УДК. 004.056.53

МОДЕЛИРОВАНИЕ СЦЕНАРИЕВ РАБОТЫ УСТРОЙСТВ НЕСАНКЦИОНИРОВАННОГО СЪЕМА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ОСНОВЕ ИМИТАЦИОННЫХ СРЕДСТВ

Бобылева София Вадимовна[1], Минзов Анатолий Степанович[2]

[1]Студент;
ГБОУ ВО МО «Университет «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: sbobylova94@gmail.com.

[2]Доктор технических наук, профессор;
ГБОУ ВО МО «Университет «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: 926-565-0570@mail.ru.

В статье дан обзор возможных ситуаций несанкционированного съема конфиденциальной информации по техническому каналу. Рассмотрены способы защиты от утечки информации при помощи моделирования данных ситуаций с использованием имитаторов сигналов. Представлен обзор существующих имитаторов сигналов, их технические характеристики и функциональные возможности. Рассмотрены возможные ситуации утечки информации и способы их обнаружения с использованием программно-аппаратного комплекса «Кассандра К6».

Ключевые слова: несанкционированный съем конфиденциальной информации, утечка информации, техническая защита информации, технический канал, имитатор сигналов, многофункциональный имитатор сигналов «Шиповник-2», комплекс радиомониторинга «Кассандра К6».

SIMULATION OF SCENARIOS FOR THE OPERATION OF DEVICES FOR UNAUTHORIZED REMOVAL OF CONFIDENTIAL INFORMATION BASED ON SIMULATION TOOLS

Bobyleva Sofia[1], Minzov Anatoly[2]

[1]Student;
Dubna State University,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: sbobylova94@gmail.com.

[2]Doctor of Computer Science, professor;
Dubna State University,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: 926-565-0570@mail.ru.

The article provides an overview of possible situations of unauthorized removal of confidential information through a technical channel. Ways to protect against information leakage by simulating situation data using signal simulators are considered. A review of existing signal simulators, their technical characteristics and functionality is presented. Possible situations of information leakage and ways of their detection using the software and hardware complex "Kassandra K6" are considered.

Keywords: unauthorized removing of confidential information, information leakage, technical information security, the technical channel, the simulator of signals, the multifunction simulator of signals "The Shipovnik-2", a radio monitoring complex "Kassandra K6".

Введение

Защита информации от несанкционированного съема конфиденциальной информации (НСКИ) является частью решений общей проблемы информационной безопасности.

В то же время использование технических средств для обработки информации и передачи её создает особый вид угроз информационной безопасности, известных как утечка по техническим каналам.

Одним из видов угроз деятельности и коммерческих предприятий является несанкционированный съем служебной, коммерческой и личной информации на каналах связи и различных коммуникаций. Наиболее распространенными техническими каналами распространения информации являются акустические сигналы. Специальные средства негласного съема информации служат для приема и видоизменения сигналов с целью получения разведывательной информации.

На любом объекте, где требуется обеспечение информационной безопасности, необходимо внедрение комплексной системы защиты информации (КСЗИ), в том числе и от утечки по техническим каналам.

Одним из эффективных способов обеспечения информационной безопасности – это предотвращение утечки информации при помощи моделирования возможных угроз безопасности.

Моделирование угроз безопасности подразумевает анализ всех возможных способов нарушения конфиденциальности информации.

Для создания модели угрозы проникновения, довольно близкой к осуществимой, необходимо попытаться мысленно представить варианты проникновения к источнику информации. Чем больше при этом будет принято в расчет факторов, влияющих на эффективность проникновения, тем выше идентичность модели. В условиях отсутствия информации о злоумышленнике, его квалификации, технической оснащенности во избежание неприемлемых ошибок лучше переоценить угрозу, чем ее недооценить, хотя такой подход и может привести к увеличению затрат на защиту.

Анализ существующих типовых имитационных средств НСКИ

Контроль состояния защиты конфиденциальной информации включает соответствие требованиям защиты от НСКИ.

Одним из методов проверки защищенности объекта от НСКИ является моделирование возможных сценариев работы устройств НСКИ. Подобные сценарии можно разработать при помощи имитационных средств. Такие средства помогают смоделировать максимально близкие к реальной ситуации утечки конфиденциальной информации.

Большинство физических имитационных средств представляют собой средства имитации утечки конфиденциальной информации по техническим каналам. Для подавляющего числа объектов под технической защитой информации подразумевается защита речевой информации. Речевая информация может передавать в следующих формах:

- речевая информация в форме акустических (механических) колебаний в воздухе;
- речевая информация в форме вибрационных колебаний в твердой (жидкой) среде;
- речевая информация в форме электрических колебаний.

Так же информация может передаваться по техническим каналам (в физической форме) в следующих формах:

- информация (неречевая) в электронной форме в виде электрических колебаний;
- информация в визуальной форме в виде видимого света (видовая);
- информация в форме модулированного ультразвука, лазерного излучения, некогерентного ИК – излучения.

Основным назначением имитаторов сигналов является создание сигналов, имитирующих излучение устройств негласного получения конфиденциальной информации (подслушивающих устройств, жучков).

Имитаторы сигналов используются в обучении поиску специальных технических средств негласного получения информации, проверки работоспособности поисковой техники. Вариантов исполнения имитаторов сигналов множество. От мини радиопередатчика до многоканального комплекса с большой библиотекой сигналов и программным обеспечением на ПК.

Многофункциональный имитатор сигналов создает излучения в очень широком диапазоне частот: от инфразвука до оптического диапазона. При этом имитатор сигналов имеет возможность подключаться к различным проводным линиям.

