

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ**

Пояснювальна записка

до магістерської роботи
на тему:

**«ТЕХНОЛОГІЯ ЗАХИСТУ МОБІЛЬНИХ ПРИСТРОЇВ НА БАЗІ McAfee
MOBILE SECURITY»**

Виконав студент 6 курсу, групи БСДМ-63
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та
кібернетична безпека»

(шифр і назва спеціальності)

Долинний Д.В.

(прізвище та ініціали)

Керівник

Чумак Н.С.

(прізвище та ініціали)

Рецензент

(прізвище та ініціали)

Нормоконтролер

Чумак Н.С.

(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут	ННІЗІ
Кафедра	Інформаційної та кібернетичної безпеки
Ступінь вищої освіти	Магістр
Спеціальність	125 Кібербезпека
Освітньо-професійна програма	Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ

Завідувач кафедри ІКБ

Гайдур Г.І.

“ ” 2022 року

З А В Д А Н Н Я НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Долинному Дмитру Вікторовичу

(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія захисту мобільних пристроїв на базі McAfee Mobile Security»

керівник магістерської роботи Чумак Надія Степанівна, старший викладач

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від «12» жовтня 2022 року №122.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи
мобільні пристрої;

рішення для захисту мобільних пристроїв;

наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Актуальність проблеми захисту мобільних пристроїв.

2. Види загроз на мобільні пристрої.

3. Аналіз методів забезпечення безпеки мобільних пристроїв

4. Аналіз рішень для захисту мобільних пристроїв.

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

2. Об'єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу методів та засобів захисту мобільних пристроїв.

4. Призначення та можливості рішення McAfee Mobile Security.

5. Аналіз рішень для захисту мобільних пристроїв.

6. Рекомендації щодо застосування рішень для захисту мобільних пристроїв. McAfee Mobile Security.

7. Висновки за результатами роботи.

6. Дата видачі завдання 26.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту мобільних пристроїв.	26.09.2022 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	30.09.2022 р.	
3.	Аналіз методів та засобів захисту мобільних пристроїв.	15.10.2022 р.	
4.	Розроблення методів забезпечення безпеки мобільних пристроїв.	26.10.2022 р.	
5.	Розроблення рекомендацій щодо застосування рішень для захисту мобільних пристроїв.	17.11.2022 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	29.11.2022 р.	
7.	Підготовка доповіді до захисту.	15.12.2022 р.	

Студент

(підпис)

Долинний Д.В.

прізвище та ініціали

Керівник магістерської роботи

(підпис)

Чумак Н.С.

прізвище та ініціали

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Долинний Д.В. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія захисту мобільних пристроїв на базі McAfee Mobile Security».

Магістерська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Долинний Д.В. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2021 року по 2023 рік повністю виконав навчальний план за напрямом підготовки,
спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту _____ Бреславська Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент Долинний Д.В. обрав тему роботи, метою якої було дослідити зміст технології захисту мобільних пристроїв на базі McAfee Mobile Security. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Долинний Д.В. показав відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента Долинного Дмитра Вікторовича на оцінку «**задовільно**» та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник магістерської роботи _____ Чумак Н.С.
(підпис) (прізвище та ініціали)
“ ____ ” _____ 2022 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Долинний Д.В.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 58 сторінок, 7 рисунків, 15 джерел.

Об'єкт дослідження – процес забезпечення безпеки мобільних пристроїв.

Предмет дослідження – технологія управління захистом мобільних пристроїв.

Мета роботи – розробити методи захисту мобільних пристроїв та рекомендації щодо їх застосування в реальному житті.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, варіанти використання рішень для захисту мобільних пристроїв.

В роботі проведено аналіз проблеми забезпечення безпеки мобільних пристроїв, визначені види та джерела загроз. Проаналізовано існуючі технології захисту мобільних пристроїв при щоденному їх використанні.

Досліджено методи та засоби захисту мобільних пристроїв на прикладі рішення McAfee Mobile Security. Проведено порівняльний аналіз та визначено різницю у використанні рішення McAfee Mobile Security в ОС Android та IOS.

Галузь використання – кібербезпека корпоративної інформаційної системи.

БЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ, КІБЕРБЕЗПЕКА, ЕЛЕКТРОННИЙ ПРИСТРІЙ, КОРПОРАТИВНЕ СЕРЕДОВИЩЕ, МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МОБІЛЬНИХ ПРИСТРОЇВ

ABSTRACT

The text part of the master's thesis: 58 pages, 7 figures, 15 sources.

The object of research – the process of ensuring the security of mobile devices.

The subject of research – the technology of managing the protection of mobile devices.

The aim of research – to develop methods of protecting mobile devices and recommendations for their use in real life.

Research methods – study of the literature on this topic, analysis of operating documentation, options for using solutions to protect mobile devices.

The paper analyzes the problem of ensuring the security of mobile devices, identifies the types and sources of threats. Existing technologies for protecting mobile devices during their daily use are analyzed.

Methods and means of protecting mobile devices are studied using the McAfee Mobile Security solution as an example. A comparative analysis was conducted and the difference in the use of the McAfee Mobile Security solution in Android and IOS was determined.

The field of use is cyber security of the corporate information system.

MOBILE DEVICE SECURITY, CYBER SECURITY, ELECTRONIC DEVICE,
CORPORATE ENVIRONMENT, MOBILE DEVICE SECURITY METHODS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	8
ВСТУП	9
1 АНАЛІЗ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МОБІЛЬНИХ ПРИБОРІВ	10
1.1. Основні характеристики мобільних пристроїв	10
1.2. Мобільні пристрої в корпоративному середовищі.....	14
1.3. Причини та джерела загроз для мобільних пристроїв	20
2 АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МОБІЛЬНИХ ПРИБОРІВ	23
2.1. Види загроз на мобільні пристрої	23
2.2. Методи забезпечення безпеки мобільних пристроїв.....	26
2.3. Рішення для захисту мобільних пристроїв	33
3 ТЕХНОЛОГІЯ ЗАХИСТУ МОБІЛЬНИХ ПРИБОРІВ.....	47
3.1. Аналіз функцій та можливостей McAfee Mobile Security	47
3.2. Рішення подібні на McAfee Mobile Security	54
3.3. Порівняльний аналіз додатка McAfee Mobile Security на базі ОС Android та IOS.....	55
ВИСНОВКИ	60
ПЕРЕЛІК ПОСИЛАНЬ	61
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація).....	63

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

BYOD – Bring your own device

HIPAA – Health Insurance Portability and Accountability Act

PCI DSS – Payment Card Industry Data Security Standard

MitM – Man in the middle

VPN – Virtual Private Network

Wi-Fi – Wireless Fidelity

URL – Uniform Resource Locator

EICAR – European Institute for Computer Antivirus Research

GPS – Global Positioning System

ВСТУП

Зараз важко уявити світ без мобільних пристроїв, але колись не було такої розкоші. Це було не так давно, коли настільні та стаціонарні апаратні засоби керували індустрією. Часи змінюються, і фокус змістився в основному на світ, населений мобільними пристроями.

Оскільки світ стає все більш взаємопов'язаним, інтегрованим і інтелектуальним, мобільні пристрої відіграють все більшу роль у зміні способу життя, роботи та спілкування людей. Але це відбувається не лише в особистому житті: смартфони та планшети також швидко впроваджуються підприємствами як нові робочі інструменти, приєднуючись до існуючих ноутбуків і настільних комп'ютерів.

Безпека мобільних пристроїв стала головною проблемою для багатьох ІТ-керівників. Хакери виявляють переваги зламу як ділових, так і особистих даних, що містяться на мобільних пристроях. Оскільки багато мобільних платформ не розроблені для забезпечення повної безпеки, хакери мають сильний стимул розробляти нові методи або створювати зловмисне програмне забезпечення, орієнтоване на мобільні пристрої, спеціально для цих пристроїв.

Об'єкт дослідження – процес забезпечення безпеки мобільних пристроїв.

Предмет дослідження – технологія управління захистом мобільних пристроїв.

Мета роботи – розробити методи захисту мобільних пристроїв та рекомендації щодо їх застосування в реальному житті.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, варіанти використання рішень для захисту мобільних пристроїв.

1 АНАЛІЗ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МОБІЛЬНИХ ПРИСТРОЇВ

1.1. Основні характеристики мобільних пристроїв

Мобільний пристрій – це загальний термін для будь-якого портативного комп'ютера чи смартфона. Цей термін використовується як синонім слів «портативний», «портативний пристрій» та «портативний комп'ютер». Планшети, електронні книги, смартфони, КПК та портативні музичні плеєри з інтелектуальними можливостями – все це мобільні пристрої.

Мобільні пристрої мають схожі параметри, включаючи:

- Wi-Fi або стільниковий доступ до Інтернету
- Акумулятор, який живить пристрій протягом кількох годин
- Фізична або екранна клавіатура для введення інформації
- Розмір та вага дозволяють носити його в одній руці та маніпулювати іншою рукою
- Сенсорний інтерфейс практично у всіх випадках
- Віртуальний помічник, такий як Siri, Cortana чи Google Assistant.
- Можливість завантаження даних з Інтернету, у тому числі програм та книг
- Бездротова робота

Смартфон

Смартфони являють собою вдосконалені версії традиційних стільникових телефонів, оскільки вони мають ті ж функції, що й мобільні телефони, такі як можливість здійснювати та приймати телефонні дзвінки, текстові повідомлення та голосову пошту, але їх також можна використовувати для перегляду веб-сторінок, надсилання та отримання листів поштою, використання соціальних мереж та робити покупки онлайн. Вони також можуть завантажувати програми з Інтернету,

використовуючи стільниковий зв'язок або Wi-Fi, щоб розширити можливості смартфона безліччю способів.

Планшет

Планшети портативні, як і ноутбуки, але пропонують інший функціонал. Замість того, щоб запускати традиційні програми для ноутбуків та настільних комп'ютерів, вони запускають програми, розроблені спеціально для планшетів. Функціонал аналогічний, але не зовсім як використання ноутбука. Планшети бувають всіх розмірів, від трохи більше смартфона до маленьких ноутбуків.

Хоча можна придбати окремий аксесуар для клавіатури, планшети мають віртуальні екранні клавіатури для введення та виведення. Вони використовують сенсорний інтерфейс і замінюють звичну мишу кінчиком пальця. Є багато виробників планшетів, але серед найбільш надійних Google Pixel, Samsung Galaxy Tab, Nexus і Apple iPad.

Електронні рідери

Електронні рідери — це спеціальні планшети, призначені для читання цифрових книг. Ці цифрові книги можна придбати або безкоштовно завантажити з онлайн-джерел. Відомі лінійки електронних пристроїв для читання включають Barnes & Noble Nook, Amazon Kindle і Kobo. Також можна читати цифрові книги на планшетах, на яких встановлено програму для електронних книг. Наприклад, iPad від Apple постачається з iBooks і підтримує завантажувані пристрої для читання цифрових книг Nook, Kindle і Kobo.

Деякі портативні музичні програвачі мають доступ до Інтернету та можуть завантажувати програми, щоб додати перевагу своїм власникам. iPod touch від Apple — це iPhone без телефону. У всіх інших аспектах він пропонує той самий досвід. Висококласний Walkman від Sony — це розкішний аудіоплеєр із потоковими програмами для Android. КПК, кращий друг ділової людини протягом багатьох років, не вдавався до впровадження смартфонів, але деякі з них виготовляються з

доступом до Wi-Fi і міцним дизайном, що робить їх корисними для військових і людей, які працюють на відкритому повітрі.

Носіння розумних годинників та фітнес-трекерів є одними з найновіших доповнень до мобільних пристроїв. Багато з них працюють на тих самих мобільних операційних системах, що й телефони та планшети, і можуть запускати власні програми. Більшість носимих пристроїв поєднуються з іншим мобільним пристроєм, наприклад смартфоном, для обміну даними та створення набагато зручнішого досвіду [1].

З появою Android та iOS смартфони зараз є найпопулярнішим мобільним пристроєм, і це не без причини. Ці пристрої портативні, поміщаються в кишеню, мають мільйон і одне використання та допомагають нам бути на зв'язку в будь-який час завдяки постійному мережевому з'єднанню від оператора бездротового зв'язку. Існує багато різних пристроїв, тому легко знайти той, який відповідає всім вашим потребам.

Подібно до смартфонів, планшети мають багато тих самих переваг, але у більшому форм-факторі. Планшет справді сяє під час виконання завдань, які більше підходять для більшого дисплея з більшим часом автономної роботи. Деякі приклади включають робочі презентації, важкі ігри або навіть пряму трансляцію шоу високої чіткості на Netflix.

Портативні комп'ютери завжди були популярними, оскільки вони надають нам функціональність настільного комп'ютера, який ми можемо брати куди завгодно. Ми можемо використовувати ту саму операційну систему з тими самими програмами, а це означає, що немає кривої навчання пристрою. Наявність повнорозмірної клавіатури, однакових входних і вихідних портів і можливості підключення зовнішнього дисплея також є деякими додатковими перевагами.

