МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт Факультет приборостроения, информационных технологий и электроники	Кафедра «Информационная безопасность систем и технологий»
Специальность 10.05.03 –	Информационная безопасность автоматизированных систем
Специализация -	Защищенные автоматизированные системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

МЕТОДИКА ОБЕСПЕЧЕНИЯ ЗАЩИТЫ АО «НПП «РУБИН» ОТ УТЕЧЕК ИНФОРМАЦИИ ПО КАНАЛАМ СОТОВОЙ СВЯЗИ И БЕСПРОВОДНЫМ КАНАЛАМ ПЕРЕДАЧИ ДАННЫХ

Студент _____ Авдеев Сергей Алексеевич

Руководитель _____ Сергеев В.О.

Нормоконтролёр _____ Фатеев А.Г.

Рецензент инженер 2 категории АО «НПП «Рубин» _____ Яшин Е.В.

Работа допущена к защите (протокол заседания кафедры от 15.06.20 № 13)

Заведующий кафедрой _____ С.Л. Зефиров

Работа защищена с отметкой хорошо (протокол заседания ГЭК от 25.06.20г № 1)

Секретарь ГЭК _____ А.П. Иванов

Пенза 2020

Оглавление

Введение.....5
1 Нормативно-правовая база защиты информации.....7
2 Стандарты беспроводной передачи данных и беспроводных телефонных технологий.....10
2.1 Стандарты беспроводной передачи данных.....10
2.2 Стандарты беспроводных телефонных технологий.....16
3 Коллективный договор и нормативно-правовая документация АО «НПП «Рубин».....19
4 Обзор методов и средств защиты от утечки информации по каналам сотовой связи и беспроводным каналам передачи данных.....21
4.1 Общая информация о мерах защиты.....21
4.2 Технические меры защиты от утечки информации по каналам сотовой связи и беспроводным каналам передачи данных.....21
4.3 Организационные меры защиты от утечки информации по каналам сотовой связи и беспроводным каналам передачи данных.....29
5 Разработка методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных.....32
5.1 Область применения методики.....32
5.2 Цель разработки методики.....32
5.3 Выбор защитных мер, использующихся в методике.....32
5.4 Определение угроз.....33
5.5 Определение уязвимостей.....33
5.6 Определение нарушителей.....34
5.7 Описание алгоритма выбора защитных мер методики.....34
5.8 Выявленные наборы защитных мер в зависимости от условий функционирования организации.....39
5.9 Описание критерия эффективности методики.....47

5.10 Описание процедуры анализа эффективности методики.....48
6 Проведение и оценка практического исследования эффективности методики и составление рекомендаций по практическому применению методики.....50
6.1 Проведение практического исследования эффективности методики...50
6.2 Оценка результатов практического исследования эффективности методики.....55
6.3 Рекомендации по практическому применению методики.....56
7 Вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....59
Заключение.....61
Список используемых источников.....63
Приложение А Схема возможной утечки информации по каналам беспроводной передачи данных.....66
Приложение Б Перечень организационных мер, содержащихся в методике……67
Приложение В Перечень технических мер, содержащихся в методике.....68
Приложение Г Алгоритм выбора мер защиты.....69
Приложение Д Методика обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи.....70
Приложение Е Схема размещения средств защиты информации.....87
Приложение Ж Результаты практического исследования эффективности методики.....88
Приложение И Рекомендации по практическому применению методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи.....89
Приложение К Протокол проверки ВКР в системе Антиплагиат.....94

Введение

Сегодня беспроводные технологии получили мощное развитие из-за того, что они доступны для подключения практически для всех у кого есть устройство, которое может к ним подключаться. С учетом повсеместного использования устройств сотовой связи и средств беспроводной передачи данных, не возможно гарантировать защиту информации от атак злоумышленников, а также исключить внутренние угрозы от персонала, использующего их. Таким образом, при использовании средств сотовой связи в организациях всегда присутствует риск утечки информации.

Актуальность данной темы обусловлена тем, что хотя на территории АО «НПП «Рубин» локальные беспроводные сети, такие как Wi-Fi, WiMax, Bluetooth, в целях повышения безопасности, не используются, но при этом использование устройств сотовой связи на территории организации никак не отслеживается, следовательно, возможны утечки информации. Отсюда возникает необходимость разработки методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных.

Целью данной выпускной квалификационной работы является разработка методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных и разработка рекомендаций для практического применения данной методики по итогам практического исследования для проверки её эффективности.

Для достижения цели выпускной квалификационной работы в ней должны быть рассмотрены следующие вопросы:

— составление методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных;

— описание критерия эффективности методики;

— описание процедуры анализа эффективности методики;

— практическое исследование методики на эффективность;

— составление рекомендаций по практическому применению методики.

1 Нормативно-правовая база защиты информации

До рассмотрения стандартов беспроводной передачи данных необходимо проанализировать нормативно-правовую базу защиты информации в Российской Федерации.

Основным источником права в области обеспечения информационной безопасности Российской Федерации является Конституция Российской Федерации [1].

Согласно Конституции Российской Федерации:

— каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 23);

— сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (статья 24);

— каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом (статья 29);

— каждый имеет право на достоверную информацию о состоянии окружающей среды (статья 42).

Одним из основных способов обеспечения информационной безопасности Российской Федерации является защита информации.