На сегодняшний день самыми популярными являются следующие имитаторы:

- имитатор сигналов сложного типа «Аврора-3»;
- многофункциональный имитатор сигналов «Шиповник-2»;
- многофункциональный управляемый имитатор сигналов «Парнас-И Плюс»;
- имитатор сигналов *ST* - 121;
- многофункциональный имитатор сигналов «ИМПУЛЬС-3»;
- многофункциональный имитатор «ИМФ-2».

Имитатор сигналов сложного типа «Аврора-3» предназначен для воссоздания радиосигналов, итмитируя работу различных радиопередающих устройств.

Такой комплекс способен формировать и излучать радиосигналы различных модуляций.

Управление данным комлексом производится по интерфейсу ЛВС типа *Ethernet* в стационарном режиме, либо с помощью встроенного пульта управления в автономном режиме. Так же комплекс может управляться дистанционно по беспроводному интерфейсу с помощью выносного пульта.

Имитационное устройство с такими характеристиками позволяет рассмотреть большое количество возможных ситуаций утечки конфиденциальной информации. Позволяет разработать несколько моделий сценариев утечки информации по техническим каналам.

Рис. 1. Имитатор сигналов сложного типа «Аврора-3»

Многофункциональный имитатор сигналов «Шиповник-2» предназначен для проверки эффективности работы средств радио мониторинга, используемых для специальных исследований защиты объектов от утечки информации. Также данный имитатор используется для обучения специалистов информационной безопасности в высших учебных заведениях.

«Шиповник-2» представляет собой передатчик, работающий в нескольких диапазонах частот. Имитатор имеет возможность генерировать сигналы различных модуляций. Может имитировать сигналы свип-генератора, микрофона, а также внешний низко частотный сигнал. «Шиповник-2» имеет встроенный таймер, что позволяет смоделировать периодические сигналы.

Рис. 2. Многофункциональный имитатор сигналов «Шиповник-2»

Многофункциональный управляемый имитатор сигналов «Парнас-И Плюс» имеет назначение такое же, как и имитатор сигналов «Шиповник-2». Главным его отличием от «Шиповник-2» является то, что данный имитатор представляет собой программно-аппаратный комплекс. Комплекс позволяет создавать следующие сигналы:

- реакции приемников дистанционного управления в цепях питания;
- акустоэлектрического преобразователя;
- источника вторичного модулированного излучения;
- источника вторичного модулированного сигнала в проводных линиях;
- источника инфракрасного излучения, в том числе модулированного;
- сотовых средств связи;
- беспроводных средств доступа.

Рис. 3. Многофункциональный управляемый имитатор сигналов «Парнас-И Плюс»

Имитатор сигналов *ST*-121 предназначен для проведения лабораторных исследований, проверки работоспособности сканирующих устройств и обучения специалистов, занимающихся поиском технических каналов утечки информации.

Имитатор способен генерировать низкочастотные и высокочастотные сигналы, сигналы передачи цифровых данных, звуковые и ультразвуковые сигналы, радиосигналы. Представляет собой небольшое переносное устройство с ВЧ-антенной.

Рис. 4. Имитатор сигналов ST–121

Многофункциональный имитатор сигналов «ИМПУЛЬС-3» предназначен для имитации работы средств съема информации по различным каналам связи.

Прибор может быть использован так же, как и выше представленные имитационные средства.

Прибор может имитировать излучение радиочастотных средств, работу переизлучателей частоты с модуляцией акустическим колебанием, работу устройств, использующих процесс ВЧ-навязывания, прохождение звуковых сигналов по структуре ограждающих конструкций и инженерных коммуникаций.

Рис. 5. Многофункциональный имитатор сигналов «ИМПУЛЬС-3»

Многофункциональный имитатор «ИМФ-2» предназначен для имитации работы средств съема информации при проведении поисковых мероприятий. Прибор воспроизводит физические процессы, сопровождающие утечки информации по техническим каналам, и позволяет провести их объективную оценку. Использует только модуляцию ЧМ максимальной частотой 490 МГц.

Рис. 6. Многофункциональный имитатор «ИМФ-2»

Проанализировав все выше представленные имитационные средства, можно сделать вывод что все они предназначены для проведения лабораторных исследований, проверки работоспособности сканирующих устройств, используемые специалистами для проверки степени защищенности объекта от несанкционированного съема конфиденциальной информации и обучения специалистов, занимающихся поиском технических каналов утечки информации (таблица 1).

Функционал данных имитаторов разнообразный, что позволяет смоделировать разнообразные сценарии несанкционированного съема информации злоумышленником. Большое количество подобных сценариев позволит предотвратить утечку информации по техническим каналам.