Розумні годинники є відносно новими і займають певну ринкову нішу на даний момент часу. Основні переваги, які може надати нам смарт-годинник, — це можливість отримувати сповіщення та необхідну інформацію на зап'ясті без

необхідності брати інший пристрій. З деякими новими автономними моделями ми можемо приймати та приймати телефонні дзвінки так само, як наші смартфони.

Електронні пристрої для читання існують уже багато років, і вони мають деякі спільні риси з планшетами, але їхнє основне призначення – читати. Amazon Kindle і Barnes & Noble Nook зробили електронний рідер популярним вибором для людей, які люблять читати книги в цифровому форматі. Ці пристрої змінили всю концепцію читання і допомогли перенести книги в нову еру.

Портативні ігрові консолі походять ще з Gameboy від Nintendo і назавжди змінили наше уявлення про мобільні ігри. Деякі з найвідоміших мобільних ігрових пристроїв, які ми маємо сьогодні, включають Nintendo Switch і Nintendo 3DS. Зараз ігри є одним із найпопулярніших видів розваг, і потреба в таких пристроях завжди буде [2].

Нові мобільні тенденції

Мобільні пристрої отримують доступ до ресурсів розумної мережі через мобільні програми, розроблені спеціально для мобільних пристроїв. Проте будь-який тип пристрою, здатний отримати доступ до програм, атакує ці мобільні програми. Мобільні пристрої дозволяють співробітникам залишатися на зв'язку з мережею та ресурсами своєї організації під час діагностики та вирішення проблем. Розробники мобільних додатків, які прагнуть охопити найширшу аудиторію, підтримують кілька платформ. Через велику різноманітність платформ, додатків і притаманну їм мобільність керувати мобільними пристроями складніше, і їм часто не вистачає централізованих можливостей керування. Це призводить до більшої довіри до окремих користувачів для впровадження безпечних методів, таких як блокування екрана та регулярне створення резервних копій [3].

1.2. Мобільні пристрої в корпоративному середовищі

Колись здебільшого заборонені ІТ-технологіями смартфони та планшети, такі як телефони на базі Android і Apple iPad, тепер використовуються сотнями мільйонів співробітників у всьому світі для доступу, передачі та зберігання корпоративної інформації в сучасному бізнес-середовищі 24/7. Це «розширене підприємство» створює нові виклики та ускладнює ІТ. Не дивно, що безпека стала проблемою № 1 у тенденції BYOD. За останні кілька років використання мобільних пристроїв для бізнесу різко зросло, і найближчим часом воно лише прискориться.

Коли справа доходить до несанкціонованого використання смартфонів і планшетів, ІТ-організації стурбовані втратою пристроїв, витоком даних і несанкціонованим доступом до корпоративних ресурсів. Подібні занепокоєння висловлювалися щодо все більшого використання «гостьового доступу» до корпоративних мереж. У відповідь на ці передбачувані ризики організації почали впроваджувати низку заходів безпеки даних. Традиційні підходи включають засоби контролю безпеки на основі периметра, такі як брандмауери та фільтри розумного екрана. Але ніякі засоби захисту периметра не можуть захистити дані, доступ до яких зберігаються на смартфонах і планшетах, особливо поза контролем підприємства.

Мобільність приносить підприємству як переваги, так і ризики

Оскільки працівники приносять мобільні пристрої на робоче місце, багато організацій мотивовані заохочувати їх використовувати в бізнес-цілях, оскільки вони, як правило, керують:

- Підвищенням продуктивності співробітників. Мобільні пристрої можуть надати співробітникам доступ до корпоративних ресурсів і безперервну співпрацю з колегами або діловими партнерами.
- Покращенням послуг клієнтам. Співробітники відділу продажів або служби підтримки, які регулярно спілкуються з клієнтами, можуть реагувати ефективніше, безпосередньо підвищуючи задоволеність клієнтів.

- Зниженням витрат на ІТ. Дозволяючи працівникам використовувати та часто оплачувати власні мобільні пристрої та бездротові послуги, компанії потенційно можуть заощадити витрати на ІТ на покупку пристроїв, а також на послуги управління та зв'язку.

Для багатьох організацій мобільні пристрої стали невід'ємною частиною повсякденних бізнес-процесів. ІТ-адміністратори, які хочуть мобілізувати робочу силу, повинні спочатку зрозуміти, які типи мобільних пристроїв доступні, чому робочі місця впроваджують ці пристрої та проблеми, пов'язані з використанням. Їм також слід ознайомитися з різними варіантами використання, щоб краще зрозуміти переваги мобільних пристроїв у бізнесі.

Типи мобільних пристроїв

На сучасному підприємстві основні типи пристроїв, які співробітники використовують для ведення бізнесу, поділяються на дві категорії: смартфони та планшети.

Відмінності між ними в першу чергу пов'язані з розміром, який не тільки визначає доступну область дисплея, але також може відігравати роль у терміні служби батареї, обчислювальної потужності, пам'яті, сховищі та інших факторах. Тим не менш, саме площа дисплея часто є однією з головних міркувань при оцінці пристрою.

Площа дисплея в сучасних смартфонах зазвичай становить від 4 до 7,1 дюйми, а ті, що знаходяться на більшому кінці шкали, іноді називають фаблетами. Навпаки, планшети набагато більші, з площею дисплея від 8 до 18,4 дюймів.

Незважаючи на відмінності у розмірах, мобільні пристрої схожі з точки зору їхньої здатності запускати програми та підключатися до хмарних служб та серверних систем. Планшети пропонують більше обчислювальної потужності та пам'яті, що може допомогти забезпечити більш високу продуктивність, ніж смартфони. Багато планшетів також підтримують використання клавіатури. Через

більший форм-фактор і чудову продуктивність на планшетах краще розміщуються певні програми, ніж на смартфонах.

Однак програми не єдина міркування при виборі між ними. Наприклад, час автономної роботи смартфонів часто більший. А в категорії смартфонів фаблети зазвичай мають триваліший час автономної роботи, тому що вони можуть вміщувати батареї більшого розміру. Деякі фаблети також підтримують стилус, як і багато планшетів.

Переваги мобільних пристроїв у бізнесі

Для багатьох організацій переваги мобільних пристроїв переважно пов'язані з веденням бізнесу. Вони пропонують працівникам велику гнучкість, покращують робочі процеси, покращують взаємодію та допомагають зробити користувачів більш ефективними та продуктивними. Мобільні пристрої в бізнесі також забезпечують організаціям конкурентну перевагу, оскільки швидший і спільніший зв'язок дозволяє компаніям швидше приймати рішення.

Переваги мобільних пристроїв дозволяють користувачам працювати будь-де і будь-коли, зберігаючи при цьому доступ до корпоративних ресурсів. Вони можуть взяти з собою свої офіси, будь то подорож, поїздка на роботу, робота в полі або сидячи за столом вдома.

Мобільні пристрої також покращують робочий процес, розширюючи бізнес-процеси та роблячи їх ефективнішими. Вони спрощують процеси, усуваючи дублювання зусиль, тому працівники можуть виконувати завдання швидше.

Наприклад, представник по роботі з клієнтами може оновлювати інформацію про клієнта під час дзвінка з продажу замість того, щоб робити нотатки, а потім надсилати інформацію щодо повернення до офісу. Це не тільки заощаджує час та зусилля, але також може зменшити кількість помилок, які можуть виникнути внаслідок додаткових кроків. Це одна з переваг мобільних пристроїв у бізнесі.

Оптимізовані бізнес-процеси скорочують паперову роботу; нікому не потрібно чекати, щоб роздрукувати документи або надіслати їх факсом, або зберегти файли в паперовому вигляді, що знижує зусилля, необхідні для управління цими системами, при цьому заощаджуючи папір, чорнило та енергоспоживання.

Мобільні пристрої також можуть спростити спілкування. Робочі пристрої доступні для виконання наступних дій:

- швидко переглянути терміновий матеріал;
- спільна робота над документами у польових умовах;
- відповідати на запити про ресурси чи інформацію;
- брати участь у соціальних мережах; а також
- підтримувати зв'язок у різний спосіб.

Ця гнучкість та мобільність також можуть допомогти організаціям краще обслуговувати своїх клієнтів. Наприклад, технічні фахівці з виїзної підтримки можуть швидше реагувати на запити клієнтів, будь-то електронною поштою, текстовими повідомленнями або в додатку для обміну повідомленнями. Технічні фахівці також можуть надсилати або надсилати клієнтів до конкретної інформації, робити фотографії або відео та взаємодіяти з клієнтами в режимі реального часу.

Мобільні пристрої також потенційно можуть дати організації перевагу над конкурентами та швидше генерувати нові потоки доходів. Вони також можуть покращити корпоративний імідж, тому що організація може здаватися більш передовою та процвітаючою у своїй галузі.

Недоліки мобільних пристроїв у бізнесі

На жаль, мобільні пристрої схильні до багатьох тих же вразливостей, що і персональні комп'ютери. Користувачі можуть відвідувати шахрайські веб-сайти або відповідати на фішингові листи, ненавмисно завантажуючи час.

ІТ-команди, які розгортають мобільні програми без ретельного тестування на наявність проблем із безпекою, можуть поставити під загрозу всю свою

організацію. Ігнорування вразливостей пристрою або невчасне застосування патчів операційної системи також може призвести до скомпрометованого середовища. Навіть погано розгорнуті серверні системи та погано керовані політики безпеки можуть призвести до ризиків.

Проблеми також пов'язані з підтримкою різних типів пристроїв. ІТ-спеціалісти тепер мають набагато більше кінцевих точок для керування, іноді перевищуючи кількість робочих столів. Якщо пристрої містять особисту інформацію, керування стає ще складнішим. Навіть якщо організація планує запровадити корпоративну платформу керування мобільними пристроями, ІТ-спеціалісти повинні переконатися, що всі реалізовані пристрої можуть працювати з цим програмним забезпеченням.

ІТ-команди також повинні переконатися, що серверні системи здатні обробляти додаткові робочі навантаження, пов'язані з мобільними пристроями, і що ці пристрої та їхні програми можуть інтегруватися з серверними системами. Насправді системна інтеграція часто є однією з найбільших проблем, з якими стикаються організації під час мобілізації робочої сили, особливо коли мова йде про застарілі системи, які не підтримують сучасні відкриті стандарти.

Крім того, організації повинні враховувати відповідність і галузеві норми під час мобілізації своєї робочої сили. Наприклад, ІТ-команді може знадобитися переконатися, що впровадження пристроїв не призведе до порушення таких стандартів, як HIPAA або PCI DSS.

ІТ-команди повинні враховувати плани обслуговування операторів, які супроводжуються впровадженням мобільних пристроїв. Деякі тарифні плани можуть обмежувати кількість дзвінків чи повідомлень або обсяг використаних даних. Також можуть існувати регіональні обмеження, як-от виїзд за межі країни або дзвінки в іншу країну. ІТ-спеціалістам може знадобитися встановити систему для моніторингу та контролю за використанням або для вимикання пристроїв, які втрачені, викрадені чи загублені.

Ще одна проблема, яку варто відзначити, — це важливість доставки правильних пристроїв потрібним користувачам. Наприклад, техніку, який працює в полі, може знадобитися тримати одну руку вільною під час роботи над системою, і в цьому випадку планшет буде надто громіздким і потенційно може знизити продуктивність. У той же час, вибрані пристрої повинні бути в змозі працювати з усіма додатками, які їм потрібні для запуску, інакше ці пристрої в кінцевому підсумку нікому не знадобляться.

Переваги керування мобільними пристроями

Є численні переваги мобільних пристроїв для співробітників, які виконують різноманітні бізнес-ролі.

Зверніть увагу на менеджерів по роботі з клієнтами безпосередньо. За допомогою відповідних мобільних пристроїв менеджери по роботі з клієнтами можуть виконувати численні завдання, не повертаючись до офісу, наприклад:

- розміщення замовлень;
- оновлення інформації про клієнтів;
- отримання цін і ставок дисконту; і
- пересилання інформації про товар клієнтам.
- інший приклад - агент з нерухомості.

Відвідуючи нерухомість або відвідуючи клієнтів, ріелтор може використовувати свій мобільний пристрій для:

- переглядання товарних запасів;
- подавати списки;
- надавати клієнтам віртуальні тури або показувати їм різні списки.

Крім того, є будівельний інспектор, який може використовувати мобільний пристрій для кількох додатків:

- переглядати інформацію про клієнтів або історію інцидентів;
- заповнити та подати бланк перевірки;

- попросіть клієнта підписати перевірку.

Насправді мобільні пристрої можуть допомогти більшості польових працівників виконувати свою роботу ефективніше.

Відділи кадрів також можуть отримати вигоду від того, що співробітники використовують мобільні пристрої. Програми HR можуть допомогти співробітникам різними способами:

- подавати табель обліку робочого часу;
- заповнювати звіти про витрати;
- затверджувати графіки тренувань; і
- отримувати оголошення по всій компанії.