Система нормативных правовых актов Российской Федерации в области защиты информации включает в себя законы, подзаконные акты, а также ряд международных договоров Российской Федерации, которые также являются согласно Конституции Российской Федерации составной частью ее правовой системы.

Основными законодательными актами в данной области являются:

— законы Российской Федерации “О средствах массовой информации”

[2] и “О государственной тайне” [3];

— федеральные законы “Об информации, информационных технологиях и защите информации” [4], “О связи” [5], “Об обязательном экземпляре документов” [6].

Помимо этого, нормы, которые регулируют общественные отношения в области защиты информации, имеются в таких кодексах, как Гражданский [7], Гражданско-процессуальный [8], Уголовный [9], Уголовно-процессуальный [10], Налоговый [11], Семейный [12] и других, а также в законодательных актах, устанавливающих правовой статус государственных органов, например в законе “О Центральном банке Российской Федерации” [13] и в ряде других федеральных законов.

Основным законом, регулирующим отношения в области защиты информации, является Федеральный закон «Об информации, информационных технологиях и защите информации», принятый в 2006 году [4].

Предметом регулирования данного Закона являются общественные отношения, возникающие в трех направлениях:

— формирование и использование информационных ресурсов;

— создание и использование информационных технологий и средств их обеспечения;

— защита информации, прав субъектов, участвующих в информационных процессах и информатизации.

В Законе отражены вопросы, связанные с порядком сертификации информационных систем, технологий, средств их обеспечения, обращением с персональными данными и лицензированием деятельности по формированию и использованию информационных ресурсов.

Основными целями защиты информации являются:

— предотвращение утечки, хищения, утраты, искажения и подделки информации (защите подлежит любая информация, в том числе и открытая);

— предотвращение угроз безопасности личности, общества и государства (то есть защита информации является одним из способов обеспечения информационной безопасности Российской Федерации);

— защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

— сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством.

Закон определяет, кем и в отношении каких сведений устанавливается режим защиты информации. При этом порядок защиты государственной тайны и персональных данных устанавливается федеральными законами. Для другой информации с ограниченным доступом режим защиты устанавливает собственник информационных ресурсов.

2 Стандарты беспроводной передачи данных и беспроводных телефонных технологий

2.1 Стандарты беспроводной передачи данных

Несанкционированный доступ к информации с ограниченным доступом может осуществляться, в том числе по беспроводным каналам передачи данных.

В настоящее время существует множество беспроводных технологий, которые чаще всего известны по их маркетинговым названиям, таким как Wi-Fi, WiMAX, Bluetooth. Область применения каждой технологии определяется её характеристиками.

WPAN (англ. Wireless personal area network) беспроводная сеть, предназначенная для организации беспроводной связи между различного типа устройствами на ограниченной площади. Стандарты, определяющие методы функционирования сети, описаны в семействе спецификаций IEEE 802.15. Далее будут рассмотрены два наиболее перспективных стандарта: Bluetooth и ZigBee.

Bluetooth — производственная спецификация беспроводных персональных сетей. Принцип действия основан на использовании радиоволн. Радиосвязь Bluetooth осуществляется в ISM-диапазоне (Industry, Science and Medicine), который имеет частоту волн от 2,4 до 2,4835 ГГц, и в большинстве стран имеет 79 частот для передачи. ISM-диапазон используется в бытовых приборах и беспроводных сетях, а также является свободным от лицензирования. В Bluetooth применяется метод расширения спектра со скачкообразной перестройкой частоты.

Информация передаётся посредством хаотичной смены частот около 1600 раз в секунду, которые в определённый момент знают времени только передатчик и приёмник со своими идентификационными ключами. Это способствует устойчивости к помехам, а также минимальный шанс на то, что

несколько устройств будут мешать друг-другу из-за перехлёстывания частот. Таким образом, это делает данный стандарт одним из самых безопасных, так как подключиться к устройству становится практически невозможно без разрешения получателя на доступ к идентификационным ключам. Безопасности также способствует малый радиус действия. Для взлома необходимо продолжительное время находиться около цели, что может вызвать подозрения.

Существуют следующие спецификации Bluetooth:

— Bluetooth 1.0 – первая версия несла множество недостатков в плане совместимости устройств разных производителей. Информация могла передаваться на несколько метров, а также была невозможна реализация анонимного соединения на протокольном уровне;

— Bluetooth 1.1 — добавлена поддержка нешифрованных каналов и индикация уровня сигнала;

— Bluetooth 1.2 — ускорен процесс обнаружения и подключения устройств, реализована сетевая анонимности, а также увеличена помехоустойчивость. Устройства, поддерживающие данный стандарт имеют возможность передачи речевых сообщений и стереозвука посредством Bluetooth;

— Bluetooth 2.0 — был представлен в 2007 году. Основным нововведением было увеличение скорости передачи данных до 2,3 Мбит/с в среднем. Также было добавлено несколько улучшений увеличивающих стабильность передачи данных, безопасность и совместимость;

— Bluetooth 2.1 — был представлен в августе 2007 года. Для этого стандарта была добавлена энергосберегающая технология Sniff Subrating, которая уменьшает энергопотребление в несколько раз. Улучшена безопасность и скорость идентификации устройств. Также появилась возможность обновления ключа шифрования без разрыва соединения;

— Bluetooth 3.0 + HS — был представлен в апреле 2009 года. Было добавлено высокоскоростное дополнение к семейству стандартов IEEE 802.11 Asymmetry Multiprocessing Programming, которое увеличивало скорость передачи данных до 24 Мбит/с, но при этом при этом увеличивает энергопотребление;

