К. С. Голубич, П. В. Бычков
(*ГГУ им. Ф. Скорины, Гомель*)

СПОСОБЫ ЗАЩИТЫ ОТ АТАК ТИПА «MEN-IN-THE-MIDDLE» В «WI-FI» СЕТЯХ

Если довольно большое количество способов защиты от атак типа «Men-in-the-middle» (далее MITM). Но естественно лучше предупредить, чем лечить, поэтому самый простой способ защиты это не допустить проникновение злоумышленника в саму сеть. В этом случае поможет: установка технологии WPA2/WPA3 со сложным паролем, сложный пароль должен быть длиной не менее 8 символов, содержать цифры, символы, буквы разного регистра, а также не содержать в себе смысловых выражений; ограничение максимального количества пользователей; установка многофакторных методов аутентификации.

Хорошим советом окажется рекомендации по избежанию подключений к общественным «Wi-Fi» точка, т.к. в этом случае злоумышленнику не составит труда провести MITM атаку на устройство.

Дальнейший уровень защиты на основе роутеров и модемов, внутри них необходимо прописать ACL списки с пулом разрешённых MAC-адресов. Необходимо признать, что это является самым лучшим методом защиты, чтобы злоумышленник не смог проникнуть в сеть и провести MITM атаку. Однако в данном случае есть вероятность того, что из-за халатности сотрудников или бреши в защите злоумышленник может проникнуть в сеть.

В предотвращении краже данных могут помочь такие протоколы, как HTTPS, SSl. В самом ПК необходимо настроить Firewall, а также в браузерах рекомендуется к установке плагины HTTPS Everywhere или ForceTLS, которые самостоятельно устанавливают защищенное соединение всякий раз, когда эта опция доступна на стороне сервера.

Добавление дополнительного слоя шифрования для конфиденциальных данных до их передачи – тоже хороший метод, но это сработает только в том случае, если получатель уже имеет ключ шифрования, который вы используете.

Важно также разграничение прав пользователей. Работать под административными правами нежелательно – при этом любой запущенный пользователем троян получает полную власть над системой. Пользователь с ограниченными правами имеет гораздо меньше возможностей что-то испортить, хотя все пользовательские данные могут быть и стёрты. На данный момент необходимость защиты конфиденциальных данных очень высока и кибератаки могут нанести огромный ущерб как интеллектуальной и финансовой собственности, так и физической собственности. Поэтому необходимо продумывать новые стратегии и методы защиты данных.

При проектировании защиты от атак типа «Men-in-the-middle» использовались способы: настройка ACL списка на определённые MAC-адреса; установка сложного пароля; установка плагинов HTTPS Everywhere и ForceTLS.