Таблица 1. Таблица характеристик имитаторов сигналов

Имитатор	Назначение	Состав комплекса	Возможности имитатора	Описание
Имитатор сигналов сложного типа «Аврора-3»	предназначены для воспроизведения радиосигналов, с нормированными значениями несущей частоты и полосы, имитирующих работу различных радиопередающих устройств с амплитудной, фазовой и частотной модуляциями и их комбинациями.	основной блок; широкополосная антенна; кабель управления основным блоком от ПЭВМ; блок питания от сети 220 В; зарядное устройство; два комплекта аккумуляторных батарей; адаптер питания от бортовой сети автомобиля; отвертка; специальное программное обеспечение; Паспорт-формуляр и инструкция по эксплуатации.	формирование и излучение в эфир радиосигналов с заданными оператором характеристиками; наличие библиотеки стандартных возможность создания собственных сигналов и сохранения их в пользовательских библиотеках; работу под управлением ПЭВМ, под управлением КПК по радиоканалу, удаленного управления по Ethernet, а также работу в автономном режиме по заданной оператором программе излучения сигналов;	конструктивно имитатор выполнен в виде моноблочного прибора. Управление имитатором осуществляется с помощью специального программного обеспечения (СПО) установленного на ПЭВМ и через карманный персональный компьютер (КПК), который обеспечивает передачу команд по беспроводному интерфейсу стандарта WiFi, что делает возможным скрытое управление генератором при его закладке или перемещении.
Многофункциональный имитатор сигналов «Шиповник-2»	Предназначен для проверки эффективности работы устройств и комплексов радиомониторинга, используемых для обследования и защиты выделенных помещений, а также для обучения специалистов, занимающихся поиском каналов утечки информации.	Имитатор сигналов «Шиповник-2»; техническое описание, инструкция по эксплуатации; сСетевой адаптер15 В/1,2А; антенна диапазона144 МГц; антенна диапазона433 МГц; антенна диапазона1200/2400 МГц.	Выбирать различные источники и характеристики низкочастотных, модулирующих сигналов: микрофонный канал или линейный низкочастотный вход с возможность включения режима закрытия (дельта-модуляция, инверсия спектра); – встроенный генератор свиппирующего сигнала. Выбирать различные виды модуляции: – широкополосная частотная (WFM); – узкополосная частотная (NFM); – FM-FM; – модуляция шумоподобным сигналом (ШПС); – ППРЧ (перестраиваемая псевдослучайным образом рабочая частота).	«Шиповник-2» отличается широким набором функций и представляет собой маломощный передатчик, работающий в нескольких диапазонах частот, в котором реализованы различные виды модуляции и имеется возможность задания типа модулирующего сигнала.

			Осуществлять высокочастотную генерацию в следующих частотных диапазонах: – 144 МГц, 433 МГц, 1,2 ГГц, 2,4 ГГц. Задавать временные режимы работы устройства: – непрерывный – кратковременный однократный – периодический. Устройство «Шиповник-2» функционирует под управлением микроконтроллера. Требуемые пользователю режимы и параметры устанавливаются с клавиатуры, и отображаются на ЖК дисплее. Мощность излучения в каждом частотном диапазоне – не менее 10 мВт.	
Многофункциональный управляемый имитатор сигналов «Парнас-И Плюс»	Имитатор сигналов предназначен для тестирования поискового оборудования и обучения специалистов, привлекаемых к работам по выявлению в технических средствах и помещениях возможно внедренных электронных устройств негласного получения информации.	Состав - аппаратная часть в кейсе (АЧ) на основе управляющей ПЭВМ и устройств подключения, сопряжения и имитации сигналов; - специальное программное обеспечение (СПО).	Изделие, позволяет имитировать (создавать) следующие сигналы: - реакции приемников дистанционного управления в цепях питания; - акустоэлектрического преобразователя; - источника вторичного модулированного излучения; - источника вторичного модулированного сигнала в проводных линиях; - источника инфракрасного излучения, в том числе модулированного; - сотовых средств связи; - беспроводных средств доступа.	Имитатор сигналов предназначен для тестирования поискового оборудования и обучения специалистов, привлекаемых к работам по выявлению в технических средствах и помещениях возможно внедренных электронных устройств негласного получения информации.
Имитатор сигналов ST – 121	Основным назначением имитаторов сигналов является генерация сигналов, имитирующих излучение устройств негласного получения информации (подслушивающих устройств, жучков).Имитация каналов	Основной блок ВЧ антенна Кабель "220В" Кабель "RJ-45" Кабель "3/RJ-45" Блок питания/зарядное устройство	обеспечивает генерацию: Радиосигналов с произвольно выбираемыми значениями частот в диапазоне 100 - 6000МГц, регулируемой выходной мощностью, АМ и ЧМ модуляцией , сигналов с ППРЧ, ШПС и СКП Сигналов, имитирующих цифровые стандарты передачи данных (GSM, DECT, BLUETOOTH и	Имитатор сигналов ST121 предназначен для имитации каналов передачи информации, используемых специальными техническими средствами негласного получения информации (СТС НПИ); нелинейного эффекта при подключении

	передачи информации, используемых специальными техническими средствами негласного получения информации (СТС НПИ) Имитация нелинейного эффекта при подключении к проводным линиям СТС НПИ Имитация побочного электромагнитного излучения СТС НПИ		WLAN) НЧ и ВЧ сигналов в сеть 220В и слаботочные линии ИК сигнала с модуляцией НЧ сигналом и выбором несущей частоты Звуковых и ультразвуковых сигналов, как с произвольно выбираемыми значениями частот, так и с частотами, соответствующим значениям октавных и трехоктавным фильтров. Обеспечено непосредственное подключение динамического излучателя к выходному разъему ST121 Низкочастотного магнитного поля	к проводным линиям СТС НПИ; побочного электромагнитного излучения СТС НПИ.
Многофункциональный имитатор сигналов"ИМПУЛЬС-3"	"ИМПУЛЬС-3" предназначен для имитации работы средств съема и передачи информации по различным каналам связи. Может быть использован при проверке работоспособности поисковых приборов, а также при проведении поисковых мероприятий.	СОСТАВ КОМПЛЕКТА: Имитатор сигналов - "ИМПУЛЬС-3" Имитатор переизлучателя Активная акустическая система- "ПРИБОЙ"(поставляется по желанию заказчика) Антенна излучающая телескопическая (для поддиапазона 1) Универсальная широкополосная антенна- "АШУ" (для поддиапазона2) Антенна радиопереизлучения ИК-излучатель Комплект соединительных кабелей и адаптеров	ПРИБОР ИМИТИРУЕТ: Излучение радиочастотных средств Работу переизлучателей частоты с модуляцией акустическим колебанием Передачу сигналов в проводных коммуникациях Работу устройств, использующих процесс ВЧ-навязывания Работу устройств, использующих в качестве канала передачи ИК-диапазон Эффект акустоэлектрического преобразования Прохождение звуковых сигналов по структуре ограждающих конструкций и инженерных коммуникаций	"ИМПУЛЬС-3" предназначен для имитации работы средств съема и передачи информации по различным каналам связи. Может быть использован при проверке работоспособности поисковых приборов, а также при проведении поисковых мероприятий.