— Bluetooth 4.0 — был представлен в июне 2010 года. Состоит из трех протоколов: высокоскоростной Bluetooth (на основе Wi-Fi), классический Bluetooth (на основе предыдущих протоколов) и Bluetooth с низким энергопотреблением. Главной его особенностью является уменьшенное энергопотребление из-за того, что сигнал передается непостоянно. Приёмник находится наготове и включается только тогда, когда ему подаётся сигнал с другого устройства, в остальное время он бездействует. Время установления соединения составляет примерно 5 миллисекунд, скорость передачи до 1 Мбит/с на расстоянии до 100 метров, а также обеспечивает безопасность благодаря шифрованию 128 бит AES;

— Bluetooth 4.1 — был представлен в конце 2013 года. Для этого стандарта реализована защита от взаимных помех с мобильной связью четвертого поколения LTE (англ. Long-Term Evolution) путем автоматического координирования передачи пакетов данных;

— Bluetooth 4.2 — был представлен в конце 2014 года. Для данного стандарта характерно повышение конфиденциальности и скорости передачи данных;

— Bluetooth 5.0 — был представлен в июне 2016 года. Для данной спецификации был увеличен радиус передачи в 4 раза и скорость передачи в 2 раза;

— Bluetooth 5.1 — отличительной особенностью является возможность определение местоположения и направление передачи с максимальной точностью;

— Bluetooth 5.2 — был представлен 6 января 2020 года. В этой

спецификации реализованы возможности по динамической оптимизации мощности для связи между подключенными устройствами, а также функция для передачи данных с привязкой ко времени на одно или несколько устройств, а также параллельно передавать данные на неограниченное количество устройств.

ZigBee — название набора сетевых протоколов верхнего уровня, использующих маленькие маломощные радиопередатчики, основанные на стандарте IEEE 802.15.4. Этот стандарт описывает беспроводные персональные вычислительные сети (WPAN). ZigBee нацелена на приложения, которым требуется длительное время автономной работы от батарей и высокая безопасность передачи данных при небольших скоростях передачи данных.

WLAN - эта категория беспроводной сети предназначена для связи между собой различных устройств, подобно LAN на основе витой пары или оптоволокна, и при этом характеризуется высокой скоростью передачи данных на относительно небольшие расстояния. Взаимодействие устройств описывается семейством стандартов IEEE 802.11, включающим в себя более 20 стандартов передачи данных:

— 802.11 — изначальный 1 Мбит/с и 2 Мбит/с, 2,4 ГГц и ИК стандарт (1997);

— 802.11a — 54 Мбит/с, 5 ГГц стандарт (1999, выход продуктов в 2001);

— 802.11b — улучшения к 802.11 для поддержки 5,5 и 11 Мбит/с (1999);

— 802.11c — процедуры операций с мостами; включен в стандарт IEEE 802.1D (2001);

— 802.11d — интернациональные роуминговые расширения (2001);

— 802.11e — улучшения: QoS, пакетный режим (packet bursting) (2005);

— 802.11F — Inter-Access Point Protocol (2003);

— 802.11g — 54 Мбит/с, 2,4 ГГц стандарт (обратная совместимость с b) (2003);

— 802.11h — распределённый по спектру 802.11a (5 GHz) для совместимости в Европе (2004);

— 802.11i — улучшенная безопасность (2004);

— 802.11j — расширения для Японии (2004);

— 802.11k — улучшения измерения радиоресурсов;

— 802.11l — зарезервирован;

— 802.11m — поправки и исправления для всей группы стандартов 802.11;

— 802.11n (WiFi 4) — увеличение скорости передачи данных (600 Мбит/с). от 2,4 до 2,5 ГГц или 5 ГГц. Обратная совместимость с 802.11a/b/g (сентябрь 2009);

— 802.11o — зарезервирован;

— 802.11p — WAVE — Wireless Access for the Vehicular Environment (беспроводной доступ для среды транспортного средства);

— 802.11q — зарезервирован, иногда его путают с 802.1Q;

— 802.11r — быстрый роуминг;

— 802.11s — ESS (Extended Service Set — расширенный набор служб; Mesh Network — многосвязная сеть);

— 802.11T — Wireless Performance Prediction (WPP, предсказание производительности беспроводного оборудования) — методы тестов и измерений;

— 802.11u — взаимодействие с не-802 сетями (например, сотовыми);

— 802.11v — управление беспроводными сетями;

— 802.11w — Protected Management Frames (защищенные управляющие фреймы);

— 802.11x — зарезервирован и не будет использоваться. Не нужно путать со стандартом контроля доступа IEEE 802.1X;

— 802.11y — дополнительный стандарт связи, работающий на частотах 3,65-3,70 ГГц. Обеспечивает скорость до 54 Мбит/с на расстоянии до 5000 м на открытом пространстве;

— 802.11ac (WiFi 5) — новый стандарт IEEE. Скорость передачи данных — до 6,77 Гбит/с для устройств, имеющих 8 антенн. Утверждён в январе 2014 года;

— 802.11ad — новый стандарт с дополнительным диапазоном 60 ГГц (частота не требует лицензирования). Скорость передачи данных — до 7 Гбит/с;

— 802.11ax (WiFi 6) — новый стандарт (до 10747 Мбит/с).

