ВОЗМОЖНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ ПО БЕСПРОВОДНЫМ КАНАЛАМ СВЯЗИ, ОПИСАННЫЕ В БАНКЕ ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ

А.А. Гавришев

Национальный исследовательский ядерный университет «МИФИ», Москва, Россия

Известно [1, 2], что при использовании беспроводных каналов связи (БКС) для передачи данных создаются условия для получения несанкционированного доступа (НСД) к БКС из-за пределов контролируемой зоны. В связи с этим представляется целесообразным определение угроз безопасности информации (УБИ), реализация которых способна нарушить безопасность передачи (БП) данных по БКС.

В России одним из наиболее важных ресурсов, содержащих относительно полный перечень и описание УБИ, является Банк данных угроз безопасности информации ФСТЭК России (БДУ) [3], необходимость использования которого закреплена в нормативных и методических документах ФСТЭК России. Однако его использование для определения УБИ при передаче данных по БКС описано в литературе недостаточно [2]. Воспользуемся данными из БДУ для определения перечня возможных УБИ, реализация которые потенциально способна нарушить БП данных по БКС. Проведенный анализ позволил выделить следующие УБИ, описанные в существующем разделе БДУ: угроза НСД к системе по беспроводным каналам (УБИ.083); угроза деавторизации санкционированного клиента беспроводной сети

(УБИ.011); угроза перехвата данных, передаваемых по вычислительной сети (УБИ.116); угроза подключения к беспроводной сети в обход процедуры аутентификации (УБИ.125); угроза подмены беспроводного клиента или точки доступа (УБИ.126); угроза получения сведений о владельце беспроводного устройства (УБИ.133). В настоящее время, в соответствии с [4], ФСТЭК России разработан новый раздел БДУ, работающий в тестовом режиме. Проведенный анализ позволил выделить следующие УБИ, описанные в новом разделе БДУ: угрозы утечки информации, передаваемой по физическим линиям связи (ФЛС): за счет использования недостатков архитектуры (УБИ.1.12.3), за счет захвата сетевого трафика (УБИ.1.12.7), за счет атаки типа «человек посередине» (УБИ.1.12.10); угрозы НСД к ФЛС за счет: использования недостатков архитектуры (УБИ.2.12.3), захвата сетевого трафика (УБИ.2.12.7), атаки типа «человек посередине» (УБИ.2.12.10), подбора аутентификационной информации (УБИ.2.12.17); угрозы несанкционированной модификации информации, передаваемой по ФЛС за счет: использования недостатков архитектуры (УБИ.3.12.3), атаки типа «человек посередине» (УБИ.3.12.10); угрозы несанкционированной подмены информации, передаваемой по ФЛС связи за счет: использования недостатков архитектуры (УБИ.4.12.3), атаки типа «человек посередине» (УБИ.4.12.10); угрозы вызова отказа в обслуживании ФЛС за счет: захвата сетевого трафика (УБИ.6.12.7), атаки типа «отказ в обслуживании» (УБИ.6.12.14); угрозы нарушения работоспособности ФЛС за счет: захвата сетевого трафика (УБИ.8.12.7).

Представленные в докладе результаты могут быть использованы специалистами по информационной безопасности в своей практической деятельности.

Список литературы

1. Сухарев, Е. М. Общесистемные вопросы защиты информации Кн. 1 / Е. М. Сухарев. – М.: Радиотехника, 2003. – 292 с.

2. Гавришев, А. А. Повышение защищенности беспроводных систем безопасности: аналитический обзор публикаций / А. А. Гавришев // Вестник НГУ. Серия: ИТ. – 2017. – № 1. – С. 5–14.

3. БДУ ФСТЭК России [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru. – Дата доступа: 07.05.2024.

4. Информационное сообщение ФСТЭК России от 04.05.2022 г. N 240/22/2432.