Cybersecurity Framework, Riadi I. Forensic analysis whatsapp mobile application on android-based smartphones using national institute of standard and technology (nist) framework. vol, 8, 2019. С. 223-231.

20. Souppaya M., Scarfone K. Guidelines for managing the security of mobile devices in the enterprise. NIST special publication, 800, 2013. 124 с.

21. Yuliani V. A., Riadi I. Forensic analysis whatsapp mobile application on android-based smartphones using national institute of standard and technology (nist) framework. vol, 8, 2019. С. 223-231.

22. Riadi I., Umar R., Firdonsyah A. Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. International Journal of Computer Science and Information Security (IJCSIS), 15(5), 2017. С. 3-8.

23. Franklin J. M., Howell G., Boeckl K., Lefkovitz N., Nadeau E., Shariati D. B., Sandlin K. F. Mobile device security corporate-owned personally-enabled (COPE), 2019. 352 с.

24. Halpert B. Mobile device security. In Proceedings of the 1st annual conference on Information security curriculum development, 2004. С. 99-101.

25. Saarinen M. J. O. Mobile energy requirements of the upcoming NIST post-quantum cryptography standards. In 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2020. С. 23-30.

26. Chen L., Franklin J., Regenscheid A. Guidelines on hardware-rooted security in mobile devices (Draft). NIST Special Publication, 800(164), 2012. С. 10-11.

27. Choong Y. Y., Greene K., Franklin J. Usability and security considerations for public safety mobile authentication (No. NIST Internal or Interagency Report (NISTIR) 8080 (Draft)). National Institute of Standards and Technology, 2015. 44 с.

28. Becher M., Freiling F. C., Hoffmann J., Holz T., Uellenbeck S., Wolf C. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In 2011 IEEE Symposium on Security and Privacy, 2011. С. 96-111.

29. ISO/IEC 27001:2013(E) Information technology - Security techniques - Information security management systems – Requirements. 34 p.

30. Андреєва Г. В., Стеценко Н. О. Інформаційна безпека: сучасні виклики та перспективи. К.: Журнал «Наука і освіта», №1 (45), 2018. С. 23-34.

31. Білецький В. С., Герасименко Ю. М. Захист інформації в умовах кіберзагроз. К.: Вісник НАУ, №3 (67), 2019. С. 45-54.

32. Гаврилюк А. І., Мельник О. М. Інформаційна безпека підприємства: теоретичні та практичні аспекти. К.: Вісник ЛНУ імені Тараса Шевченка, №4 (92), 2020. С. 78-89.

33. Даниленко С. В., Коваленко Р. О. Методи та засоби захисту інформації. К.: Збірник наукових праць УкрДМТУ, №5 (68), 2017. С. 33-42.

34. Жук І. В., Тарасенко А. С. Сучасні тенденції в управлінні інформаційною безпекою. К.: Журнал «Економіка та управління», №2 (51), 2018. С. 112-121.

35. Захарченко П. О., Бойко В. А. Інформаційна безпека: основні положення та методи забезпечення. К.: Вісник НТУУ «КПІ», №1 (57), 2019. С. 67-75.

36. Іванова Л. В., Мартинюк В. П. Формування політики інформаційної безпеки підприємства. К.: Збірник наукових праць ХНЕУ, №3 (64), 2021. С. 98-109.

37. Клименко О. М., Савченко Л. В. Управління ризиками інформаційної безпеки. К.: Журнал «Інформаційні технології», №4 (76), 2017. С. 44-52.

38. Левченко А. І., Петров М. С. Системи управління інформаційною безпекою. К.: Журнал «Науковий вісник», №5 (88), 2020. С. 56-64.

39. Мороз С. В., Кучерук Н. Г. Стратегії захисту інформації в умовах глобалізації. К.: Вісник ОНУ імені І. І. Мечникова, №2 (47), 2018. С 22-32.

40. Новак О. В., Сидоренко В. П. Аналітичні методи захисту інформації. К.: Журнал «Інформаційні системи», №3 (73), 2019. С. 49-57.

41. Пилипенко Г. М., Шевченко Ю. В. Моделі управління інформаційною безпекою. К.: Вісник КНТЕУ, №6 (84), 2021. С. 105-114.

42. Романчук І. М., Суховій Т. В. Організаційні аспекти забезпечення інформаційної безпеки. К.: Журнал «Економічна безпека», №2 (59), 2020. С. 88-97.

43. Соловей О. С., Ковальчук Д. І. Технології інформаційної безпеки. К.: Збірник наукових праць ХНУРЕ, №1 (62), 2018. С. 71-79.

44. Ткаченко В. П., Лисенко І. О. Підходи до захисту інформації в сучасних умовах. К.: Вісник НУБіП, №4 (91), 2021. С. 66-75.