IEEE 802.11a это один из стандартов беспроводных локальных сетей, который описывает принципы функционирования устройств в частотном диапазоне ISM по принципу мультиплексирования с разделением по ортогональным частотам. Полоса подразделяется на три рабочие зоны, каждая из которых шириной 100 МГц, и для каждой зоны определена максимальная излучаемая мощность 50 мВт, 250 мВт, 1 Вт соответственно.

В закрытых помещениях радиус действия устройств составляет около 12 метров на скорости 54 Мбит/с, до 90 метров при скорости 6 Мбит/с, а в открытых помещениях или зоне прямой видимости - около 30 метров (54 Мбит/с), и до 300 метров при 6 Мбит/с. Также возможен обмен данными в Turbo 802.11a на скоростях до 108 Мбит/с благодаря внедрению технологий ускорения.

IEEE 802.11b первый стандарт, получивший широкое распространение (первоначально носил торговую марку Wi-Fi), которая дала возможность создавать беспроводные локальные сети в офисах, домах, квартирах. Эта

спецификация описывает принципы взаимодействия устройств в диапазоне от 2,4 до 2,4835 ГГц. Стандартом определены четыре обязательные скорости 1, 2, 5,5 и 11 Мбит/с.

IEEE 802.11g стандарт беспроводной сети, который является развитием 802.11b и использует тот же частотный диапазон, а также предполагает обратную совместимость с устройствами, отвечающими стандарту 802. В стандарте предусмотрены шесть обязательных скоростей 1, 2, 5,5, 6, 11, 12, 24 Мбит/с, и четыре опциональных 33, 36, 48 и 54 Мбит/с. Радиус зоны действия увеличен в закрытых помещениях до 30 метров (54 Мбит/с), и до 91 метра при скорости 1 Мбит/с, в пределах же прямой видимости связь доступна на расстоянии 120 метров со скоростью 54 Мбит/с, а при удалении на 460 метров возможна работа со скоростью 1 Мбит/с.

IEEE 802.11n — версия стандарта 802.11 для сетей Wi-Fi. Скорость передачи данных увеличивается в 4 раза по сравнению с устройствами стандарта 802.11g , при условии использования устройств в режиме 802.11n с другими устройствами в этом режиме. Устройства 802.11n работают в диапазонах от 2,4 до 2,5 ГГц или 5,0 ГГц.

WMAN — беспроводные сети масштаба города. Предоставляют собой широкополосный доступ к сети через радиоканал. Описываются семейством стандартов IEEE 802.16, в которых используется диапазон частот от 10 до 66 ГГц. Так как это сантиметровый и миллиметровый диапазон, то необходимо условие «прямой видимости». Стандарт определяет пропускную способность 120 Мбит/с на каждый канал в 25 МГц.

2.2 Стандарты беспроводных телефонных технологий

2G. Основными стандартами 2G являются GSM 900/1800 и CDMA 450. И GSM, и CDMA используются для голосовых звонков, текстовых сообщений, а также мобильного доступа в интернет. В стандарте GSM используются частоты 900 и 1800 МГц. Поскольку все мобильные телефоны являются дуплексными

устройствами, то для связи используются сразу две частоты, одна для приема, вторая для передачи данных. CDMA использует две частоты в диапазонах 450 и 850 МГц, с таким же дуплексным распределением.

XRTT — 2.5G. Технология передачи цифровых данных, которая основана на технологии CDMA. Использует принцип передачи с коммутацией пакетов. XRTT использует лицензируемый радиочастотный диапазон и, подобно другим мобильным технологиям, широко распространена. Теоретически возможная скорость передачи 144 Кбит/сек, но на практике реальная скорость менее 60 Кбит/сек.

3G**.** Все цифровые системы второго поколения основаны на методе множественного доступа с временным разделением каналов. Принципиальное отличие сетей 3G от предыдущих поколений заключается в использовании технологии множественного доступа с кодовым разделением каналов (CDMA). Наибольшее распространение в России и странах Европы получил стандарт UMTS, который имеет 2 наиболее распространенные частоты 900 МГц и 2100 МГц, на которых скорость передачи составляет до 10 Мбит/с и до 21 Мбит/с соответственно. Основной проблемой частоты передачи данных 2100 МГц является то, что распространение волны значительно ухудшается из-за препятствий, в том числе и из-за высокой растительности. При этом волны передачи данных 900 МГц более устойчива к препятствиям, но имеет ниже скорость передачи.

4G. Поколение мобильной связи с повышенными требованиями. К четвёртому поколению принято относить перспективные технологии, позволяющие осуществлять передачу данных со скоростью, превышающей 100 Мбит/с для подвижных абонентов и 1 Гбит/с для стационарных абонентов[14].

Технологии LTE Advanced (LTE-A) была официально признана беспроводным стандартом связи четвёртого поколения 4G Международным союзом электросвязи на конференции в Женеве в 2012 году. В данной технологии поддерживаются гибкие варианты полосы пропускания с несущей

частотой от 1,4 МГц до 20 МГц и дуплексная передача с разделением по частоте и по времени, где при разделении по времени вся пропускная способность попеременно отдается на загрузку или выгрузку данных, а при разделении по частоте загрузка данных идет на одной частоте, а выгрузка на другой.

