БЕЗПЕЧНЕ ПІДКЛЮЧЕННЯ МОБІЛЬНИХ ПРИСТРОЇВ ДО КОРПОРАТИВНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТУНЕЛЮ VPN

Сердюков Д.В., Сєвєрінов О.В., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Останнім часом все більше мобільні пристрої використовуються не тільки для повсякденних цілей, а і для виконання професійних завдань організацій та підприємств. Залежно від того, як організація використовує пристрої, несанкціонований доступ до смартфону, планшета або іншого пристрою може призвести до кіберінциденту, пов'язаного зі всією інформаційною системою організації [1, 2].

Метою доповіді є аналіз можливостей використання тунелю VPN для захисту корпоративної інформації на мобільних пристроях, які використовуються для доступу до комп'ютерної мережі установи.

Проведений аналіз основних методів захисту мобільних пристроїв. Одним з найбільш ефективних способів захисту інформації від несанкціонованого доступу є використання тунелю VPN. Співробітники підключаються до VPN щоразу з отриманням доступу до корпоративних даних. Цей тунель дозволяє захистити трафік від несанкціонованого доступу та прослуховування.

В доповіді розглянуті обмеження та недоліки сервісу VPN. А також виконана оцінка ризиків щодо інформаційної безпеки та заходи щодо обробки їх [2]. Однак, VPN не є панацеєю в усіх випадках. Крім того, при низькій пропускній здатності або ненадійному зв'язку у мережі, можуть виникати складності з обробкою даних через VPN канал. Іншим недоліком є можливість злому системи безпеки, що відбувається, якщо зловмисники отримають доступ до тунелю VPN. Тому, для забезпечення максимального рівня безпеки, пропонується використовувати VPN-системи з багатофакторною автентифікацією, які вимагають від користувачів введення додаткового пароля, або використання біометричних методів ідентифікації.

Загалом, використання тунелю VPN для підключення мобільних пристроїв до інформаційної системи організації дозволяє забезпечити захист даних та знизити ризики інформаційної системи.

Варто пам'ятати, що це не є єдиним засобом забезпечення безпеки і вимагає постійного контролю і підтримки.

Список літератури

1. Сєвєрінов О., Федорченко В., Перепадя В. Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків. Системи озброєння і військова техніка 4 (2016): 42-45.

2. Северинов А.В., Черныш, В.И. Анализ угроз и рисков безопасности информации в беспроводных сетях. // Системи управління, навігації та зв'язку.– Вип, 1, 229-232.

3. Why VPNs on mobile devices are a crucial part of securing access to corporate data - ManageEngine Blog. ManageEngine Blog. DOI: https://cutt.ly/V41SZjN (date of access: 30.03.2023).