ПОИСК ЗАКЛАДНЫХ УСТРОЙСТВ КОМБИНАЦИОННЫМ МЕТОДОМ

В.М. Алефиренко, В.С. Андрушкевич

Обнаружение, поиск и локализация закладных устройств может осуществляться с помощью различных специализированных приборов, каждый из которых имеет свои преимущества и недостатки при работе в тех или иных условиях состояния электромагнитной обстановки на объекте (в помещении). К таким приборам в первую очередь относятся индикаторы электромагнитного поля, сканирующие приемники и аппаратно-программные комплексы, а также ряд дополнительных приборов, таких как интерсепторы, радиочастотомеры, радиотестеры, анализаторы спектра и др. [1]. Использование в комбинации нескольких видов приборов может повысить эффективность обнаружения, поиска и локализации закладных устройств.

Для экспериментальных исследований были использованы индикатор электромагнитного поля и интерсептор частного производства и портативный частотомер ROGER RFM-31, сканирующие приемники AR-3000A и IC-R5 промышленного производства. В качестве закладного устройства использовался имитатор радиомикрофона, работающий на частоте 509,5 МГц. Поиск и обнаружение радиомикрофона осуществлялось с помощью индикатора поля и интерсептора методом акустической завязки, а локализация – с помощью радиочастотомера и сканирующих приемников. Как показали исследования, захват сигнала радиомикрофона индикатором поля и интерсептором происходил на расстоянии 0,2–1,5 м, а захват (измерение) частоты радиочастотомером – на расстоянии 0,1–0,5 м в зависимости от взаимного расположения антенн радиомикрофона и используемых приборов. После определения радиочастотомером частоты радиомикрофона, что указывало на стабильную работу радиопередатчика в помещении, осуществлялось сканирование сканирующими приемниками только узкого диапазона частот, в который попадала измеренная частота. В результате, по звуковому фону помещения, воспроизводимому динамиком сканирующего приемника, однозначно устанавливалось наличие закладного устройства. Захват сигнала радиомикрофона сканирующими приемниками происходил на расстоянии 30–60 м в зависимости от условий распространения радиоволн (свободное пространство, наличие стен, перегородок).

Таким образом, для обнаружения, поиска и локализации закладных устройств можно использовать комбинацию различных приборов поиска, которая позволяет повысить эффективность обнаружения.

Литература

1. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации. М. : Горячая линия – Телеком, 2013. 240 с.

ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ И БЕЗОПАСНОСТИ ГОЛОСОВЫХ АССИСТЕНТОВ

В.М. Алефиренко, В.В. Костюченко

В современном мире все чаще в новые смарт-устройства внедряются системы голосовых ассистентов, таких как Siri, Alexa и Google Assistant. Все крупные IT компании ведут разработку своих систем и предлагают их на рынке, встраивая в собственное оборудование. На данный момент различные голосовые системы устанавливаются на все смартфоны, некоторые автомобили и умные дома. Голосовые помощники поддерживают управление умными устройствами в доме и офисе напрямую со смартфона, имеют доступ к управлению большинством автомобильных систем. Также голосовые ассистенты уже умеют вызывать такси, оплачивать самостоятельно покупки в интернет-магазинах, отправлять сообщения, совершать звонки, настраивать параметры систем умного дома, записывать сценарии действий пользователя, прокладывать по просьбе пользователя маршруты любым транспортом и т.д. Но все эти возможности несут в себе риски безопасности и конфиденциальности. Устройство, имеющее голосовой помощник, при помощи встроенных микрофонов прослушивает

окружающий звуковой фон и реагирует на поступающие команды. Так как устройства не умеют корректно отличать голос владельца системы от голоса других людей, то любой человек может передать команду на выполнение голосовому ассистенту, например, отправить секретные документы по названному адресу почты. Эта проблема хорошо известна всем компаниям, разрабатывающим системы голосового управления, но без потери функционала для пользователя она пока не решена. Так же известен способ, при котором голосовые команды для ассистентов передаются удаленно и массово. Микрофоны современных устройств умеют улавливать звуковые колебания, неслышные человеку. Это позволяет записывать голосовые команды в любые массовые аудио и видео трансляции. Голосовые помощники интерпретируют услышанные звуки, различают буквы и составляют предложения. Благодаря этому им можно давать любые команды, например, перевести деньги на озвученный счет или зайти на сайт и заполнить форму с личными данными. Такие команды могут быть зашифрованы в ролике на YouTube, вставлены в фильм или сделаны как фоновый шум. На данный момент защитных систем от данных видов угроз не представлено.

Литература

1. Audio Adversarial Examples // University of California, Berkeley, and Georgetown University [Электронный ресурс]. –. URL https://nicholas.carlini.com/code/audio_adversarial_examples (дата обращения: 14.05.2018).

2. Ronan De Renesse – Virtual digital assistants to overtake world population by 2021 [Электронный ресурс]. – URL https://ovum.informa.com/resources/product-content/virtual-digital-assistants-to-overtake-world-population-by-2021 (дата обращения: 14.05.2018).

МОБИЛЬНАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

В.М. Алефиренко, Ч.Ф. Нгуен

Мобильные системы видеонаблюдения могут широко использоваться на объектах, имеющих небольшие территории или помещения при проведении мероприятий, носящих временный характер, таких как спортивные соревнования, выставки, собрания и т.п. Эффективность таких систем может быть повышена, если они используют компьютерные технологии и возможность контроля и управления по сети Интернет.

Разработанная мобильная система видеонаблюдения предназначена для обеспечения видеоконтроля на охраняемых объектах с использованием компьютерных технологий и управлением по сети Интернет. Система построена на базе компьютерного зрения [1], протоколов MQTT и HTTP. Технология компьютерного зрения позволяет проводить обработку и анализ видеоинформации, что обеспечивает своевременное обнаружение угроз и оперативное реагирование в соответствии с обстановкой. Мозгом системы является одноплатный компьютер, на котором осуществляются обработка видеосигнала (распознавание объектов, отслеживание, обнаружение движения), управление серводвигателями, видеотрансляция с помощью протокола HTTP, ответы на запросы пользователя и оповещение о тревоге с помощью протокола MQTT. Для видеотрансляции используется веб-фреймворк Flask. С помощью Flask и Python, одноплатный компьютер становится сервером видеотрансляции. Доступ к изображениям выполняется с помощью протокола HTTP с веб-браузера или приложения. Компоненты системы включают: одноплатный компьютер Raspberry Pi 3, модуль Pi Camera, микроконтроллер ATmega 328, два серводвигателя и управляющее приложение для персонального компьютера. Программирование реализовано на языках Си, Python и Java. Конструктивно компоненты системы размещены в одном корпусе, на котором имеются соответствующие органы управления, индикации и разъемы для подключения внешних устройств и сети Интернет. Основными преимуществами разработанной системы является невысокая стоимость, мобильность, возможность быстрого развертывания и свертывания на объекте, гибкость размещения отдельных компонентов, адаптация к индивидуальным требованиям пользователя.

Литература

1. Ворона В.А., Тихонов В.А. Технические средства наблюдения в охране объектов. М.: Горячая линия – Телеком, 2012. 184 с.