Співробітники в усіх галузях промисловості можуть використовувати мобільні пристрої незліченною кількістю інших способів, а також:

- переглядати або керувати робочими замовленнями;
- генерувати квитки підтримки; і отримувати підписи на документах [4].

1.3. Причини та джерела загроз для мобільних пристроїв

Мобільні пристрої можуть атакуватися на різних рівнях. Це включає потенціал для шкідливих додатків, атак на мережевому рівні і використання вразливостей в пристроях і мобільних ОС.

Оскільки мобільні пристрої стають більш важливими, кіберзлочинці привертають до них додаткову увагу. В результаті кіберзагрози проти цих пристроїв стали різноманітнішими.

1. Шкідливі програми та веб-сайти

Як і настільні комп'ютери, мобільні пристрої мають програмне забезпечення та доступ до Інтернету. Мобільні шкідливі програми (тобто шкідливі програми) та

шкідливі веб-сайти можуть виконувати на мобільних телефонах ті самі завдання (крадіжка даних, шифрування даних тощо), що й на традиційних комп'ютерах.

Шкідливі програми бувають різних форм. Найбільш поширеними типами шкідливих мобільних програм є трояни, які також виконують шахрайство з рекламою та кліками.

2. Мобільні програми-вимагачі

Мобільні програми-вимагачі — це особливий тип мобільного шкідливого програмного забезпечення, але ширше використання мобільних пристроїв для бізнесу зробило його більш поширеним та небезпечним варіантом шкідливого програмного забезпечення. Мобільні програми-вимагачі шифрують файли на мобільному пристрої, а потім вимагають викуп за ключ дешифрування, щоб відновити доступ до зашифрованих даних.

3. Фішинг

Фішинг - один із найпоширеніших векторів атак. Більшість кібератак починаються з фішингового листа, що містить шкідливе посилання або вкладення, що містить зловмисне програмне забезпечення. На мобільних пристроях фішингові атаки використовують різноманітні засоби доставки своїх посилань та шкідливих програм, включаючи електронну пошту, обмін SMS-повідомленнями, платформи соціальних мереж та інші програми.

Насправді, хоча електронні листи — це те, про що люди найчастіше думають, коли чують про фішинг, вони навіть не відповідають найбільш поширеному вектору фішингу на мобільних пристроях. Фактично, на електронні листи припадає лише 15% мобільних фішингових атак, що ставить їх позаду обміну повідомленнями, соціальних мереж та «інших» додатків (не соціальних, обміну повідомленнями, ігор чи продуктивності).

4. Атаки «людина посередині» (MitM)

Атаки «людина посередині» (MitM) включають перехоплення мережових комунікацій зловмисником з метою підслуховування або зміни даних, що передаються. Хоча цей тип атаки може бути можливим у різних системах, мобільні пристрої особливо вразливі для MitM-атак. На відміну від веб-трафіку, який зазвичай використовує для зв'язку зашифрований HTTPS, SMS-повідомлення можна легко перехопити, а мобільні програми можуть використовувати незашифрований HTTP для передачі потенційно конфіденційної інформації.

Атаки MitM зазвичай вимагають, щоб співробітник був підключений до ненадійної або скомпрометованої мережі, такої як загальнодоступна мережа Wi-Fi або мережі. Однак у більшості організацій відсутні політики, що забороняють використання цих мереж, що робить такі атаки цілком можливими, якщо не використовуються такі рішення, як віртуальна приватна мережа (VPN).

5. Просунуті методи джейлбрейку та рутингу

Джейлбрейк та рутування – це умови для отримання адміністраторського доступу до мобільних пристроїв iOS та Android. Ці типи атак використовують уразливості у мобільних ОС для отримання root-доступу на цих пристроях. Ці розширені дозволи дозволяють зловмиснику отримати доступ до більшої кількості даних і завдати більшої шкоди, ніж з обмеженими дозволами, доступними за умовчанням. Багато мобільних користувачів роблять джейлбрейк/рутування своїх власних пристроїв, щоб мати можливість видаляти непотрібні програми за промовчанням або встановлювати програми з ненадійних магазинів додатків, що робить цю атаку ще простіше.

6. Експлойти пристроїв та ОС

Часто в центрі уваги кібербезпеки знаходиться програмне забезпечення верхнього рівня, але нижчі рівні стека програмного забезпечення можуть містити вразливості і атакувати. У разі мобільних пристроїв, таких як комп'ютери, зловмисник може використовувати вразливість у мобільній ОС або самому

пристрої. Часто ці експлойти завдають більшої шкоди, ніж експлойти вищого рівня, тому що вони існують нижче та поза видимістю рішень безпеки пристрою.

Висновок

Враховуючи великий та різноманітний ландшафт мобільних загроз, компаніям потрібні корпоративні рішення для забезпечення безпеки мобільних пристроїв. Це особливо вірно, оскільки перехід на віддалену роботу робить ці мобільні пристрої більш поширеним та важливим компонентом ІТ-інфраструктури організації.

Ефективне рішення для захисту від загроз для мобільних пристроїв повинно виявляти і реагувати на безліч різних атак, забезпечуючи при цьому позитивний досвід користувача. Для цього необхідно реалізувати такі керівні принципи:

- 360-градусний огляд безпеки пристрою, програм та мережі.
- Повна гнучкість та масштабованість
- Повна видимість рівня ризику мобільних працівників
- Дизайн захисту конфіденційності
- Оптимальний досвід користувача [5]

2 АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МОБІЛЬНИХ ПРИСТРОЇВ

2.1. Види загроз на мобільні пристрої

Найновіші смартфони створені для забезпечення широкого підключення до Інтернету та мережі через різні канали, такі як 3G або 4G, Wi-Fi, Bluetooth або дротове підключення до ПК. Загрози безпеці можуть виникати в різних місцях уздовж цих різноманітних шляхів, де можуть передаватися дані.

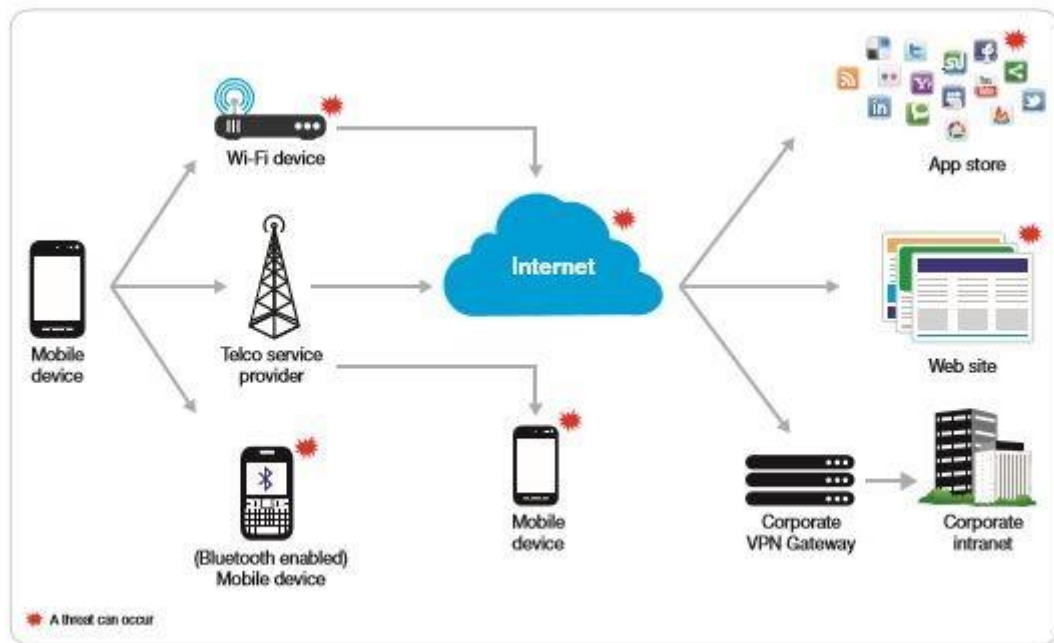


Рис.1 – Місця, в яких можуть бути джерелами загроз в мобільних пристроях

Коли пристрій завантажує нову мобільну програму з будь-якого інтернет-магазину програм, програмне забезпечення може містити зловмисне програмне забезпечення, яке може викрасти або пошкодити дані на пристрої, а в деяких випадках навіть вивести з ладу сам мобільний пристрій. Зараз більшість мобільних пристроїв мають підключення до Інтернету, тому поширені веб-загрози, які атакували ноутбуки чи настільні комп'ютери, також можуть стосуватися мобільних пристроїв. Пристрій, підключений через Wi-Fi або Bluetooth, піддається більшому ризику, оскільки джерело Wi-Fi або інший пристрій із підтримкою Bluetooth може бути скомпрометовано та може зіграти роль в атаці «людина посередині» (коли хакер налаштовує ноутбук, сервер або мобільний пристрій для прослуховування або зміни законних комунікацій) або інший тип атаки.

Через різноманітність доступних механізмів зв'язку та збільшення використання бізнес-додатків на мобільних пристроях загрози безпеці мобільних пристроїв еволюціонували до всіх загроз, застосовних до настільних комп'ютерів і ноутбуків, а також до нових загроз, справді унікальних для мобільних пристроїв. Таким чином, мобільні пристрої потрібно захищати ще ширшим набором методів

безпеки, ніж ті, які використовуються для традиційних операційних середовищ настільних ПК або ноутбуків.

Незалежно від того, які загрози, цілі, до яких хакери намагаються отримати доступ і використати їх, зазвичай складаються з одного або кількох із наведеного нижче:

- Облікові дані для доступу до бізнес-або особистих облікових записів
- Конфіденційна службова чи особиста інформація
- Послуги телефону або передачі даних
- Сам мобільний пристрій

Найпоширеніші загрози безпеці мобільних пристроїв:

- Втрата та крадіжка
- Зловмисне програмне забезпечення
- Спам
- Фішинг
- Bluetooth і Wi-Fi

Мобільні пристрої нікуди не зникають, а BYOD і «споживання ІТ» — це не мода. Ці тенденції кількісно покращують корпоративну гнучкість, але ризик безпеки є реальним.

Традиційні підходи безпеки блокують інфраструктуру, але це не мета для сучасних кіберзлочинців. Їм потрібні конфіденційні дані, які є цінними; легко монетизується; і все частіше в русі, в ІТ-інфраструктуру та поза нею. І вони чудово розуміють, де і коли знайти «відкриті дані», коли вони найбільш вразливі, і вони готові чекати.

Але чекати — це те, чого ви не можете собі дозволити. Впровадження орієнтованого на дані підходу до безпеки мобільних пристроїв із шифруванням

допомагає зберігати конфіденційні дані в безпеці, де б вони не були, незалежно від того, як вони використовуються та протягом усього життєвого циклу. Зрештою, це зменшує ризик витоку даних та інших загроз, тому мобільність може бути максимально використана. І хіба це не мета будь-якого заходу безпеки [6]?

2.2. Методи забезпечення безпеки мобільних пристроїв

До пандемії коронавірусу багато співробітників уже використовували смартфони та планшети для співпраці, доступу до інформації компанії та виконання більших завдань.

Але з нещодавнім переходом до віддаленої роботи мобільні пристрої стали абсолютно невід'ємною частиною робочого життя людей.

Сьогодні співробітники використовують свої персональні пристрої, щоб приєднуватися до викликів Zoom за кухонним столом або перевіряти електронну пошту під час чищення зубів.

Фактично, згідно з даними Syntonic, 87% підприємств покладаються на те, що їхні співробітники використовують їхні особисті мобільні пристрої для доступу до корпоративних програм.

Незалежно від того, чи шукаєте ви останню статистику щодо смартфонів і продуктивності чи безпеки BYOD, ми зібрали 40 статистичних даних щодо мобільних пристроїв на робочому місці, які допоможуть вам налаштувати мобільну стратегію вашої організації, покращити співпрацю та підтримати перехід до віддаленого використання працювати.

Статистика використання мобільних пристроїв

Сьогодні у світі більше людей мають мобільний телефон, ніж зубну щітку. Оскільки мобільні телефони стають невід'ємною частиною нашого повсякденного життя, розуміння того, як використовувати мобільні пристрої на робочому місці, є

ключовим для успіху вашої організації. Ці мобільні статистичні дані показують, наскільки повсюдними стали мобільні пристрої.