Многофункциональный имитатор «ИМФ-2»	"ИМФ-2" предназначен для имитации работы средств съема информации при проведении поисковых мероприятий. Прибор воспроизводит физические процессы, сопровождающие процесс утечки информации по указанным каналам и позволяет провести их объективную оценку.	Имитатор "ИМФ-2" * Кабель сетевой * Кабели для подключения к телефонной линии.	Прибор воспроизводит физические процессы, сопровождающие утечки информации по перечисленным ниже каналам, и позволяет провести их объективную оценку. Акустический канал: оценка утечки по вентиляционным каналам, сквозным щелям, трещинам и нарушениям уплотнителей, по структуре ограждающих конструкций и инженерных коммуникаций. выявление микрофонного эффекта различного оборудования. Передача сигнала по электросети и телефонной линии: имитация подозрительных электрических сигналов в линиях силового и слаботочного электрооборудования. Радиоканал: имитация излучения средств съема информации с ЧМ модуляцией. Канал инфракрасного излучения: имитация оптического излучения осветительных приборов, индикаторов, датчиков сигнализации. Канал телефонного передатчика: имитация работы телефонного передатчика с передачей информации по радиоканалу	Во всех режимах существует возможность имитации акустического сигнала (меняющийся тон или микрофон) или обрабатываемой информации (меняющийся тон) в речевом диапазоне частот.

Современные требования к подготовке специалистов по технической защите информации

Компетенция «Информационная безопасность» входит в список наиболее востребованных и перспективных профессий в соответствии с лучшими зарубежными стандартами и передовыми технологиями.

Значимость специалистов в области информационной безопасности неумолимо растет. Представители данной специальности могут работать организациях, имеющих собственные компьютерные сети и нуждающихся в сохранности конфиденциальной информации (государственная тайна, служебная тайна, коммерческая тайна, сохранность персональных данных).

Информационная безопасность требует широкий спектр познаний и навыков в области информационных технологий. В связи с быстрым развитием этой области, требования к техникам по защите информации постоянно возрастают.

Специалиста по технической защите информации называют техником по защите информации. Техник по защите информации – это специалист, занимающийся обеспечением информационной безопасности объекта и его информационной инфраструктуры, техническим обслуживанием средств защиты информации.

Согласно ФСТЭК, функциональными квалификационными требованиями к специалистам, обеспечивающим техническую защиту информации ограниченного доступа, являются знания:

- основных понятий в области технической защиты информации и обеспечения безопасности информации в ключевых системах информационной инфраструктуры;
- технических каналов утечки информации ограниченного доступа;
- характеристик различных типов информационных сигналов, содержащих информацию ограниченного доступа;
- системы организации комплексной защиты информации;
- перспективных направлений, программно – аппаратных средств, методов и средств технической защиты информации ограниченного доступа;
- основ проведения технической защиты информации;
- методов выявления угроз безопасности информации;
- методов и порядка организации и проведения специальных исследований, нацеленных на выявление степени защищенности информации на объекте от утечки информации по техническим каналам;
- отечественного и зарубежного опыта в области технической защиты информации;
- нормативных правовых актов в области технической защиты.

Также в документации ФСТЭК прописаны необходимые навыки:

- Работы с нормативными правовыми актами навыки;
- работы с базами данных, содержащих информацию ограниченного доступа;
- планирования и организация проведения работ в области технической защиты информации на объекте;
- проектирования, построения и эксплуатации КСЗИ;
- оценки возможных технических разведок, выявление угроз безопасности, технических каналов утечки информации, выявление нарушений в использовании технических систем и средств при обработке конфиденциальной информации.

Требования к подготовке специалистов в области обеспечения технической защиты указаны в ФГОС ВО 10.03.01 «Информационная безопасность» уровня бакалавриата.

Просмотрев все нормативно – правовые документы можно выделить требования, предъявляемые к технику по защите информации, которые ценятся превыше всего. Среди них:

- Участие в работе по обеспечению информационной безопасности предприятия, соблюдению охраняемой законом тайны (государственной, служебной, коммерческой).
- Осуществление проверки технического состояния, установки, наладки и регулировки аппаратуры и приборов, их профилактические осмотры и текущий ремонт.
- Выполнение работы по эксплуатации средств защиты и контроля информации, отслеживание работы аппаратуры и другого оборудования.
- Ведение учета работ и объектов, подлежащих защите, установленных технических средств, журналы нарушений их работы, справочники.
- Подготовка технических средств для проведения всех видов плановых и внеплановых контрольных проверок, аттестации оборудования, а также в случае необходимости к сдаче в ремонт.
- Проведение наблюдения, выполнение работ по оформлению протоколов специальных измерений и другой технической документации, в том числе отчетной, связанной с эксплуатацией средств и контроля информации.
- Выполнение необходимых расчетов, анализа результатов, составление технических отчетов и оперативных сведений.
- Определение причин отказов в работе технических средств, подготовка предложений по их устранению и предупреждению
- Обеспечение высокого качества и надежности используемого оборудования, повышение эффективности мероприятий по контролю и защите информации.
- Участие во внедрении разработанных технических решений и проектов, оказание технической помощи при изготовлении, монтаже, наладке, испытаниях и эксплуатации проектируемой аппаратуры.