DECT — технология беспроводной связи на частотах от 1880 до 1900 МГц с модуляцией GMSK, которая используется в современных радиотелефонах. DECT является стандартом с частотно-временным разделением каналов. Также стандарт DECT предусматривает меры защиты доступности телекоммуникационных систем, характерной для беспроводной связи. Реализация беспроводной связи происходит как в рамках аналоговой телефонии, так и IP-телефонии. Корпоративные радиотелефоны, работающие по принципу Voice over IP, являются одним из самых востребованных и быстрорастущих сегментов рынка IP-телефонии [15].

Схема возможной утечки информации по каналам беспроводной передачи данных представлена в приложении А.

3 Коллективный договор и нормативно-правовая документация АО «НПП «Рубин»

«Коллективный договор между работодателем и работниками Акционерного общества «Научно-производственное предприятие «Рубин» на 2017-2020 годы», принятый на 34-ой профсоюзной конференции 10 ноября 2017 года, не содержит в себе понятия «сотовый телефон», «мобильный телефон», «устройство связи», а также не имеет пунктов об их применении или запрете на территории предприятии. Кроме того, не раскрываются требования о соблюдении требований режима секретности, установленного на предприятии, а также о неразглашении сведений, полученных в силу служебного положения и составляющих государственную или коммерческую (служебную) тайну, распространение которой может нанести вред предприятию и/или его работникам, которые установлены в разделе 3 «Основные права, обязанности и ответственность работников» Правил внутреннего трудового распорядка Акционерного общества «Научно-производственное предприятие «Рубин» приложения №1 «Коллективного договора между работодателем и работниками Акционерного общества «Научно-производственное предприятие «Рубин» на 2017-2020 годы».

Положение о порядке организации и проведении работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну в АО «НПП «Рубин» также не регламентирует использование или не имеет запрета на использование устройств сотовой связи на территории предприятия.

Устройства сотовой связи, используемые работниками АО «НПП «Рубин» и лицами, имеющими временный пропуск на территорию АО «НПП «Рубин», могут быть средствами реализации угрозы утечки конфиденциальной информации по каналам сотовой связи и беспроводным каналам передачи

данных как целенаправленно, так и при случайном попадании конфиденциальной информации в разговор.

Таким образом, в результате реализации разрабатываемой методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных в коллективный договор на следующий календарный период должны быть добавлены правила использования устройств сотовой связи на территории АО «НПП «Рубин».

4 Обзор методов и средств защиты от утечки информации по каналам сотовой связи и беспроводным каналам передачи данных

4.1 Общая информация о мерах защиты

В устройствах сотовой связи передача данных может осуществляться по различным каналам, в соответствии с различными стандартами беспроводной передачи данных. Для того, чтобы обеспечить защиту от утечки информации посредством устройств сотовой связи, необходимо применение как организационных, так и технических мер защиты в комплексе.

Техническими мерами защиты информации называют меры, которые направленны на предотвращение утечки конфиденциальной информации с помощью технических средств.

Организационными мерами защиты информации называют меры, которые направленны на предотвращение утечки конфиденциальной информации путем регламентации производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение информацией и проявление внутренних и внешних угроз.

4.2 Технические меры защиты от утечки информации по каналам сотовой связи и беспроводным каналам передачи данных

К техническим мерам защиты от утечки информации по каналам сотовой связи можно отнести различные устройства блокирования работы систем мобильной связи. Они могут быть непрерывного действия или же включаться лишь во время попыток передачи информации устройствами мобильной связи. Оба вида этих устройств блокирования работы систем мобильной связи имеют свои недостатки и достоинства [16].

Устройства блокирования работы систем мобильной связи непрерывного действия всегда активны и перекрывают своей работой лишь строго

определенную полосу частот. В сравнении с устройствами, которые включаются лишь при начале передачи сигнала устройствами, они обладают меньшей стоимостью и большей простотой в эксплуатации. При этом устройства такого типа имеют и свои недостатки. К ним можно отнести постоянно воздействие излучения на людей, а также сравнительно небольшой ресурс автономной работы из-за постоянной работы устройства при аккумуляторном питании.

Устройства блокирования работы систем мобильной связи, которые включаются лишь при начале передачи сигнала не имеют постоянного излучения, которое отрицательно сказывается на работоспособности персонала объекта, где данные устройства установлены, а также имеют длительное время автономной работы из-за пребывания в режиме, при котором лишь отслеживают начало передачи данных по различным частотам и включаясь лишь при обнаружении этой передачи. При этом данные устройства имеют высокую стоимость и, кроме того, тяжелы в обслуживании и настройке.

Также все устройства блокирования работы систем мобильной связи можно разделить на два типа по способу постановки помехи: на приемный сигнал, на передающий сигнал устройства сотовой связи. Чаще используется первый тип, так как постановка помехи на передающий сигнал имеет более сложно реализуемую схему. Для подавления приемного сигнала формируется сигнал с равномерной характеристикой по частоте и затем передается устройству сотовой связи. В результате, на вход устройства поступает сигнал от базовой станции, а также сигнал помехи от устройства блокирования работы систем мобильной связи с более высокой частотой, что ухудшает соотношение сигнал/шум, что препятствует установлению связи между устройством сотовой связи и базовой станцией.

Кроме того, устройства блокирования работы систем мобильной связи можно разделить на два типа по направленности антенн: всенаправленные и секторные. Устройства блокирования работы систем мобильной связи имеющие всенаправленные антенны имеют меньшую дальность действия, при этом

препятствует работе всех устройств в определенном радиусе. Устройства блокирования работы систем мобильной связи имеющие секторные антенны имеют большую дальность действия, но при этом могут препятствовать работе лишь устройств сотовой связи, которые попадают в сектор действия данного устройства [17].