До кінця 2021 року до Інтернету буде підключено понад 27,1 мільярда пристроїв — це більше ніж 3 пристрої на кожну людину на планеті! [Cisco, 2021]

Станом на січень 2021 року 5,22 мільярда людей (66,6% населення світу) користуються мобільними пристроями. [Datareportal, 2021]

Станом на 2020 рік у світі налічувалося 3,5 мільярда користувачів смартфонів. Це на 6,7% більше, ніж у минулому році. [Newzoo, 2020]

Переважна більшість (97%) американців мають будь-який мобільний телефон, а 85% – смартфони. Крім того, 53% володіють планшетами. [Дослідницький центр Pew, 2021]

Мобільний пристрій перевершив настільний комп'ютер як основний спосіб доступу до Інтернету. [Comscore, 2018]

Сьогодні 15% дорослих американців є користувачами Інтернету «лише зі смартфонів», тобто вони не мають домашнього широкосмугового зв'язку, але мають смартфон. [Дослідницький центр Pew, 2021]

Дорослі американці витрачатимуть на смартфони в середньому 3 години 12 хвилин на день, що на 6 хвилин більше за рік. [eMarketer, 2020]

Додатки займають 90% часу мобільного медіа. Інші 10% витрачаються на веб-сайти. [Smart Insights, 2020]

75% американців кажуть, що найчастіше використовують свої смартфони для перевірки електронної пошти. [Віжно, 2018]

Статистика мобільних пристроїв на роботі

Сучасні працівники на роботі значною мірою покладаються на мобільні пристрої. Насправді важко уявити робоче життя без ноутбуків, смартфонів і

планшетів. Ця статистика проливає світло на те, як працівники зараз використовують свої мобільні пристрої на робочому місці.

70% співробітників тримають свої телефони «в зоровому контакті» на роботі. [Будівельник кар'єри, 2016]

91% корпоративних співробітників використовують принаймні один мобільний додаток. [Апперян, 2016]

Середній мобільний працівник працює на 240 годин на рік довше, ніж населення в цілому. [iPass, 2017]

84% мобільних працівників перевіряли свій смартфон у ліжку, тоді як 72% зізналися, що перевіряли свій смартфон в туалеті. [iPass, 2017]

Більше половини мобільних працівників стверджують, що відсутність Wi-Fi під час віддаленої роботи негативно вплине на їхню здатність виконувати свою роботу певною мірою. [iPass, 2017]

Статистика продуктивності мобільного підприємства

Із зростанням кількості мобільних пристроїв на роботі навколо смартфонів і продуктивності точиться багато дискусій. Ці статистичні дані продуктивності мобільного підприємства пропонують уявлення про продуктивність, коли роботодавці дають робочі телефони або дозволяють працівникам використовувати власні пристрої.

75% людей кажуть, що їхні смартфони роблять їх більш продуктивними. [Google, 2017]

Для 97% користувачів додатки для продуктивності є найбільш домінуючим типом програм на їхніх смартфонах. [GoodFirms, 2019]

Серед IT-керівників 82% сказали, що смартфони дуже важливі для продуктивності співробітників. [Samsung/Oxford Economics, 2018]

88% високозалучених працівників контролюють своє робоче місце. BYOD забезпечує частковий контроль. [Стілкейс, 2016]

64% лідерів кажуть, що інвестиції в технології привели до підвищення продуктивності. [Швидкість, 2020]

Близько половини (53%) керівників сказали, що програми покращують бізнес-процеси та підвищують продуктивність. [Апперян, 2016]

Статистика BYOD і мобільних додатків

Враховуючи потенціал мобільних пристроїв для підвищення продуктивності, не дивно, що все більше компаній заохочують працівників використовувати свої пристрої на роботі та пропонують їм бізнес-додатки. Ці статистичні дані дають уявлення про тенденції BYOD і впровадження мобільних додатків на робочому місці.

Лише 26% представлених американських компаній забезпечують своїх співробітників мобільними телефонами — це найменший показник для будь-якої країни. [Стілкейс, 2016]

87% компаній очікують, що їхні працівники використовуватимуть їхні особисті пристрої для роботи, і 77% цих компаній очікують, що ця кількість зросте протягом року. [Синтонік, 2016]

72% компаній мають політику «приносити свій власний пристрій» (BYOD) і дозволяють співробітникам приносити власні пристрої на роботу [7].

Умови 21 століття передбачають часте використання інформаційних технологій і гаджетів. І одним із найпоширеніших, щоденних супутників кожної людини є мобільний телефон. Однак із зростанням використання інтелектуальних пристроїв зростає ризик витоку та втрати даних. Тому кожен користувач повинен подбати про відповідний рівень безпеки (кібербезпеки) цифрових пристроїв. Рівнів безпеки смартфона існує два основних рівні захисту смартфона:

– фізичний захист. Включає основні правила догляду за мобільним телефоном. Наприклад, не можна залишати його без нагляду, вводити код доступу на очах у інших людей або банально носити смартфон у задній кишені. Адже хтось може «зламати» ваш пристрій і використовувати його в своїх інтересах, наприклад, очистити підключені до смартфона акаунти, отримати потрібні дані або видалити потрібну вам інформацію. У гіршому випадку телефон вкрадуть.

– захист «начинки» - операційної системи, програм та інших додатків. Існує безліч способів захисту смартфона на «внутрішньому» рівні. Найважливіші з них, без сумніву, це своєчасне оновлення операційної системи, використання багатофакторної аутентифікації та складних паролів.

Як захистити свій смартфон? Основні правила кібербезпеки

1. Своєчасне оновлення операційної системи пристрою. Виробники смартфонів постійно оновлюють програмне забезпечення. Такі оновлення часто усувають усі виявлені вразливості операційних систем, запобігають витоку даних користувача, блокують несанкціонований доступ тощо. 90% оновлень усіх операційних систем включають покращення заходів безпеки, тому що компанії постійно моніторять і знаходять все більше вразливостей у своїх власних ОС. Тому в оновленнях системи все частіше безпека виходить на перший план. Крім того, деякі компанії приділяють особливу увагу питанню захисту смартфона. Наприклад, Samsung випустила сервіс Knox, який виводить безпеку смартфонів Samsung на принципово новий рівень захисту даних. Це мобільна платформа безпеки, розроблена для компаній із передовою системою корпоративної мобільності. Knox пропонує: – дистанційне налаштування великої кількості пристроїв Samsung та їх адаптацію до конкретних потреб; – одночасне додавання тисяч пристроїв до ЕММ без необхідності ручної реєстрації кожного пристрою; – просте керування багатьма пристроями за допомогою хмарного рішення ЕММ; – застосування комплексу функцій захисту та управління для корпоративних пристроїв; – керуйте версіями ОС на мобільних пристроях Samsung для максимальної економічності.

2. Використання складних паролів і менеджерів паролів. Перш за все, ви не повинні використовувати однакові паролі для різних служб. Це те саме, що мати один ключ від машини, будинку та сейфа. Якщо пароль вгаданий або вгаданий, це вплине на всі служби, де використовувалася ця комбінація символів. Рекомендується вибирати дійсно складні паролі, які складаються з комбінації різних символів і цифр. Адже дівоче прізвище мами або ім'я домашнього улюбленця можна дізнатися дуже швидко. Крім того, для таких дій використовується аналіз вашого профілю в соціальних мережах (соціальна інженерія). Тому намагайтеся не використовувати стандартні типи запитань, які пропонує сервіс, а будьте оригінальні. Вибирайте паролі з 8 символів, також вони повинні містити літери (великі та малі), спеціальні символи та цифри. Крім того, ми рекомендуємо використовувати менеджер паролів. Це спеціальні сервіси та програми, які зберігають логіни та паролі в зашифрованому вигляді. Адже запам'ятати всі складні паролі практично неможливо. Доступ до таких менеджерів паролів часто має максимальний рівень захисту за допомогою паролів, SMS-кодів і відбитків пальців, повністю відповідаючи правилам багатофакторної аутентифікації.

3. Використання багатофакторної аутентифікації. Використовуйте двофакторну (або багатофакторну) автентифікацію, де це можливо. Двофакторна аутентифікація означає захист за допомогою 2 паролів з різними каналами доступу. Наприклад, отримання захисного коду через SMS на смартфон після введення логіна та пароля. У цьому випадку, навіть якщо хтось дізнається ваш логін і пароль, він все одно не отримає доступу до смартфона і не зможе отримати SMS-код, тому не зайде в профіль. Іноді замість смс-повідомлень для доступу використовуються месенджери (Viber, Telegram тощо). Крім того, експерти з кібербезпеки радять захистити особистий мобільний номер, прив'язавши його до даних мобільного оператора.

4. Використання біометричного захисту. Рекомендується використовувати додатковий захист - за допомогою відбитка пальця або сканування особи (faceID

для IOS). Щоб заблокувати доступ до телефону, необов'язково використовувати паролі та пін-коди, вони не завжди можуть забезпечити належний захист даних. Набагато безпечніше використовувати біометричну ідентифікацію. Це досить надійний і зручний інструмент. Крім того, сьогодні практично всі смартфони надають таку можливість.

5. Встановлення додатків лише з офіційних джерел. Не дивіться завантажувати та встановлювати програми для смартфонів із невідомих джерел. Часто самі операційні системи, встановлені в смартфонах, не можуть (або попереджають про небезпеку) інсталиувати такий софт. ОС об'єднує користувача тільки своїми додатками з офіційного магазину – App Store, Google Play, Galaxy Store, AppGallery та ін. Безпечним є також скачування додатків з офіційних сайтів виробника. Часто, встановлюючи добавки з інших джерел (наприклад, піратські версії платних програм), ви встановлюєте і віруси чи інші шкідливі дані. Особливо проблемним це є для смартфонів на ОС Android. Проте, навіть завантажуючи застосунок з офіційного магазину, слід перевірити всі доступні дані, як відомості про розробників, доступи, які потрібні додатку при встановленні, відгуки користувачів.

6. Користування лише відомими, безпечними мережами Wi-Fi. Відкриті, загальнодоступні мережі Wi-Fi небезпечні для використання, оскільки через них можна отримати доступ до смартфона чи інших гаджетів. Часто зловмисники створюють точки доступу з назвами, ідентичними до тих, які пропонують заклади. Таким чином шахраї можуть отримати доступ до електронної пошти, акаунтів у соціальних мережах, персональних даних і навіть банківських карток. Також, при підключенні до такої мережі, ви можете попросити перейти за посиланням чи натиснути якусь кнопку, це може бути ознакою шахрайства. Рекомендуємо користуватися мобільними даними в загальнодоступних місцях або, принаймні, користуватися VPN.

7. Встановлення додаткового захисту. В якості додаткового захисту варто використовувати антивірусне програмне забезпечення. зазвичай воно вже встановлене у смартфоні. Проте не варто встановлювати відразу кілька таких застосунків, оскільки вони починають ворогувати між собою, що

приведе до проблеми в роботі пристрою. Також дивіться вмикати всі доступні “захисти”, які пропонують операційну систему та використання смартфона, наприклад, у розділі “Конфіденційність”. Варто зберегти дані в безпечній хмарі, ізольований від залишків системи; вона забезпечує додатковий захист даних навіть у разі злому чи втрати смартфона. 8. Постійне увімкнення геолокації. Не варто відключати геолокацію, хоча часті користувачі бажають її приховати. Адже з допомогою додаткових сервісів у будь-який момент можна побачити телефон, навіть якщо він був викрадений або загублений. Наприклад, Google розробила для таких помилок сервіс Find My Phone для Android. Він не дозволяє тільки активувати дзвінок (навіть, якщо цей гаджет був розміщений у беззвучному режимі), але й заблокувати пристрій і видалити всі дані даних на ньому. Іншими словами, власник телефона може самостійно контролювати його навіть на відстані. Єдине, що для цього потрібно – підключення до інтернету. Отже, способів захистити смартфон існує чимало. Варто слідкувати за ними та не залишати гаджет без погляду. Тоді використання додаткових пристроїв приносить лише позитивні враження [8].

2.3. Рішення для захисту мобільних пристроїв

У наш час більшість людей витрачають значну частину часу на перегляд веб-сторінок за допомогою настільних комп’ютерів, ноутбуків, планшетів, смартфонів та інших підключених пристроїв. Але хоча життя без Інтернету здається неможливим через його численні можливості та переваги, це не завжди безпечно чи приємне середовище.

Протягом останніх кількох років у мережі зросла кількість ризиків, таких як фішинг, віруси, зловмисне програмне забезпечення, програми-вимагачі, шпигунські програми, веб-відстеження, крадіжка особистих даних, витоки даних, хакерство тощо.

Незважаючи на те, що технологічні компанії постійно вдосконалюють безпеку пристроїв, кіберзлочинці продовжують розробляти нові види зловмисного програмного забезпечення та методи злому набагато швидше. Отже, не можна просто покладатися на вбудовані механізми безпеки пристроїв.

Найефективніший спосіб захистити себе від зростаючих ризиків кібербезпеки – це встановити на свій пристрій антивірусне рішення. Ці програми можуть постійно сканувати пристрої на наявність вірусів або зловмисного програмного забезпечення, виявляти загрози безпеці в режимі реального часу, видаляти їх із вашого пристрою та, зрештою, запобігати проблемам кібербезпеки.

Отже, на що слід звернути увагу в антивірусному рішенні? Найкращі антивірусні програми не тільки пропонують захист від усіх типів вірусів і зловмисного програмного забезпечення, але й надають додаткові функції, такі як вбудовані віртуальні приватні мережі (VPN), менеджери паролів, сканування темної мережі, батьківський контроль, інструменти оптимізації продуктивності, безпечні браузері, багатоплатформна підтримка та багато іншого.

Однак, маючи на увазі, що сьогодні на ринку доступна велика кількість різних антивірусних продуктів, варто замислитись, який постачальник найкраще відповідатиме пристрою, бюджету та потребам користувача.