Моделирование сценариев работы НСКИ на основе технического средства «Шиповник»

Имитатор сигналов «Шиповник-2» представляет собой многофункциональное устройство и позволяет модулировать ситуации несанкционированного съема конфиденциальной информации

«Шиповник-2» позволяет смоделировать более 120 ситуаций утечки информации по акустическим каналам различных модуляций, частот, позволяет имитировать различные источники сигналов.

С использованием имитатора можно смоделировать работу микрофонного канала линейный низкочастотный вход с возможность включения режима закрытия (дельта-модуляция, инверсия спектра). Имеется возможность использования встроенного генератора свиппирующего сигнала (генератор качающейся частоты - определенный вид генератора сигналов, объединенного с осциллографом, в котором частота выходного сигнала не является постоянной).

Все представленные источники сигналов могут иметь разную модуляцию.

- частотная (широкополосная (*WFM*), узкополосная *(NFM*), *FM-FM*);
- Дельта-модуляция;
- модуляция шумоподобным сигналом (ШПС);
- ППРЧ (перестраиваемая псевдослучайным образом рабочая частота).

Осуществляет высокочастотную генерацию в следующих частотных диапазонах:

- 144 МГц,
- 433 МГц,
- 1,2 ГГц,
- 2,4 ГГц.

Задавать временные режимы работы устройства: непрерывный; кратковременный, однократный; периодический.

Устройство функционирует под управлением микроконтроллера. Требуемые пользователю режимы и параметры устанавливаются с клавиатуры, и отображаются на ЖКИ-дисплее.

С использование имитатора можно смоделировать ситуацию утечки информации на частоте 144 МГц. При этом сигналы могут быть разные, так как «Шиповник-2» позволяет выбрать различные модуляции. Например, на данной частоте можно имитировать любительскую радиосвязь модуляции *NFM*, например, ультракороткие волны (УКВ). Данная ситуацию можно наблюдать в виде графика при радиомониторинге, а программе *RadioInspector RT* (рисунок 7).

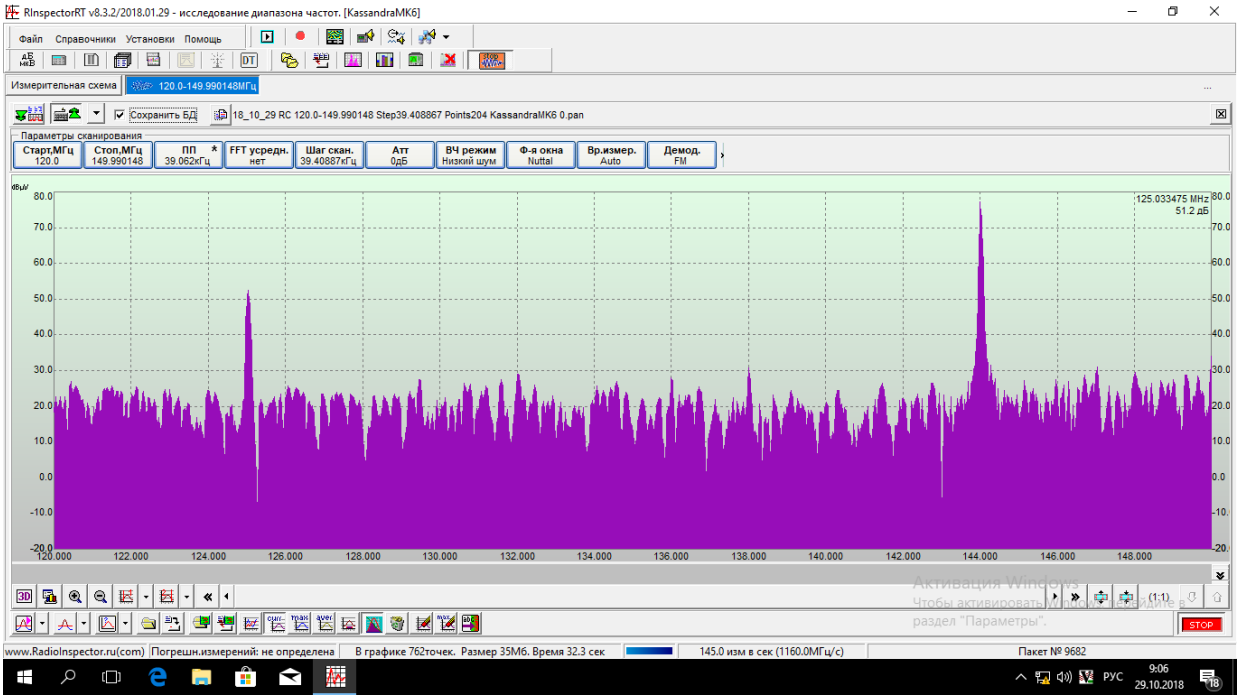

Рис. 7. Имитация радиосигнала модуляции NFM на частоте 144 МГц

Также можно имитировать транковую связь (системы подвижной радиосвязи, которые основаны на тех же принципах, что и обычные телефонные сети) на частотах 144 МГц или 433 МГц, используя дельта-модуляцию.

На частоте 1,2 ГГц можно моделировать радионавигационные системы гражданской авиации. «Шиповник-2» также позволяет смоделировать сигнал беспроводной связи Wi-Fi на частоте 2,4 ГГц, что очень важно в настоящее время, так как беспроводные связи сейчас используются повсеместно.

Все возможные варианты моделирования ситуаций несанкционированного съёма конфиденциальной информации по техническому каналу при помощи многофункционального имитатора сигналов «Шиповник-2» представлены в таблице 2, в которой представлены два источника сигнала «СВИП» и «микрофон» и возможные модуляции их сигналов на частотах 144 МГц, 433 МГц, 1,2 ГГц, 2,4 ГГц.