Большинство современных устройств блокирования работы систем мобильной связи имеют возможность регулировки зоны блокирования работы систем мобильной связи. Из-за высокой стоимости устройств, имеющих большую максимальную дальность действия, экономически нецелесообразно применять их для защиты небольших помещений, в которых обрабатывается информация ограниченного доступа, и небольших территорий, в пределах которых нежелательна работа средств сотовой связи. Поэтому стоит разделить устройства блокирования работы систем мобильной связи по дальности их действия на устройства с большой дальность действия и устройства с малой дальностью действия.

К устройствам с большой дальностью действия можно отнести устройство блокирования работы систем цифровой связи и передачи данных «Торнадо» и устройство блокирования беспроводных цифровых каналов радиосвязи «Тарантул».

Устройство блокирования работы систем цифровой связи и передачи данных «Торнадо» предназначено для блокирования работы устройств, использующих каналы цифровой связи стандартов GSM-900, GSM-1800, E-GSM, CDMA-800, AMPS/N-APS/D-AMPS800, IMT-MC-450, CDMA-2000, IMT-2000/UMTS (3G), DECT, Wi-Fi 2,4 ГГц, Wi-Fi 5 ГГц, Bluetooth, ZigBee, LTE2500, LTE800. Устройство может применяться для технического ограничения использования мобильных телефонов на контролируемых территориях, для защиты информации от утечки с использованием каналов сотовой связи. В зависимости от расстояния до ближайшей базовой станции сотовой связи дальность блокирования абонентских терминалов составляет до 80 метров. Для

защиты территорий с большей площадью может применяться метод пространственного размещения необходимого количества устройств.

В базовом исполнении «Торнадо» представляет функционально законченный блок с внутренней антенной системой и с внешним питанием от сети 220 В. Дополнительно может комплектоваться адаптером питания от бортовой сети автомобиля. Устройство может оснащаться модулем беспроводного дистанционного управления по радио или ИК каналу. Предусмотрена возможность подключения проводного дистанционного управления.

Основными особенностями являются настройка частот подавления, а также размера зоны блокирования для каждого стандарта отдельно.

Внешний вид устройства «Торнадо» представлен на рисунке 1.

Рисунок 1 - Устройство блокирования работы систем цифровой связи и передачи данных «Торнадо»

Устройство блокирования беспроводных цифровых каналов радиосвязи «Тарантул» предназначено для ограничения использования беспроводных цифровых каналов радиосвязи на протяженных объектах. Оно может блокировать работу устройств, использующих каналы цифровой связи стандартов GSM-900, GSM-1800, E-GSM, CDMA-2000, IMT-2000/UMTS (3G),

DECT, Wi-Fi 2,4 ГГц, Wi-Fi 5 ГГц, LTE2500, LTE800.

В зависимости от расстояния до базовых станций возможно блокирование беспроводных цифровых каналов радиосвязи на расстоянии до 200 метров от места размещения средства. Зона блокирования формируется с помощью мультидиапазонных панельных секторных антенн с усилением 9 дБ и секторами излучения 55 градусов в вертикальной плоскости и 70 градусов в горизонтальной плоскости. Внешнее питание от сети 220 В. Изделие имеет возможность настройки уровня выходной мощности с помощью специального программного обеспечения, входящего в комплект поставки.

Внешний вид устройства «Тарантул» представлен на рисунке 2.

Рисунок 2 - Устройство блокирования беспроводных цифровых каналов радиосвязи «Тарантул»

К устройствам с малой дальностью действия можно отнести переносное автономное устройство подавления систем цифровой связи и передачи данных

всех стандартов «Мозаика-7К» и устройство блокирования работы систем цифровой связи «Квартет-С».

Переносное автономное устройство подавления систем цифровой связи и передачи данных всех стандартов «Мозаика-7К» предназначено для блокирования работы всех типов устройств несанкционированного прослушивания и передачи данных, аудио передатчиков и видео передатчиков, использующих стандарты GSM-900/1800, 3G и 4G (LTE), DECT, CDMA, Wi-Fi, Bluetooth, ZigBee.

Устройство имеет встроенную антенну круговой направленности. Максимальный радиус подавления устройство устройством «Мозаика-7К» составляет до 40 метров в зависимости от от условий эксплуатации и мощности сигнала базовых станций. Особенностью данного устройства является его бесшумность и регулировка уровня мощности выходного сигнала в каждой полосе частот.

Внешний вид устройства «Мозаика-7К» представлен на рисунке 3.

Рисунок 3 - Переносное автономное устройство подавления систем цифровой связи и передачи данных всех стандартов «Мозаика-7К»

Устройство блокирования работы систем цифровой связи «Квартет-С» предназначено для блокирования работы устройств, использующих каналы цифровой связи стандартов GSM-900, GSM-1800, IMT-2000/UMTS (3G), LTE

2600, LTE 800. В зависимости от расстояния до ближайшей базовой станции сотовой связи дальность блокирования абонентских терминалов составляет до 30 метров. Для защиты территорий с большей площадью используется метод пространственного размещения необходимого количества устройств.