17 березня 2022 року німецьке агентство з кібербезпеки BSI попередило, що користувачі антивірусного програмного забезпечення, створеного російською фірмою «Лабораторія Касперського», можуть опинитися під загрозою злому. BSI заявив, що «рекомендує замінити програми з портфолію антивірусного програмного забезпечення Kaspersky альтернативними продуктами».

Найкращі антивірусні програми на 2022 рік:

- Найкраще загалом – Norton 360 premium: £39,99, Norton.com
- Найкраще для Mac – повний захист McAfee: від £39,99, McAfee.com

- Найкраще для мобільних пристроїв – мобільний захист McAfee: безкоштовно, [Mcafeemobilesecurity.com](https://mcafeemobilesecurity.com)
- Найкраще безкоштовне антивірусне програмне забезпечення – Avira free security: безкоштовно, Avira.com
- Найкраще для зручності використання – Sophos Home: £37,46, Home.sophos.com
- Найкраще для батьківського контролю – F-Secure Total: від £39,99, F-secure.com
- Найкраще для ігрового ПК – преміальний захист BullGuard: £69,99, Bullguard.com

Norton 360 premium: £36,99, Norton.com

- Операційна система: Windows, Mac, Android, iOS
- Максимальна кількість охоплених пристроїв: 10
- Особливості, що виділяються: Менеджер паролів, VPN, відстежує темну мережу на предмет витоку інформації
- Програмне забезпечення для резервного копіювання: хмарне сховище до 75 ГБ
- Брандмауер: так

Norton 360 Premium ідеально підходить для тих, хто хоче захистити всі свої підключені технології. Він пропонує антивірусний захист до 10 різних пристроїв, включаючи комп'ютери, смартфони та планшетні ПК, за однією підпискою.

Використовуючи технології штучного інтелекту та машинного навчання, Norton 360 може виявляти та зменшувати поширені ризики кібербезпеки, такі як віруси, шпигунське програмне забезпечення, програми-вимагачі та інші форми зловмисного програмного забезпечення.

Але на цьому його можливості не закінчуються. Norton 360 також надає інструмент хмарного резервного копіювання для захисту файлів, що зберігаються

на вашому комп'ютері, брандмауер, який ідентифікує та блокує зловмисний веб-трафік, менеджер паролів для створення надійних паролів і їх безпечного зберігання, батьківський контроль, вбудований VPN, захист веб-камери, сервіс темного веб-моніторингу, який попередить вас, якщо ваші особисті дані були порушені, тощо.

Окрім великого набору функцій, Norton 360 простий у встановленні, налаштуванні та використанні. При відкритті програми, можна побачити домашню сторінку, яка пропонує доступ до основних функцій, таких як безпека пристрою, моніторинг темної мережі, безпечна VPN, резервне копіювання в хмарі, менеджер паролів і батьківський контроль.

Повний захист McAfee: від £39,99, [Mcafee.com](https://www.mcafee.com)

Найкраще: для Mac

- Операційна система: Windows, Mac, Android, iOS
- Максимальна кількість охоплених пристроїв: 10
- Особливості, що виділяються: інструменти оптимізації ПК, шредер чутливих файлів
- Програмне забезпечення для резервного копіювання: зашифроване сховище файлів до 2 ГБ
- Брандмауер: так

McAfee total protection — це антивірусне рішення преміум-класу, яке захищає від вірусів, програм-вимагачів та багатьох інших ризиків безпеки в Інтернеті. Однією з найкращих переваг цього програмного забезпечення є те, що воно працює на пристроях Windows, Mac, iOS і Android, тож ви можете захистити майже кожен електронний продукт у домі.

Окрім багатоплатформного антивірусу, ця програма також має функцію веб-захисту, яка попереджатиме про підозрілі веб-сайти, посилання та файли під час перегляду Інтернету. Як і багато інших антивірусних рішень, він також має

вбудований VPN, який використовує 256-бітне шифрування для захисту онлайн-даних користувача.

З точки зору інших функцій, McAfee Total Protection пропонує інструменти оптимізації ПК, безпеку домашньої мережі, батьківський контроль, менеджер паролів, сканер уразливостей, який перевіряє наявність оновлень програмного забезпечення, зашифроване сховище файлів, конфіденційний файл-шредер, фільтр спаму для Microsoft Office, і більше.

Додаток простий у встановленні та використанні, пропонує зрозумілу та просту панель навігації у верхній частині сторінки. На домашній сторінці можна додавати пристрої, виконувати сканування, перевіряти наявність оновлень, отримати доступ до довідки тощо. Є доступні окремі пакети, пакети для кількох пристроїв і сімейні пакети.

McAfee mobile security: безкоштовно, [Mcafeemobilesecurity.com](https://mcafeemobilesecurity.com)

Найкраще: для мобільних пристроїв

- Операційна система: Android, iOS
- Максимальна кількість охоплених пристроїв: один
- Відмінні функції: Mobile VPN, інструменти відновлення втраченого пристрою
 - Програмне забезпечення для резервного копіювання: резервне копіювання носіїв, до 2 Гб
 - Брандмауер: так

Це відмінний варіант, якщо ви хочете захистити свій смартфон, а не комп'ютер. Він пропонує кілька чудових безкоштовних функцій, зокрема сканер безпеки системи, який виявляє незахищені точки доступу Wi-Fi, атаки Wi-Fi та застаріле програмне забезпечення.

Існує спеціальний сканер безпеки Wi-Fi, який скануватиме інтернет-мережу на наявність загроз безпеці та видасть попередження, якщо користувач підключився до незахищеного з'єднання Wi-Fi. Завдяки вбудованому мультимедійному сховищу можна безпечно зберігати фотографії та отримувати до них доступ за допомогою Touch ID або Face ID.

Безкоштовна версія мобільного захисту McAfee також має захист від крадіжок, який включає такі функції, як GPS-трекер, який допоможе знайти втрачений або викрадений телефон, дистанційне видалення даних і можливість резервного копіювання контактів у хмарі. Також можна перейти на преміум-акаунт, якщо є бажання отримати доступ до служби VPN і додаткового веб-захисту.

Додаток доступний для завантаження як на Android, так і на iOS. Під час тестування програми для iOS було виявлено, що вона проста у використанні. Щойно ви відкриєте програму, ви побачите велику кнопку, за допомогою якої можна запустити перевірку безпеки. Під нею розташовані зручні кнопки для доступу до таких функцій, як безпечний Інтернет, захист Wi-Fi, медіа-сховище та резервне копіювання контактів.

Avira: безкоштовно, Avira.com

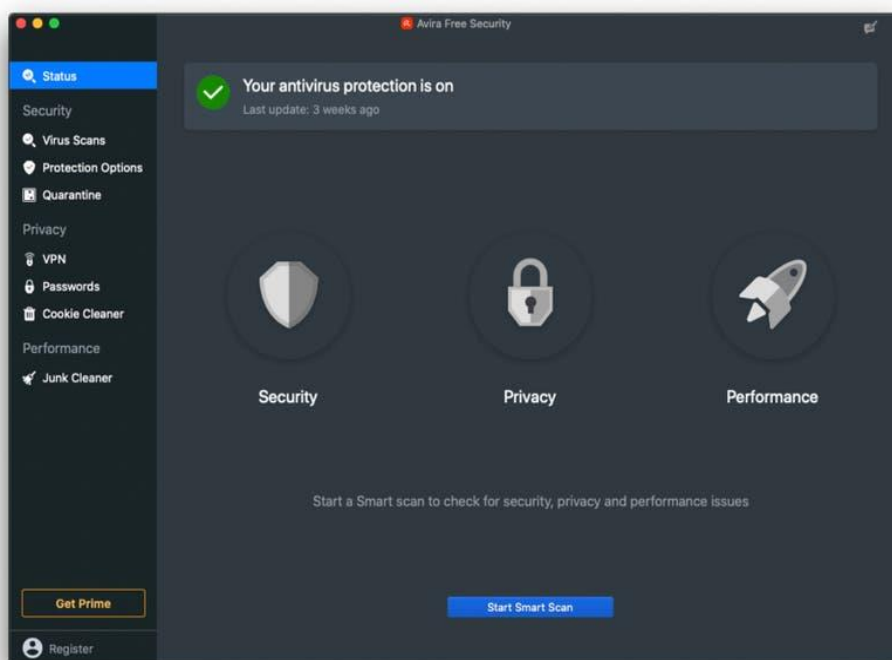


Рис.2 – інтерфейс Avira

Найкраще: безкоштовне антивірусне програмне забезпечення

- Операційна система: Windows, Mac, Android, iOS
- Максимальна кількість охоплених пристроїв: один з безкоштовною версією, п'ять з преміум-версією
- Відмінні функції: безкоштовний VPN до 500 Мб
- Програмне забезпечення для резервного копіювання: Ні
- Брандмауер: Ні

Якщо ви не хочете витратити гроші на антивірусне рішення преміум-класу, варто ознайомитися з пропозицією Avira. Доступний для комп'ютерів Windows і Mac, а також для всіх платформ, від iOS до Android, він пропонує захист у

реальному часі від ряду онлайн-загроз. До них належать шпигунське програмне забезпечення, програми -вимагачі та інші типи шкідливих програм.

Також є вбудований антивірусний сканер, який дозволяє виконувати швидке або повне сканування, планувати сканування та налаштовувати сканування. Ще одна чудова безкоштовна функція — це віртуальна приватна мережа, яка шифрує веб-трафік, хоча існує мізерне обмеження в 500 Мб даних на місяць.

Також є базовий менеджер паролів, очищувач сміття для збереження пам'яті на комп'ютері та темний і світлий режими. Додаток для комп'ютера простий у використанні та навігації загалом, із чітким викладом результатів конфіденційності, безпеки та продуктивності, які відображаються на сторінці «статус».

Sophos Home: £37,46, [Home.sophos.com](https://home.sophos.com)

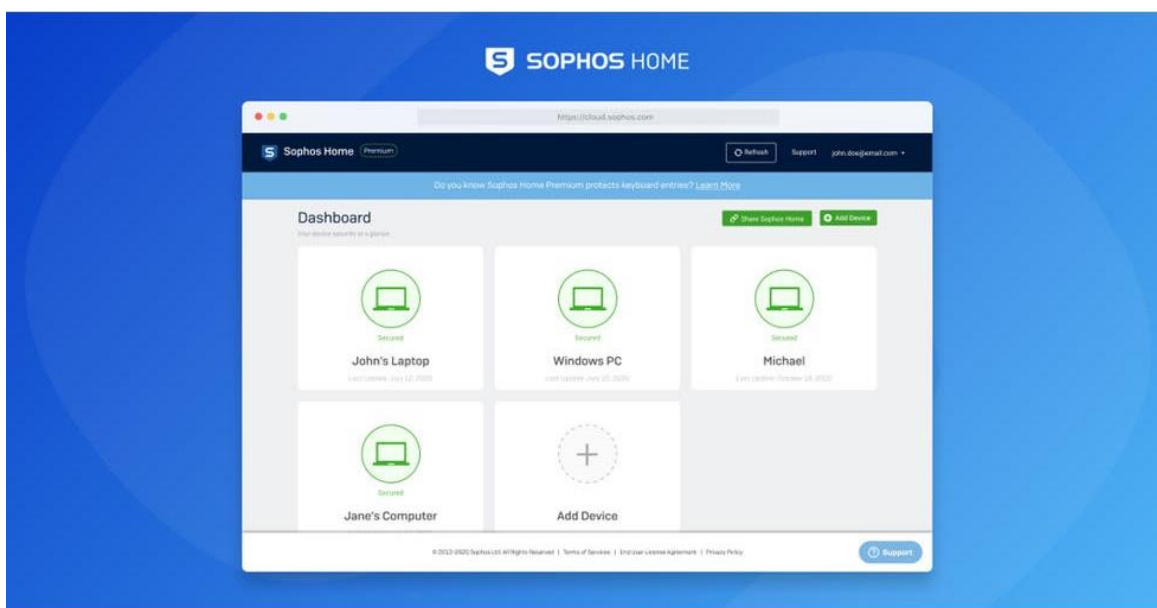


Рис.3 – інтерфейс Sophos Home

- Операційна система: Windows, Mac, Android, iOS
- Максимальна кількість охоплених пристроїв: 10
- Особливості, що виділяються: захист конфіденційності веб-камери
- Програмне забезпечення для резервного копіювання: Ні

- Брандмауер: так

Це рішення забезпечує безпеку та захист конфіденційності для широкого спектру підключених пристроїв, включаючи ПК з Windows, комп'ютери Mac, iPhone, iPad та пристрої Android.

Він надає різноманітні можливості та функції, включаючи антивірус у режимі реального часу, сканування та очищення шкідливих програм, виявлення загроз на основі штучного інтелекту, захист від програм-вимагачів, захист конфіденційності в Інтернеті, веб-захист, батьківські веб-фільтри, преміальну підтримку та багато іншого. Однак функції можуть відрізнятися залежно від операційної системи, яку ви використовуєте.