Таблица 2. Варианты моделирования ситуаций НСКИ при помощи «Шиповник-2»

	144 МГц	433 МГц	1,2ГГц	2,4ГГц
СВИП	ЧМ	ЧМ	ЧМ	ЧМ
	Дельта мод.	Дельта мод.	Дельта мод.	Дельта мод.
	ППРЧ	ППРЧ	ППРЧ	ППРЧ
	ШПРС	ШПРС	ШПРС	ШПРС
Микрофон	ЧМ	ЧМ	ЧМ	ЧМ
	Дельта мод.	Дельта мод.	Дельта мод.	Дельта мод.
	ППРЧ	ППРЧ	ППРЧ	ППРЧ
	ШПРС	ШПРС	ШПРС	ШПРС

В данной таблице не представлены возможные ситуации НСКИ при подключении к «Шиповник-2» внешних устройств, при подключении которых моделирование возможных ситуаций будет зависеть от технических характеристик устройств.

Технология обнаружения НСКИ с использованием комплекса «Кассандра К6»

Процесса обнаружения устройств несанкционированного съема конфиденциальной информации с передачей ее по техническим каналам проводится комплексами мониторинга технических каналов утечки информации. К таким комплексам относятся комплексы радиомониторинга. Такие комплексы помогают обнаружить сигналы, по которым может происходить утечка информации.

К таким комплексам относится комплекс радиомониторинга «Кассандра К6». Комплекс позволяет проводить постоянный, периодический или оперативный мониторинг радиообстановки для выявления несанкционированных радиоизлучений со сложными алгоритмами скрытия информации, анализ цифровых стандартов связи. Комплекс «Кассандра К6» работает с программным обеспечением «*RadioInspector*», что позволяет проводить мониторинг радиоизлучений и выявлять каналы несанкционированного съема информации.

При моделировании ситуации утечки информации с использование имитатора сигналов «Шиповник-2» наблюдались графики сигналов в программе *RadioInspector RT*. Так, например, при моделировании сигнала на частоте 144 МГц с модуляцией «дельта – модуляция» наблюдался график, имеющий вид амплитуды. График имел в вершине небольшое раздвоение, которое сложно было зафиксировать, так как смена частоты (небольшое отклонение от заданной имитатором частоты) происходило в доли секунды. График представлен на рисунке 8.

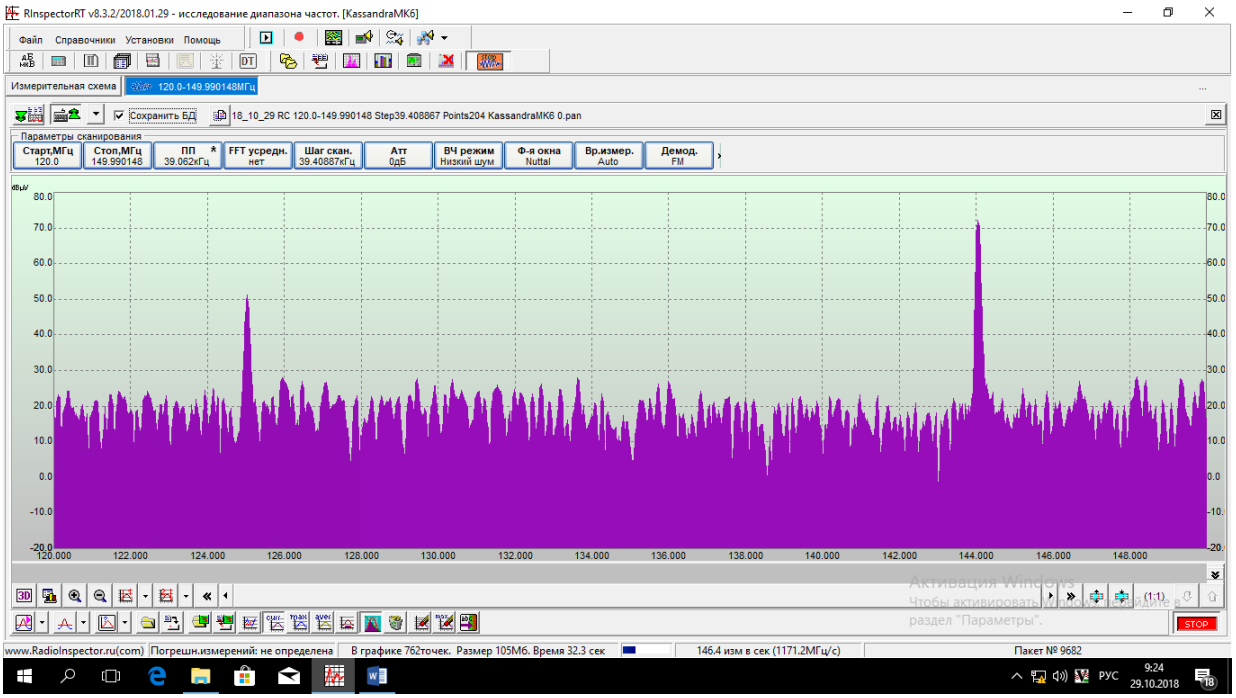

Рис. 8. Моделирование сигнала с частотой 144 МГц и модуляцией «дельта-модуляция»

Также при моделировании закладного устройства, работающего на частоте 144 МГц с модуляцией перестраиваемой псевдослучайным образом рабочей частоты (ППРЧ), были получены графики, на которых амплитуда меняла свою частоту в диапазоне 144-146 МГц. Так же менялась мощность сигнала. Зафиксировать частоту было сложно, т. к. скорость пристраивания частоты происходило быстрее, чем скорость сканирования.