В базовом исполнении «Квартет-С» представляет функционально законченный блок с внутренней антенной системой и с внешним питанием от сети 220 В. Дополнительно может комплектоваться адаптером питания от бортовой сети автомобиля.

Устройство может оснащаться модулем беспроводного дистанционного управления по радио или ИК каналу. Предусмотрена возможность подключения проводного дистанционного управления.

Внешний вид устройства «Квартет-С» представлен на рисунке 4.

Рисунок 4 - Устройство блокирования работы систем цифровой связи «Квартет-С»

Недостатком данного устройства является невозможность блокирования каналов стандартов Wi-Fi, Bluetooth, ZigBee. Для устранения данного недостатка необходимо использовать «Квартет-С» вместе с устройством блокирования систем передачи данных стандартов Wi-Fi, Bluetooth, ZigBee «Квартет-W».

Устройство блокирования систем передачи данных стандартов Wi-Fi, Bluetooth, ZigBee «Квартет-W» предназначено для блокирования работы устройств, использующих каналы цифровой связи стандартов Wi-Fi, Bluetooth,

ZigBee. В зависимости от расстояния до ближайшей базовой станции сотовой связи дальность блокирования абонентских терминалов составляет до 50 метров. Для защиты территорий с большей площадью используется метод пространственного размещения необходимого количества устройств.

В базовом исполнении «Квартет-W» представляет функционально законченный блок с внутренней антенной системой и с внешним питанием от сети 220 В.

Внешний вид устройства «Квартет-W» представлен на рисунке 5.

Рисунок 5 - Устройство блокирования систем передачи данных стандартов Wi-Fi, Bluetooth, ZigBee «Квартет-W»

Для определения повышения уровня электромагнитного поля при переходе устройства сотовой связи в режим передачи данных применяются индикаторы электромагнитного излучения [18]. Также для этих целей может применяться автоматизированный комплекс выявления и идентификации электронных устройств беспроводных связи «Цифра».

Автоматизированный комплекс выявления и идентификации электронных устройств беспроводных связи «Цифра» предназначен для решения задач спецпроверок технических средств и специальных обследований помещений на наличие устройств несанкционированного получения информации в соответствии с действующими методиками и нормативными документами.

Комплекс предназначен для исследований каналов наиболее распространенных беспроводных интерфейсов на наличие признаков несанкционированной передачи информации. Цифра позволяет оперативно выявлять сигналы устройств несанкционированной передачи информации в сетях GSM900/1800, UMTS (3G), DECT, WiFi, Bluetooth, ZigBee Pro и локализовывать места установки таких устройств в помещении. Таким образом, могут быть также выявлены и устройства сотовой связи в зоне работы данного комплекса [19].

Экранирование является действенным методом защиты от утечки информации по каналам сотовой связи и беспроводным каналам передачи данных при условии, что необходимо защитить отдельные помещения, а не весь объект полностью.

4.3 Организационные меры защиты от утечки информации по каналам сотовой связи и беспроводным каналам передачи данных

К организационным мерам защиты от утечки информации по каналам сотовой связи и беспроводным каналам передачи данных можно отнести пропускной режим на территорию контролируемой зоны организации для персонала и транспортных средств и их водителей.

Установка индивидуальных сейфов для хранения устройств сотовой связи перед входом на территорию организации или в режимные помещения, в зависимости от того необходимо ли исключить нахождение средств сотовой связи на всей территории организации или же лишь внутри режимных помещений. Также необходимо установить индивидуальные сейфы в местах поезда в контролируемую зону транспортных средств для водителей транспортных средств и сопровождающих их лиц при условии, что необходимо исключить нахождение средств сотовой связи на всей территории контролируемой зоны. В данные сейфы персонал организации и посетители должны размещать свои средства связи по приходе на рабочее место, совещание или с иной целью при входе в контролируемую зону или же в режимные

помещения. По убытии средства сотовой связи забираются из индивидуальных сейфов. Для доступа к данному сейфу может использоваться либо магнитная карта пропуска на территорию организации, либо индивидуальный ключ.

Работники охраны организации на контроль-пропускных пунктах должны быть обеспечены металлодетекторами, либо должны быть установлены рамочные металлодетекторы, которые позволят обнаруживать запрещенные устройства сотовой связи и другие технические устройства получения и передачи информации. При этом должны быть внесены соответствующие поправки в Должностные инструкции охранника организации, а также с ними должны быть ознакомлены работники отдела охраны организации под роспись.

Организационным мероприятием по защите от утечки информации по каналам сотовой связи и беспроводным каналам передачи данных может также являться разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Для обеспечения защиты от утечки информации по каналам сотовой связи и беспроводным каналам передачи данных может создаваться структурное подразделение организации, которое должно следить за тем, чтобы на территорию организации при условии, что необходимо исключить нахождение средств сотовой связи на всей территории контролируемой зоны, или же лишь в режимные помещения не проносились средства сотовой связи, осуществляло внеплановые проверки индивидуальных сейфов для хранения средств сотовой связи, исполнения обязанностей охранников по недопущению проноса средств сотовой связи на территорию организации, при условии, что необходимо исключить нахождение средств сотовой связи на всей территории контролируемой зоны, а также осуществлять внеплановые проверки наличия у персонала и посетителей средств сотовой связи с помощью средств выявления и идентификации электронных устройств беспроводных связи, а также с помощью индикаторов электромагнитного излучения.