Однією з речей, які подобаються в Sophos Home, є його проста у використанні та багатофункціональна онлайн-панель. Це дозволяє вам керувати різними пристроями, підключеними до облікового запису, додавати нові пристрої до облікового запису, виконувати сканування безпеки, змінювати налаштування, отримувати доступ до служби підтримки, переглядати інформацію про статус і багато іншого.

Якщо ви плануєте придбати Sophos Home, у вас є вибір із однорічного, дворічного та трирічного планів. Але варто зазначити, що також є безкоштовна пробна версія та 30-денна гарантія повернення грошей, що дозволить спробувати, перш ніж купувати.

F-Secure Total: від £39,99, F-secure.com

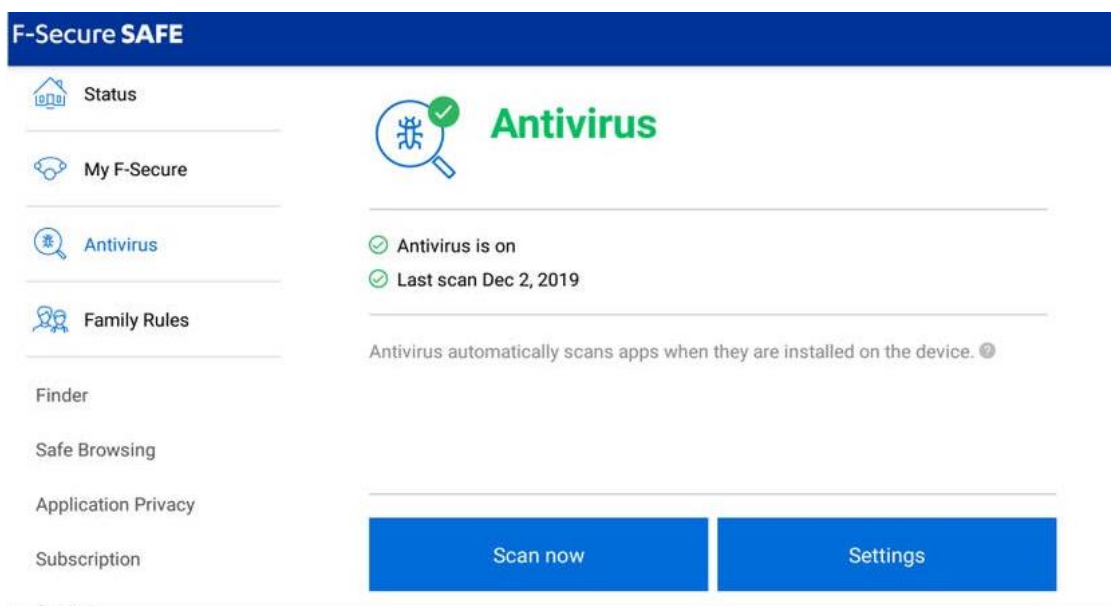


Рис.4 – рішення F-Secure Total

Найкраще: для батьківського контролю

- Операційна система: Windows, Mac, Android, iOS
- Максимальна кількість охоплених пристроїв: один, три або п'ять залежно від вашого підпорядкованого
- Відмінні функції: банківський захист, необмежений VPN
- Програмне забезпечення для резервного копіювання: Ні
- Брандмауер: так

Це комплексний пакет кібербезпеки, який працює на пристроях Windows, Mac, Android та iOS. Його антивірусна технологія була розроблена для захисту від вірусів, троянів, рекламних програм-вимагачів, клавіатурних шпигунів та інших форм шкідливого програмного забезпечення.

Інші основні функції включають захист веб-перегляду, захист від програм-вимагачів, захист банківських операцій, захист Wi-Fi, захист веб-відстеження, батьківський контроль, пошук вашого телефону, вбудований VPN, перемикач, менеджер паролів, автоматичне заповнення імен користувачів в Інтернеті і паролі,

онлайн-моніторинг ідентифікаційних даних, сповіщення про порушення безпеки, безкоштовна підтримка клієнтів тощо.

Під час реєстрації в обліковому записі F-Secure Total ви отримаєте доступ до трьох різних продуктів: F-Secure safe (антивірус), F-Secure Freedom (VPN) і F-Secure ID Protection (менеджер паролів).). Що чудово в цих програмах, так це те, що їх усі легко встановити та налаштувати.

Особливо подобається простота F-secure Safe, яка має корисні вкладки для антивірусу, сімейних правил, інструментів і мого F-Secure. При відкритті F-Secure Safe, ви побачите велику синю кнопку для проведення антивірусної перевірки. Інші програми також пропонують простий для навігації інтерфейс користувача.

Якщо подобається F-Secure Total, є підписки на один, три та п'ять пристроїв. Кожен план має 30-денну гарантію повернення грошей і підтримку клієнтів. Існує також місячна безкоштовна пробна версія, і не потрібно надавати дані кредитної картки для цього, що також є хорошою перевагою.

Преміальний захист BullGuard: £69,99, Bullguard.com

Найкраще: для ігрового ПК

- Операційна система: Windows, Mac, Android, iOS
- Максимальна кількість охоплених пристроїв: 10 пристроїв
- Особливості, що виділяються: Ігровий режим, сканує темну мережу в пошуках ваших деталей
- Програмне забезпечення для резервного копіювання: Так, хмарне резервне копіювання до 5 ГБ
- Брандмауер: так

Преміум-захист BullGuard — це вдосконалене рішення для кібербезпеки, яке використовує найсучаснішу технологію машинного навчання для виявлення та пом'якшення загроз кібербезпеці в режимі реального часу.

Він сумісний із пристроями Windows, Mac і Android, його можна використовувати на десяти пристроях і захищає від усіх форм шкідливого програмного забезпечення. Він також має функцію захисту ідентифікаційної інформації, яка сканує темну мережу, щоб захистити кредитні картки та банківські рахунки.

Тим часом сканер домашньої мережі BullGuard виконує цілодобовий моніторинг мережі Wi-Fi і сканує безпеку кожного пристрою, який використовує ваше підключення до Інтернету. Якщо ви завзятий гравець, вам сподобається Game Booster, оскільки він гарантує, що інциденти з кібербезпекою ніколи не завадять ігровому досвіду. Інші функції включають безпечний перегляд, багаторівневий брандмауер, сканування вразливостей, батьківський контроль тощо.

Під час тестування версії BullGuard Premium Protection для Mac було виявлено, що її легко встановити, налаштувати та використовувати. Під час процесу налаштування BullGuard надає корисний ролик, який показує зміни, які потрібно внести в налаштування Mac. Додаток Mac простий у використанні: зелена галочка вказує на те, що система безпечна, кнопка повного сканування, перемикач захисту в режимі реального часу та панель карантину [10].

Висновок

Чи справді потрібен антивірус у 2022 році?

Ну і так, і ні. Операційна система набагато краще захищає від вірусів і шкідливих програм, ніж раніше. Windows має ефективний вбудований захист від вірусів, який тихо працює у фоновому режимі, оновлюється автоматично, не сповільнює роботу комп'ютера та не вимагає будь-якої конфігурації. Введіть «безпеку» на панелі завдань, щоб відкрити меню Windows Defender і переглянути повний звіт про стан ПК, останні перевірки на віруси та будь-які дії, які вам можуть знадобитися.

Mac традиційно менш схильні до вірусів. Частково це пов'язано з хорошим антивірусним захистом – у новіших комп'ютерах Mac і MacBook вбудовано захист

безпосередньо в ЦП, щоб запобігти будь-яким вторгненням – але також і через той простий факт, що ПК популярніші, і тому розробники вірусів частіше стають мішенню для них. Для додаткового захисту від нових вірусів та інших типів атак антивірусне програмне забезпечення може надати вашій машині додатковий рівень захисту.

Антивірусне програмне забезпечення виявляє шкідливі додатки та програми та вимикає їх, перш ніж вони можуть зашкодити вашому пристрою. У найпростішому вигляді антивірусні інструменти виявляють загрози, порівнюючи код, запущений на вашій машині, з величезною базою даних відомих вірусів. Якщо виявить щось підозріле, антивірусне програмне забезпечення зупинить код і помістить на карантин будь-яку відповідальну програму.

Більшість антивірусного програмного забезпечення фактично містить багато різних інструментів, що працюють разом: моніторинг веб-трафіку, виявлення хитрих посилань на веб-сторінках і сканування завантажених файлів і вкладень.

Як вибрати найкращий антивірус?

Є так багато антивірусних інструментів, між якими можна вибрати, що може бути важко визначити, які з них ефективні, а які вигідні за ціною. Різне антивірусне програмне забезпечення може відповідати різним потребам, тому подумайте, для чого вам потрібне антивірусне програмне забезпечення. Чи дбаєте ви про безпеку своїх дітей, коли вони онлайн? У вас є більше одного пристрою, який потрібно захистити? Ви встановлюєте антивірус для людини, яка не володіє комп'ютерною грамотністю?

Багато антивірусних засобів розроблено таким чином, щоб бути ненав'язливими та простими у використанні навіть для менш досвідчених користувачів комп'ютера. Інші орієнтовані на сім'ю та розроблені, щоб зробити Інтернет безпечнішим місцем для молоді. Деякі призначені для мобільних пристроїв. Перегляньте наш список вище, щоб дізнатися, яке антивірусне програмне забезпечення найкраще відповідає вашим потребам.

Як змінити свій антивірус?

Багато видалити попереднє антивірусне програмне забезпечення перед переходом на нове. Це пояснюється тим, що конкуруючі антивірусні інструменти іноді можуть помилково ідентифікувати один одного як потенційну загрозу, створюючи безладні проблеми, коли кожен намагається ізолювати частини іншого.

Поки ви встановлюєте нове антивірусне програмне забезпечення відразу після видалення старого, ваш ПК має бути в безпеці. Ваше вихідне антивірусне програмне забезпечення може спробувати налякати вас, щоб ви залишилися клієнтом, страшними попередженнями про небезпеку, якщо залишити свій пристрій незахищеним навіть на секунду, але немає скарбів вірусів, які постійно намагаються проникнути на ваш ПК. Ваш ПК витримає деякий час між встановленнями антивірусу.

Чи достатньо безкоштовного антивіруса?

Для досвідчених користувачів, так. Якщо ви орієнтуєтесь в Інтернеті та можете відрізнити підроблену кнопку «завантажити» від справжньої, безкоштовного антивірусного інструменту достатньо, щоб захистити вас від більшості загроз.

Але для тих, кому потрібен більш надійний захист або для цілого бізнесу, інвестування в антивірусний інструмент преміум-класу з підтримкою кількох пристроїв може допомогти вам керувати компанією, не турбуючись про втрату даних або зловмисне програмне забезпечення.

Вердикт: антивірусне програмне забезпечення

Для більшості людей Norton 360 преміум буде найкращим загальним антивірусним рішенням, оскільки він пропонує надійний захист від ряду онлайн-загроз на додаток до брандмауера, вбудованої VPN, менеджера паролів, захисту веб-камери, моніторингу темної мережі, мульти- підтримка платформи та багато

інших корисних функцій. Крім того, зараз ви можете придбати ліцензію на десять пристроїв за вигідною ціною £44,99.

Але якщо ви не хочете витратити гроші на антивірусне рішення преміум-класу, вам обов'язково варто розглянути безкоштовну безпеку Avira , оскільки вона пропонує широкий захист для пристроїв Windows і Mac. І якщо вам потрібен хороший антивірусний додаток для вашого смартфона, шукайте мобільний захист McAfee [11].

3 ТЕХНОЛОГІЯ ЗАХИСТУ МОБІЛЬНИХ ПРИСТРОЇВ

3.1. Аналіз функцій та можливостей McAfee Mobile Security

McAfee Mobile Security — це пакет засобів безпеки, який допомагає кінцевим користувачам керувати безпекою своїх мобільних пристроїв. Він використовується в усій організації. Його основне використання – це безпека та захист даних. Він також використовується для вторинних утиліт, таких як стирання даних, оптимізація батареї та виявлення шкідливих програм.

Плюси і мінуси

Програма добре справляється з можливостями сканування на віруси та шкідливі програми. Він також має унікальну функцію захисту від крадіжок, яка може допомогти захистити мобільні пристрої. Програма пропонує кілька ролей конфіденційності, що дозволяє спільно використовувати різні рівні доступу до програм. Програма може потребувати деяких удосконалень у процесі налаштування та встановлення. Іншою областю, яка потребує вдосконалення, може бути інтерактивний інтерфейс. Можливо, до програми можна додати навчальний посібник або посібник.

McAfee Mobile Security надає досить простий і недорогий засіб безпеки для базового та середнього рівня безпеки для мобільних пристроїв. Хоча він не ідеальний, він досить добре виконує свою основну роботу.

Від деяких кінцевих користувачів програма може «вимагати» навчання з її інтерфейсом і процесами встановлення. У програмі відсутні деякі з поширених можливостей захисту даних, які є в інших продуктах конкурентів. Результатом може бути потреба в додаткових програмах безпеки.