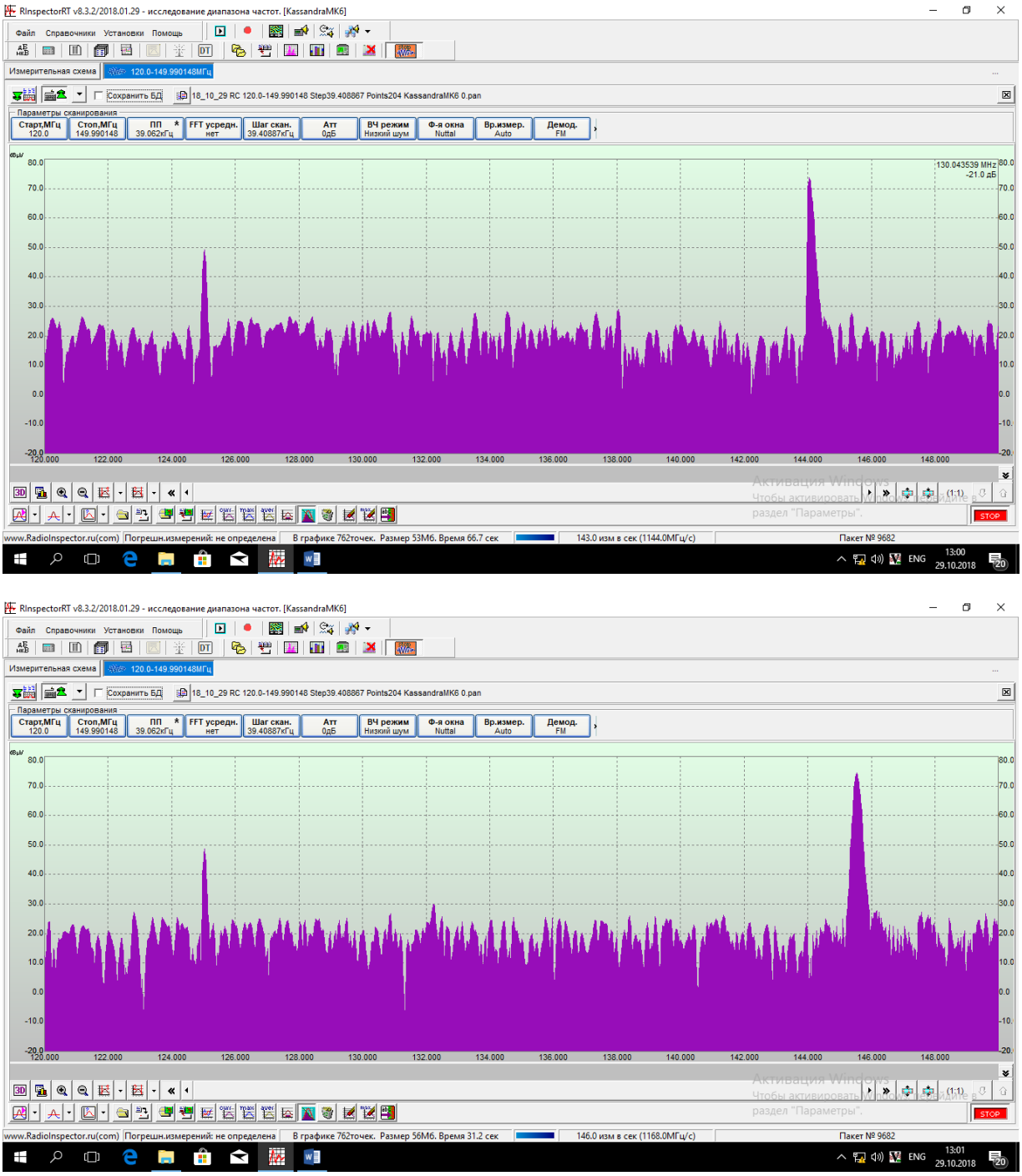

Рис. 9. Моделирование сигнала с частотой 144 МГц и модуляцией ППРЧ

При помощи комплекса «Кассандра К6» так же был проведен анализ сигналов, которые имитирует многофункциональный имитатор сигналов «Шиповник-2». На основе полученных данных был проведен анализ работы имитатора. Результаты представлены в таблице 3.

Таблица 3. Результаты анализа работы имитатора сигналов «Шиповник-2» при помощи комплекса радиомониторинга «Кассандра К6»

