Гаецький Богдан Богданович, Курсант
КВВУ им. Генерала-армии С.М. Штеменко

Нечаев Данил Павлович, Курсант
КВВУ им. Генерала-армии С.М. Штеменко

Енин Николай Николаевич, Слушатель
КВВУ им. Генерала-армии С.М. Штеменко

Кубенко Егор Георгиевич, Слушатель
КВВУ им. Генерала-армии С.М. Штеменко

ТЕХНИЧЕСКИЕ ВОЗМОЖНОСТИ ЭЛЕКТРОННЫХ УСТРОЙСТВ НЕГЛАСНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ НА БАЗЕ СРЕДСТВ СОТОВОЙ СВЯЗИ И СПОСОБЫ ЗАЩИТЫ ОТ НИХ

Аннотация. В условиях стремительного развития цифровых технологий проблема защиты информации приобретает особую актуальность. В данной статье рассматривается важный аспект информационной безопасности, связанный с использованием современных средств сотовой связи для негласного получения конфиденциальных данных.

Ключевые слова: Информационная безопасность, средства негласного получения информации, защита данных, мобильная связь, радиоконтроль.

Современный этап технологического развития характеризуется повсеместным проникновением цифровых технологий во все сферы человеческой деятельности. В этом контексте вопросы обеспечения информационной безопасности выходят на первый план, приобретая особую значимость для государственных структур, коммерческих организаций и частных лиц. Одной из наиболее актуальных проблем в данной области является противодействие электронным устройствам негласного получения информации, использующим инфраструктуру сотовой связи.

Развитие технологий мобильной связи привело к появлению целого класса технических средств, способных осуществлять скрытый перехват информации. Эти устройства отличаются высокой эффективностью и сложностью обнаружения, что обусловлено их работой в стандартных частотных диапазонах, используемых обычными средствами связи.

Среди наиболее распространенных технических решений следует отметить устройства типа IMSI-катчеров, принцип работы которых основан на имитации базовых станций операторов связи. Данная технология позволяет осуществлять перехват не только служебной информации, но и содержания передаваемых данных. При этом сложность обнаружения таких устройств обусловлена их способностью маскироваться под легитимное оборудование.

Отдельного внимания заслуживает проблема уязвимостей в сигнальных системах, в частности, в системе SS7. Эти уязвимости создают потенциальную возможность для несанкционированного доступа к передаваемой информации, включая голосовые сообщения и текстовые данные. Особую опасность представляет тот факт, что эксплуатация данных уязвимостей может осуществляться дистанционно, без физического доступа к оборудованию.

Современные методы обнаружения подобных технических средств требуют комплексного подхода, сочетающего как активные, так и пассивные методы контроля. Среди наиболее эффективных решений можно отметить технологии подавления сигнала и имитации базовых станций, которые позволяют выявлять скрытые устройства за счет анализа их реакций на управляющие воздействия.

Проведенный анализ позволяет сделать вывод о необходимости разработки комплексной системы защиты информации, учитывающей современные угрозы, связанные с использованием средств сотовой связи для негласного получения данных. Эффективное

противодействие таким угрозам требует не только применения технических средств контроля, но и совершенствования нормативно-правовой базы, а также повышения уровня осведомленности пользователей о потенциальных рисках.

Перспективными направлениями дальнейших исследований в данной области могут стать разработка новых алгоритмов обнаружения скрытых устройств и совершенствование криптографических методов защиты передаваемой информации.

Список литературы:

1. Бузов, Г. А. Выявление специальных технических средств несанкционированного получения информации / Г. А. Бузов. – Москва: Горячая линия – Телеком, 2019. – 204 с. – ISBN 978-5-9912-0674-3. – EDN XZZXQX.

2. Стародубцев, Ю. И. Экспериментальная методика и результаты обработки данных об электромагнитной обстановке в ультракоротковолновом диапазоне / Ю. И. Стародубцев, А. В. Акишин // Системы управления, связи и безопасности. – 2018. – № 4. – С. 226–248. – EDN YUJWQK. URL: https://www.elibrary.ru/item.asp?id=36254182

3. Акишин, А. В. Экспериментальная методика и результаты оценки стационарности уровня помех в ультракоротковолновом диапазоне / А. В. Акишин, В. В. Алашеев, Ю. И. Стародубцев // Проблемы технического обеспечения войск в современных условиях: Труды III Межвузовской научно-практической конференции, Санкт-Петербург, 16 февраля 2018 года. Том 1. – Санкт-Петербург: ВАС им. С. М. Буденного, 2018. – С. 62–66. – EDN ZVXKPT. URL: https://www.elibrary.ru/item.asp?id=35267193

4. Акишин, А. В. Экспериментальная методика и результаты оценки уровня помех в ультракоротковолновом диапазоне / А. В. Акишин, В. В. Алашеев, П. Ю. Стародубцев // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): сборник научных статей: в 4 томах. Том 3. – Санкт-Петербург: СПбГУТ им. проф. М. А. Бонч-Бруевича, 2018. – С. 4–9. – EDN XQLMNR. URL: https://www.elibrary.ru/item.asp?id=35678214

5. Акишин, А. В. Экспериментальная методика и результаты оценки временной устойчивости уровня помех в ультракоротковолновом диапазоне до 2 ГГц / А. В. Акишин, А. А. Бречко, Ю. И. Стародубцев // Радиолокация, навигация, связь: Сборник трудов XXIV Международной научно-технической конференции. Том 4. – Воронеж: ООО "Вэлборн", 2018. – С. 397–401. – EDN YTKGPV. URL: https://www.elibrary.ru/item.asp?id=35432871