McAfee Mobile Security пропонує базові заходи безпеки для мобільних пристроїв без високої вартості чи тривалого навчання. Однак у ньому також можуть бути відсутні деякі необхідні функції, наприклад шифрування даних, яке використовується іншими продуктами. Хоча його інтерфейс не ідеальний, його легше освоїти, ніж більш надійні продукти на ринку.

Програма справді відмінно справляється з базовим захистом мобільних пристроїв від шкідливих програм і вірусів. Вона пропонує деякі унікальні функції, наприклад додаток для захисту від крадіжок, який може допомогти захистити мобільні пристрої від неавторизованого використання користувачами. Він добре працює, коли забезпечує базову безпеку для мобільних пристроїв у польових умовах або під час віддаленої роботи. Однак компаніям можуть знадобитися більш широкі або додаткові програми безпеки, щоб забезпечити належний захист [12].

Після того як було скасовано низку функцій, елегантніша та потужніша McAfee Mobile Security поєднує в собі сканування зловмисного програмного забезпечення, веб-захист зі скануванням темної мережі та недорогий доступ до VPN.

Плюси:

- + Простий оптимізований додаток
- + Топова версія включає VPN

+Загальний бал захисту

+Недорого

Мінуси:

- Немає порівняльних даних про ефективність шкідливих програм

-Деякі основні функції припинено з останньої версії

-Не вдається встановити призначення на VPN

Залежно від вашого погляду, McAfee або скоротила зайве, щоб створити простішу програму Mobile Security, яка може краще захистити користувачів, або видалила корисні функції, які є в інших.

У будь-якому випадку Mobile Security спрощує захист за допомогою програми, яка включає захист від зловмисного програмного забезпечення, функції конфіденційності та моніторинг ідентифікаційних даних. Хоча Secure VPN необмежений, він не дозволяє вибирати країни, що робить його непотрібним для перегляду гео заблокованого контенту. На жаль, McAfee не бере участь у тестуванні сторонніх зловмисних програм для своєї програми Mobile Security, що ускладнює порівняння ефективності.

Тим не менш, він коштує 60 доларів з VPN і конкурує з тарифним планом Malwarebytes Premium + Privacy за 100 доларів.

Огляд McAfee Mobile Security: витрати та що покривається

Як і багато інших конкурентів, McAfee Mobile Security не має безкоштовної версії, але можна випробувати повну програму на п'яти пристроях протягом 30 днів.

Існує дві версії McAfee Mobile Security, починаючи з базового плану за 30 доларів на рік (3 долари на місяць) за один пристрій із скануванням зловмисного програмного забезпечення, електронною поштою та базовим онлайн-моніторингом особистих даних. Наступний крок вперед, McAfee Total

Protection, додає VPN і може охоплювати до п'яти пристроїв за 60 доларів США на рік (6 доларів США на місяць).

Є дві міжплатформні підписки, які охоплюють Windows, Mac, Android та iOS. Обидва включають доступ до VPN, але план Plus коштує 110 доларів і охоплює до п'яти систем, тоді як план Premium за 130 доларів додає батьківський контроль і збільшує охоплення до 10 пристроїв. Однак лише п'ять можуть одночасно використовувати VPN.

Недостатньо? Передплата McAfee Ultimate починається з плану Premium і додає послуги захисту особистих даних і страхування та відновлення на 1 мільйон доларів. Коштує він 160 доларів, хоча захист ідентифікатора лише для однієї людини.

Програма Android працює з телефонами та планшетами з ОС Android версії 7 (Nougat) або новішої. Однак йому не вистачає сумісності з пристроями WearOS і Chromebook. Для iPhone та iPad програма Mobile Security потребує версії iOS 13 або новішої та загалом відповідає функціям програми Android. Через обмеження Apple він не може сканувати систему на наявність шкідливих програм. Програма iOS компенсує це додаванням сканування системи, щоб переконатися, що пристрій має останні оновлення.

Огляд McAfee Mobile Security: захист від шкідливих програм

Можливо, немає безкоштовної версії McAfee Mobile Security, але її легко випробувати протягом 30 днів; його можна завантажити на п'ять систем. McAfee націлена на особистий онлайн-захист для запобігання атакам, починаючи з локального сканування вірусів. Він може ідентифікувати та зупиняти широкий спектр експлойтів і спроб фішингу.

Сканер URL-адрес безпечного перегляду в додатку є основним і центральним для захисту. Він стежить за веб-сайтами, які, як відомо, розповсюджують зловмисне програмне забезпечення, і тими, які намагаються завантажити небажані програми.

На відміну від свого попереднього Web Advisor, безпечний перегляд тепер вбудовано в програму. Таким чином, на телефон нічого не потрібно завантажувати, а після ввімкнення його захист буде автоматичним незалежно від того, який браузер використовується. Подібно до Lookout, це робить його захист більш узгодженим і універсальним, ніж програми безпеки, які покладаються на надбудови браузера. У дорозі програма Wi-Fi Scan може допомогти, підключаючись лише до безпечних мереж; він замінює Safe Wi-Fi з попередніх версій.

Він аналізує доступні мережі та попереджає, коли вони не використовують шифрування; його можна налаштувати на постійне сканування, але не може захистити від атак типу "людина посередині". Однак він стежить за мережами, які піддаються атакам.

Огляд McAfee Mobile Security: виявлення шкідливих програм

Незважаючи на те, що продукти безпеки McAfee протягом багатьох років показали хороші результати в оцінках сторонніх розробників, компанія наразі не бере участі в опитуваннях виявлення зловмисного програмного забезпечення для свого додатка Android, проведених AV-Test і AV Comparatives.

Востаннє перевірка за допомогою AV-Test відбулася в грудні 2021 року, коли McAfee отримала вражаючі 100 відсотків як за новими, так і за поширеними загрозами. Сканування також було надзвичайно точним без помилкових спрацьовувань.

Останній запуск з AV Comparatives датується липнем 2019 року, коли програма McAfee набрала вражаючих 99,9 відсотка без помилкових спрацьовувань. Це поставило його в одну лігу з Avast і Bitdefender і значно випередила Google Play Protect.

З іншого боку, без порівняльних даних щодо ефективності здатність McAfee Mobile Security виловлювати та зупиняти шахрайські віруси залишається відкритим.

Огляд McAfee Mobile Security: функції та інструменти безпеки

Хоча McAfee може багато чого запропонувати, кілька основних функцій зникли після нашого останнього огляду. За словами компанії, це були елементи, які не були популярні серед користувачів або були охоплені Android. Загалом, це схоже на значний відступ, оскільки Mobile Security тепер не має блокування програм і гостьового режиму, а також утиліт Memory Booster і Storage Cleaner.

Елементи, яких користувачі, ймовірно, найбільше розчаровують, це засоби захисту від крадіжок, але функція «Знайти мій пристрій» Android є хорошою заміною.

Те, що він має, чітко зосереджено на трьох завданнях: безпека, захист особистих даних і конфіденційність. Хоча перевірку конфіденційності було вилучено з McAfee Mobile Security без заміни, компанія Secure VPN може покращити профіль безпеки в публічному доступі. Його можна ввімкнути завжди або лише для з'єднань Wi-Fi, але ви також можете ввімкнути його вручну. Коли VPN активна, на панелі стану Android відображається логотип ключа, а на головному екрані Mobile Security з'являється маленький значок.

Компанія посилює присутність своєї VPN і тепер має сервери в 50 країнах; 14 у США та 3 у Канаді. На жаль, це не дозволяє вибрати місце, де буде виникати потік комунікацій. Це робить його марним для трансляції гео заблокованого вмісту та зосереджує увагу на захисті зв'язку.

McAfee Mobile Security може постійно перевіряти онлайн-профіль за допомогою свого Dark Web Monitoring. Він шукає 60 різних особистих ідентифікаторів, як-от банківські рахунки та рахунки кредитних карток, адреси електронної пошти та ідентифікаційні номери. Якщо він виявить порушення, Dark Web Monitoring покаже вказівки щодо вирішення проблеми. План Ultimate доповнює це страхуванням на 1 мільйон доларів США для повернення вкрадених коштів і отримання нових документів.

Усе це об'єднується в рейтингу захисту програми. Помітно показано на головному екрані, оцінка враховує всі аспекти присутності в Інтернеті, які програма може відстежувати або контролювати.

Огляд McAfee Mobile Security: вплив на систему

Системі знадобилося 8,2 секунди, щоб переглянути 482 програми та 313 файлів, але лише після двох запусків. Перше сканування тривало 2 хвилини 19 секунд, було розглянуто 482 програми та 8048 файлів. Подібно до повільнішої програми Malwarebytes, програмне забезпечення з часом дізнається, що перевіряти, а що ігнорувати.

Під час сканування системи на наявність шахрайського коду продуктивність програми впала на скромні 1,7 відсотка, як і у Malwarebytes Premium + Privacy та в середині пакету. Він був легшим за Norton 360: Mobile Security, але важчим за Google Play Protect і Avast Mobile Security.

Огляд McAfee Mobile Security: налаштування та підтримка

Захист пристрою за допомогою програми McAfee Mobile Security розпочався із завантаження 53 Мб, яке розпочало процес автоматичного встановлення. Коли було прийнято ліцензійну угоду, програма перевірила систему на несумісність.

Є вибір між 30-денною пробною версією та оплатою продукту. Якщо ви використовуєте безкоштовні версії, будьте готові до пропозицій щодо оновлення. Якщо ні, McAfee приймає кредитні картки та PayPal. Від початку до фінішу, це зайняло 6 хвилин 40 секунд.

На додаток до телефонної підтримки та підтримки в чаті для вирішення проблем, McAfee має посилання з програми для пошуку в базі даних або безпосереднього зв'язку зі своїми технічними спеціалістами. Вони доступні 24/7 [13].

3.2. Рішення подібні на McAfee Mobile Security

Ніхто не хоче, щоб на їхніх телефонах стався інцидент із безпекою, але мало хто насправді вжив заходів, щоб захистити свої телефони від них. Навіть встановлення однієї програми безпеки може змінити безпечний пристрій і мінне поле безпеки. Однак як ви знаєте, які програми підходять саме вам? Ми перерахували п'ять найкращих мобільних програм безпеки для Android та iOS, перерахувавши їхні ключові функції та тип безпеки, який вони забезпечують.

Avast Premium Security

Avast Premium Security пропонує користувачам повний онлайн-захист комп'ютерів, телефонів і планшетів. Сервіс надає спеціальні функції безпеки для ПК, Mac, Android і iPhone/iPad, щоб захистити ваші пристрої там, де це найбільше потрібно. Avast пропонує як одноплатформні, так і багатоплатформні варіанти, дозволяючи вам вирішувати, який рівень захисту вам потрібен для всіх ваших пристроїв. У той час як безкоштовна версія Avast блокує віруси та шпигунське програмне забезпечення в режимі реального часу, версія Premium захищає від програм-вимагачів, шахрайських веб-сайтів, крадіжки паролів тощо.

BitDefender Mobile Security

BitDefender Mobile Security для Android та iOS пропонує користувачам захист для мобільних телефонів і планшетів Android/iOS. Платформа постачається з безпечною службою VPN, яка дозволяє швидко та безпечно переглядати веб-сторінки на мобільних пристроях. BitDefender також може дистанційно знаходити, блокувати та стирати втрачені чи викрадені пристрої, а постачальник рекламує мінімальний вплив на час автономної роботи. Крім того, програма забезпечує конфіденційність облікового запису, щоб перевірити, чи не було зламано ваш обліковий запис електронної пошти.

Lookout Personal

Lookout Personal надає користувачам мобільну безпеку, захист особистих даних і запобігання крадіжкам за допомогою однієї програми. Програма захищає своїх користувачів від мобільних загроз, таких як зловмисне програмне забезпечення, рекламне програмне забезпечення та фішинг, перш ніж вони завдадуть шкоди пристрою. Lookout також надає вам цілодобовий доступ до експертів із відновлення ідентифікаційних даних і страхування від крадіжки особистих даних на 1 мільйон доларів США, щоб допомогти відновити вашу особу, якщо ваш пристрій зникне або його вкрадуть. Рішення також попереджає користувачів, коли мережа Wi-Fi небезпечна.

Norton Mobile Security

Norton Mobile Security — це програма для захисту мобільних пристроїв і вірусів, яка захищає та очищає пристрої від зловмисного програмного забезпечення, вірусів та інших загроз. Програма забезпечує інноваційний захист конфіденційності, виявлення незахищених Wi-Fi, розширені функції захисту від крадіжок, критичний веб-захист і перевірку програм. Для користувачів, які хочуть захистити більше пристроїв, Norton Security Deluxe захищає до п'яти різних ПК, Mac, смартфонів і планшетів за допомогою однієї підписки [14].