	У-ЧМ	Ш-ЧМ	ДЕЛЬТА МОДУЛЯЦИЯ	ЧМ-ЧМ	ППРЧ	ШПРС
144 МГц	частота стабильная, амплитуда не меняет своего положения, частота полностью поглощается при создании шума	в отличие от у-чм амплитуда незначительно шире и небольшое увеличение мощности (дБ)	при сканирование данная модуляция отображается на графике как амплитуда, имеющая раздвоение в вершине	мощность данной модуляции выше всех представленных модуляций имитатора	частота в доли секунды меняется по ± 2 МГц. Данную частоту можно обнаружить при создании шума, так как скорость перестраивания быстрее скорости сканирования	частота постоянно меняется в диапазоне ± 4 МГц и по мощности меньше ППРЧ. В отличие от ППРЧ шумом поглощается полностью
433 МГц	при запуске имитатора помимо фиксированной частоты возникают побочные частоты в диапазоне 420-460 МГц меньшей мощности	при запуске имитатора помимо фиксированной частоты возникают побочные частоты в диапазоне 420-460 МГц меньшей мощности	при запуске имитатора помимо фиксированной частоты возникают побочные частоты в диапазоне 420-460 МГц меньшей мощности	при запуске имитатора помимо фиксированной частоты возникают побочные частоты в диапазоне 420-460 МГц меньшей мощности	График "прыгающий" в диапазоне 423 - 440 МГц,	График "прыгающий" в диапазоне 423 - 440 МГц, мощность излучения меньше чем у ППРЧ
1.2 ГГц	при запуске имитатора помимо фиксированной частоты возникают побочные частоты в диапазоне 1206 - 1228 МГц меньшей мощности, более точный сигнал на частоте 1216 МГц, не поглощается полностью шумом	при запуске имитатора помимо фиксированной частоты возникают побочные частоты в диапазоне 1206 - 1228 МГц меньшей мощности, более точный сигнал на частоте 1216 МГц, не поглощается полностью шумом	при запуске имитатора помимо фиксированной частоты возникают побочные частоты в диапазоне 1206 - 1228 МГц меньшей мощности, более точный сигнал на частоте 1216 МГц, не поглощается полностью шумом	при запуске имитатора помимо фиксированной частоты возникают побочные частоты в диапазоне 1206 - 1228 МГц меньшей мощности, более точный сигнал на частоте 1216 МГц, не поглощается полностью шумом	График "прыгающий" в диапазоне 1204 - 1235 МГц,	Амплитуда расширена в диапазоне 1214 - 1221 МГц, точную частоту определить сложно, так как график "прыгающий"

2.4 ГГц	при запуске имитатора помимо фиксированной частоты возникают побочные частоты в диапазоне 2400 - 2450 МГц меньшей мощности, более точный сигнал на частоте 2449 МГц, не поглощается полностью шумом	при запуске имитатора помимо фиксированной частоты возникают побочные частоты в диапазоне 2400 - 2450 МГц меньшей мощности, более точный сигнал на частоте 2449 МГц, не поглощается полностью шумом	при запуске имитатора помимо фиксированной частоты возникают побочные частоты в диапазоне 2400 - 2450 МГц меньшей мощности, более точный сигнал на частоте 2449 МГц, не поглощается полностью шумом. Имеет еле заметное колебание	при запуске имитатора помимо фиксированной частоты возникают побочные частоты в диапазоне 2400 - 2450 МГц меньшей мощности, более точный сигнал на частоте 2449 МГц, не поглощается полностью шумом	перестройка частоты в очень маленьком диапазоне,	диапазон частоты значительно увеличивается

Можно заметить, что при моделировании сигналов при помощи «Шиповник-2» большую роль играет модуляция сигнала при отображении сигнала в программе *RadioInspector*. Совершенно очевидно, что изменение частоты является ключевым, так как средства несанкционированного съема конфиденциальной информации определяются в основном своей рабочей частотой.

Заключение

Контроль радиообстановки крайне важен, так как утечка конфиденциальной информации по техническим каналам трудно выявить. О том, что произошла утечка информации можно понять только после того, как информация стала известна посторонним. Поэтому очень важно проводить радиомониторинг объекта.

Специалисты по защите технических каналов утечки информации необходимы для сохранение государственной, коммерческой тайны, конфиденциальной информации, персональных данных в различных организациях. И подготовка этих специалистов крайне важна. Для того, чтобы специалист мог предвидеть различного рода каналы несанкционированного съема конфиденциальной информации, необходимо моделировать ситуации утечки информации. Отлично подходят имитационные средства, среди которых большую нишу занимают многофункциональные имитаторы сигналов.

Так же имитационные средства позволяют провести анализ защищенности объекта от несанкционированного съема конфиденциальной информации. Подобный анализ необходим для более полного обеспечения информационной безопасности.

Список литературы

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. — С. 436. — ISBN 978-59901488-1-9.
2. Блиялкин П. А., Смоленков А. В. Выявление электронных устройств перехвата акустической речевой информации, построенных на базе средств беспроводной связи // Молодой ученый. — 2016. — №14. — С. 124-128. — [Электронный ресурс]. URL: https://moluch.ru/archive/118/32820/.
3. Кривцун А.В. Комплекс радиомониторинга «Кассандра». – [Электронный ресурс]. URL: https://cyberleninka.ru/article/v/kompleks-radiomonitoringa-kassandra.
4. Проселков Л.С., Кравченко А.Н. – [Электронный ресурс]. URL: http://www.findpatent.ru/patent/220/2207586.html © FindPatent.ru - патентный поиск, 2012-2018.
5. Технические средства поиска каналов утечки информации. Имитаторы сигналов. – [Электронный ресурс]. URL: https://nelk.ru/catalog/tekhnicheskie_sredstva_poiska_kanalov_utechki_informatsii/imitatory_signalov/.
6. Методические рекомендации по формированию аналитического прогноза по укомплектованию подразделений по обеспечению безопасности значимых объектов критической информационной инфраструктуры, противодействию иностранным техническим разведкам и технической защиты информации подготовленными кадрами, утвержденных ФСТЭК России 30 сентября 2016 г. (в редакции от 28 февраля 2018 г.).
7. Информационное сообщение. О внесении изменений в примерные программы профессиональной переподготовки и повышения квалификации специалистов, работающих в области технической защиты информации, утвержденный ФСТЭК России от 31 мая 2018 г. № 240/11/2426. – [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obuchenie-spetsialistov/1600-informatsionnoe-soobshchenie-fstek-rossii-ot-31-maya-2018-g-n-240-11-2426?highlight=WzI0MCwxMSwyNDI2LCIyNDAgMTEiLCIyNDAgMTEgMjQyNiIsIjExIDI0MjYiXQ==.
8. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите инфор-

мации. — [Электронный ресурс]. URL https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument.

9. Приказ Минобрнауки России от 01.12.2016 N 1515 «Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата)».