УДК 37.016:004.056.5

А. И. СЕРЫЙ
Брест, БрГУ имени А. С. Пушкина

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА ОСНОВНЫХ МЕТОДОВ АТАК НА СМАРТ-КАРТЫ

Учебной программой дисциплины «Технические средства и методы защиты информации» предусмотрено, в частности, изучение тем, связанных со смарт-картами [1, с. 358, 364–366]. Ниже представлена таблица, в которой сравниваются основные методы атак на такие карты. Таблица может быть использована в образовательном процессе для лучшего усвоения материала.

Таблица – Сравнительная характеристика основных методов атаки на смарт-карты

Название метода	Сущность	Чего позволяет достичь
1. Поиск уязвимостей криптоалгоритмов	*Очевидна из названия метода.* Обусловлена практически полной открытостью всех используемых алгоритмов	Получить доступ к информации
2. Простой и дифференциальный анализ питания, дифференциальный анализ высокого порядка [2]	Оценка осциллограмм потребляемой смарт-картой электроэнергии в момент выполнения криптоалгоритма	Расшифровать криптоалгоритм и получить доступ к информации
3. Физический взлом	Получение доступа к электрическим цепям смарт-карты после химического снятия защитных слоев с кристалла	Выполнить анализ устройства смарт-карты и подключиться к ней с помощью микроэлектродов
4. Необычные условия эксплуатации смарт-карт	Например, нештатный температурный режим, напряжения и частоты сигнала на контактах и т. д.	Получить доступ к информации вследствие сбоев в алгоритмах

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Технические средства и методы защиты информации : учеб. пособие для вузов / А. П. Зайцев [и др.] ; под ред. А. П. Зайцева и А. А. Шелупанова. – 4-е изд., испр. и доп. – М. : Горячая линия – Телеком, 2012. – 616 с.

2. Надежно ли защищены смарт-карты? [Электронный ресурс]. – Режим доступа: kiwibyrd.org/2016/01/05/993/. – Дата доступа: 15.10.2022.