3.3. Порівняльний аналіз додатка McAfee Mobile Security на базі ОС Android та IOS

Цифрова безпека не прив'язана тільки до комп'ютера або ноутбука — зловмисне програмне забезпечення буває різних форм і розмірів, і оскільки наші мобільні пристрої використовуються для покупок і банківських операцій, вони можуть розкрити нашу найважливішу інформацію під час здійснення транзакцій. Там, де є банківські реквізити, ви побачите зловмисне програмне забезпечення, яке «лазить», намагаючись знайти спосіб вирвати його з сітки безпеки та шифрування, на які ми покладаємося, щоб забезпечити роботу цифрової економіки.

Звідси нещодавнє зростання популярності мобільного пакету безпеки. Ці програми застосовують такий самий рівень захисту до мобільних пристроїв, як і до комп'ютера чи ноутбука, і хоча є безкоштовні варіанти, отримати найбільший захист і функції краще від платної програми. Усі додатки безпеки перейшли на модель підписки, за якою ви платите щорічно за захист певної кількості пристроїв. Вони стягують нижчу ціну за вашу підписку на перший рік, тому важливо перевірити ціну, за якою буде поновлено підписку, інакше є ризику отримати неприємний сюрприз через рік.

Програму McAfee досить просто встановити – вона доступна в Google Play Store для пристроїв Android і в Apple App Store для пристроїв iOS. Його можна завантажити безкоштовно, і можна активувати 30-денну безкоштовну пробну версію, не повідомляючи дані своєї кредитної картки.

Нещодавно компанія внесла кілька значних змін у свій мобільний додаток безпеки, не всі з них сподобалися користувачам. Деякі функції, про які повідомляється, наприклад про видалення, повернулися, у версії для Android і в додатки для iOS.

Було встановлено McAfee Mobile Security на iPad pro з iOS 15 і телефон Android 11. Потім перевірено його в домашній мережі Wi-Fi на обох пристроях і піддано його тестовим файлам від Європейського інституту комп'ютерних антивірусних досліджень (EICAR) і spyshelter.com. Він виявив 100 відсотків тестових файлів.

Як працює McAfee ?

Дві версії програми досить різні. На Android ви отримуєте програму, яка постійно працює у фоновому режимі (спочатку запитує дозвіл) і сканує ваші програми та підключення до Інтернету на наявність уразливостей і шкідливих програм. Обидві програми пропонують VPN і можуть перевіряти безпеку поточного з'єднання Wi-Fi, але програма для iOS потім робить крок назад і вдається до просування служби VPN, а не діє як пакет безпеки.

Лише якщо ви торкнетесь до «служб» у додатку для iOS, можна буде знайти будь-які інструменти: один для сканування поточного з'єднання Wi-Fi на його статус шифрування, сканування темної мережі, щоб побачити, чи ваші дані були включені в порушення даних, і VPN знову. У версії iOS немає активного сканера шкідливих програм. Можливо, це пов'язано з обмеженнями, встановленими Apple, оскільки мало що ще може пояснити прірву між двома версіями однієї програми.

Керування конфіденційністю

Android досить добре тримає програми під контролем і не дозволяє їм шпигувати в тих областях, де вони не повинні бути, наприклад отримувати ваше місцезнаходження у фоновому режимі або мати доступ до ваших контактів, коли їм там нема чого робити. Засіб перевірки конфіденційності додатків McAfee Mobile Security сканує ці дозволи для вас і повідомляє, чи має щось доступ до частин вашого телефону, чи не має. Ця функція, здається, відсутня у версії iOS.

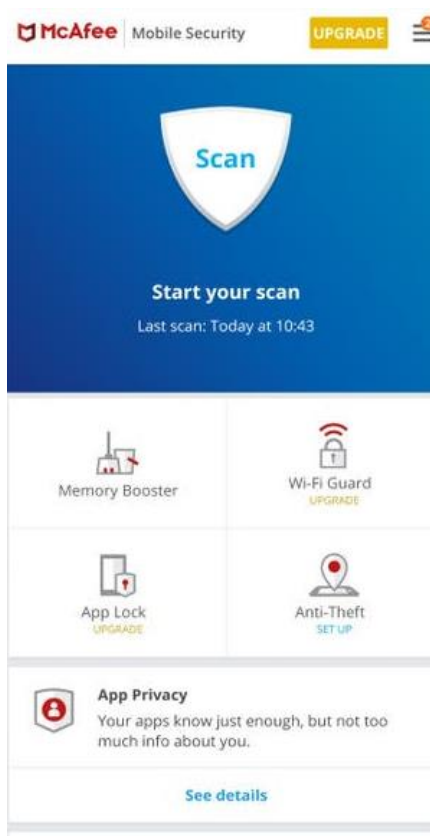


Рис.5 – інтерфейс додатку McAfee Mobile Security

Засіб перевірки конфіденційності додатків версії Android не дозволяє додаткам шпигувати там, де вони не повинні

VPN – це те, що можна знайти в обох версіях програми, і це чудова спроба запровадити додаткове шифрування та конфіденційність фінансових операцій. Він приховує місцезнаходження та застосовує рівень шифрування до вашого веб-перегляду, щоб хакери та шпигуни не могли виявити інформацію, як-от те, коли використовується онлайн-банк або навіть де ви живете. Це приємно мати, але це не варте лише вартості підписки, оскільки існують інші програми, які пропонують подібні послуги з кращими функціями безпеки.

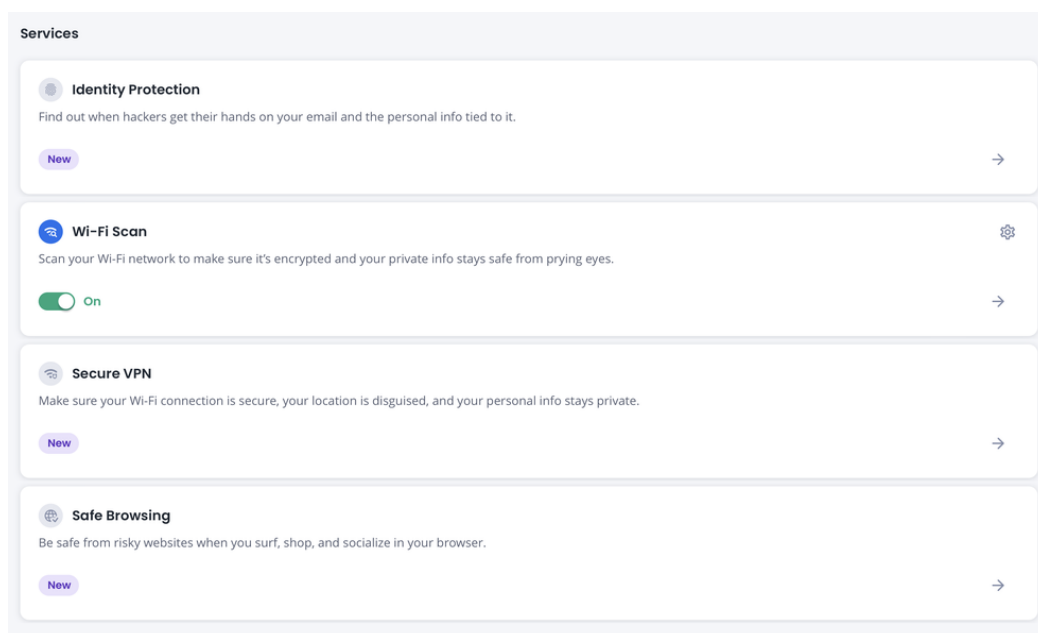


Рис.6 – функціонал, який є доступним в додатку McAfee Mobile Security для користувачів ОС Android

VPN в обох версіях програми забезпечує додаткове шифрування та конфіденційність ваших фінансових операцій

Також, у цій версії McAfee Mobile Security нічого не заважає батьківському контролю – це обробляється через окрему програму Safe Family, яка дозволяє встановлювати та керувати обмеженнями використання на необмеженій кількості

пристроїв, відстежувати їх за допомогою GPS і отримувати сповіщення, якщо ваші діти намагаються отримати доступ до обмеженого вмісту. Знову ж таки, iOS програє, оскільки такі функції, як моніторинг веб-користування, використання додатків, фільтрування веб-сайтів і заборона дітям видаляти програму, не підтримуються на платформі Apple.

Версія мобільної безпеки McAfee для Android має корисний гостьовий режим, який дозволяє накладати обмеження на пристрій, коли ви передаєте його комусь іншому, дозволяючи вам налаштувати, які програми вони можуть використовувати, чи можуть вони надсилати електронні листи чи здійснювати платежі. Якщо ввімкнути цю функцію перед тим, як дати дітям свій телефон, це буде хорошим способом заблокувати їх на YouTube або заборонити їм платити за річну підписку на будь-який додаток без згоди батьків.

Хоча програма для Android сканує на наявність шкідливих програм, для iOS такої функції немає.

Висновок

У своїй інкарнації iOS мобільна безпека McAfee є блідою імітацією настільного додатка, який, здається, значною мірою зацікавлений у тому, щоб підштовхнути до використання його служби VPN. На Android це корисна програма безпеки, яка сканує встановлені програми та перевіряє, чи не зловживають вони своїми дозволами. Було б добре, щоб батьківський контроль був включений в основний додаток, тому що покладатися на надсилання клієнтів до VPN стає втомливим (хоча, ймовірно, необхідним). Як результат, важко рекомендувати McAfee Mobile Security на пристрої iOS, доки його не буде оновлено відповідно до версії Android, яка загалом чудова [15].

ВИСНОВКИ

З кожним роком у світі технологій з'являються нові тенденції. Можна очікувати досить багато мобільних тенденцій, особливо протягом наступних кількох років. Наприклад, побачимо більш значний перехід до прогресивних веб-додатків, більше веб-сайтів, які надають середовище, орієнтоване на мобільні пристрої, і постійну увагу до програм і послуг на основі штучного інтелекту.

Тому обов'язково треба не забувати про безпеку усіх пристроїв, з якими кожен день проходить життя кожної людини. Тим паче, є багато рішень, які мають зручний інтерфейс та досить легкі в налаштуванні.

Обране рішення McAfee Mobile Security надає досить простий і недорогий засіб безпеки для базового та середнього рівня безпеки для мобільних пристроїв. Рішення добре справляється з можливостями сканування на віруси та шкідливі програми. І хоча він не ідеальний, але досить добре виконує свою основну роботу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Що таке мобільний пристрій? [Електронний ресурс] – Режим доступу: <https://tebapit.com/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D0%BC%D0%BE%D0%B1%D1%96%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9-%D0%BF%D1%80%D0%B8%D1%81%D1%82%D1%80%D1%96%D0%B9/>
2. Mobile Devices: Examples, Impact & Trends [Електронний ресурс] – Режим доступу: <https://study.com/academy/lesson/mobile-devices-examples-impact-trends.html>
3. What is Mobile Device [Електронний ресурс] – Режим доступу: <https://www.igi-global.com/dictionary/design-mobile-learning-museums/18836>
4. Mobile Device [Електронний ресурс] – Режим доступу: <https://www.sciencedirect.com/topics/computer-science/mobile-device>
5. Advantages and disadvantages of mobile devices in business [Електронний ресурс] – Режим доступу: <https://www.techtarget.com/searchmobilecomputing/feature/Discover-the-benefits-of-mobile-devices-in-the-enterprise>
6. Advantages and Disadvantages of Mobile Phone [Електронний ресурс] – Режим доступу: <https://quicklearncomputer.com/advantages-and-disadvantages-of-mobile-phone/>
7. Top 6 Mobile Security Threats and How to Prevent Them [Електронний ресурс] – Режим доступу: <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-mobile-security/top-6-mobile-security-threats-and-how-to-prevent-them/>
8. Securing mobile devices in the business environment [Електронний ресурс] – Режим доступу: <https://www.linkedin.com/pulse/securing-mobile-devices-business-environment-keith-andere>

9. Mobile Devices in the Workplace: 40 Statistics You Should Know in 2021 [Електронний ресурс] – Режим доступу: <https://www.perillon.com/blog/mobile-statistics-devices-at-work>
10. Безпека і кібербезпека смартфонів [Електронний ресурс] – Режим доступу: <https://datami.ua/bezpeka-i-kiberbezpeka-smartfoniv/>
11. Best antivirus software for protecting your connected devices [Електронний ресурс] – Режим доступу: <https://www.independent.co.uk/extras/indybest/gadgets-tech/computer-accessories/best-antivirus-software0-b1820958.html>
12. Overall Satisfaction with McAfee Mobile Data Protection [Електронний ресурс] – Режим доступу: <https://www.trustradius.com/reviews/mcafee-mobile-data-protection-2018-02-08-09-48-46>
13. McAfee Mobile Security review [Електронний ресурс] – Режим доступу: <https://www.tomsguide.com/reviews/mcafee-mobile-security>
14. The 5 Best Mobile Security Applications for Android and iOS [Електронний ресурс] – Режим доступу: <https://solutionsreview.com/mobile-device-management/the-5-best-mobile-security-applications-for-android-and-ios/>
15. McAfee mobile security review: Excellent antivirus for Android, but the iOS version falls short [Електронний ресурс] – Режим доступу: <https://www.independent.co.uk/extras/indybest/gadgets-tech/phones-accessories/mcafee-mobile-security-review-b1940100.html>

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)