Введение процедуры информирования за материальное вознаграждение работниками руководство об использовании устройств сотовой связи на территории организации, где их использование запрещено.

Обеспечение звукоизоляции помещений, в которых обрабатывается информация ограниченного доступа. При отсутствии возможности проведения данного мероприятия — запретить использование средств сотовой связи в смежных помещениях.

В коллективном договоре закрепить запрет на использование средств сотовой связи на всей территории контролируемой зоны организации при условии, что необходимо исключить нахождение средств сотовой связи в пределах контролируемой зоны.

5 Разработка методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных

5.1 Область применения методики

Данная методика предназначена для применения на АО «НПП «Рубин», а также в иных организациях, где уже осуществляется обработка информации ограниченного доступа, в том числе являющейся государственной тайной, коммерческой тайной, персональными данными, а также имеющей гриф «Для служебного пользования».

5.2 Цель разработки методики

Целью разработки методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных является систематизация мер защиты информации от утечки по каналам сотовой связи и беспроводным каналам передачи данных, определение условий, при которых указанные защитные меры могут быть применены, а также для помощи специалистам по информационной безопасности организаций по созданию системы защиты от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных.

5.3 Выбор защитных мер, использующихся в методике

Перечень организационных защитных мер, использующихся в методике приведен в приложении Б.

Перечень технических защитных мер, использующихся в методике приведен в приложении В.

Защитные меры, которые не были выбраны для применения в данной методике (с указанием причин отказа от применения):

— введение пропускного режима для персонала, транспортных средств и их водителей, а также для посетителей организации (по причине того, что в

организациях, для которых может быть применена данная методика, уже ведется обработка информации ограниченного доступа, соответственно уже приняты меры защиты, устраняющие её утечку по техническим каналам);

— введение процедуры информирования за материальное вознаграждение работниками руководство об использовании устройств сотовой связи на территории организации, где их использование запрещено (по причине того, что данная мера может привести в ухудшению корпоративного климата, за чем могут последовать финансовые потери);

— обеспечение звукоизоляции помещений, в которых обрабатывается информация ограниченного доступа (по причине того, что в организациях, для которых может быть применена данная методика, уже ведется обработка информации ограниченного доступа, соответственно уже приняты меры защиты, устраняющие её утечку по техническим каналам);

— запрет на использование средств сотовой связи в помещениях, смежных с помещениями, в которых обрабатывается информация ограниченного доступа (по причине того, что в организациях, для которых может быть применена данная методика, уже ведется обработка информации ограниченного доступа, соответственно уже приняты меры защиты, устраняющие её утечку по техническим каналам).

5.4 Определение угроз

Угрозой является утечка информации информации по каналам сотовой связи и беспроводным каналам передачи данных.

5.5 Определение уязвимостей

Единственной уязвимостью для реализации утечки информации информации по каналам сотовой связи и беспроводным каналам передачи данных является уязвимость персонала и лиц, допущенных на территорию контролируемой зоны, который является способом появления устройств

сотовой связи в пределах контролируемой зоны. Также уязвимостью является недостаточная информированность персонала об опасности утечки информации по каналам сотовой связи и беспроводным каналам передачи данных посредством устройств сотовой связи.

5.6 Определение нарушителей

Возможные нарушители приведены в таблице 1.

Таблица 1 — Возможные нарушители

№ п/п	Вид нарушителя	Цель реализации угроз безопасности
1	Конкурирующие организации	Получение конкурентных преимуществ.
2	Преступные группы	Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
3	Специальные службы иностранных государств	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики.

5.7 Описание алгоритма выбора защитных мер методики

Алгоритм выбор мер защиты для данной методики представлен в приложении Г.

Перед началом определения защитных мер, принимаемых для защиты организации от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных, необходимо провести комплексный анализ условий функционирования организации и примененных защитных мер. Для этого необходимо исследовать организацию на предмет уже реализованных защитных мер, которые перечислены в пункте о защитных мерах, которые используются в методике обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных.

После определения условий функционирования организации и уже

принятых защитных мер проводится оценка максимально возможных финансовых затрат на реализацию мер защиты от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных.

Затем необходимо определить, будет производиться защита всей территории организации или же лишь помещений, в которых обрабатывается информация ограниченного доступа. Если на территории всей организации должна быть исключена возможность использования средств сотовой связи, то необходимо в нормативно-правовых документах организации закрепить запрет на использование устройств сотовой связи для всех сотрудников организации.

Далее, если на территории всей организации должна быть исключена возможность использования средств сотовой связи, то определяется возможно ли использование использование устройства блокирования работы систем мобильной связи, для блокирования сигнала по всей площади организации. Схема для определения такой возможности представлена на рисунке 6.

Если при использовании средств блокирования работы систем мобильной связи создается возможность блокирования работы систем мобильной связи за пределами территории организации, что может нарушить деятельность других организаций, социально-значимых объектов, а также привести к неудобствам людей, то необходимо отказаться от устройств блокирования работы систем мобильной связи большого радиуса действия в пользу устройств с малым радиусом действия, устанавливаемых в режимных помещениях и с границами блокирования работы систем мобильной связи, не выходящими за пределы контролируемой зоны.

Таким образом, если организация имеет такое расположение, что у её границ нет других организаций, объектов, а также нет возможности создания помех для средств сотовой связи людей, не являющихся посетителями либо работника данной организации, то стоит использовать устройства блокирования работы систем мобильной связи большего радиуса действия.

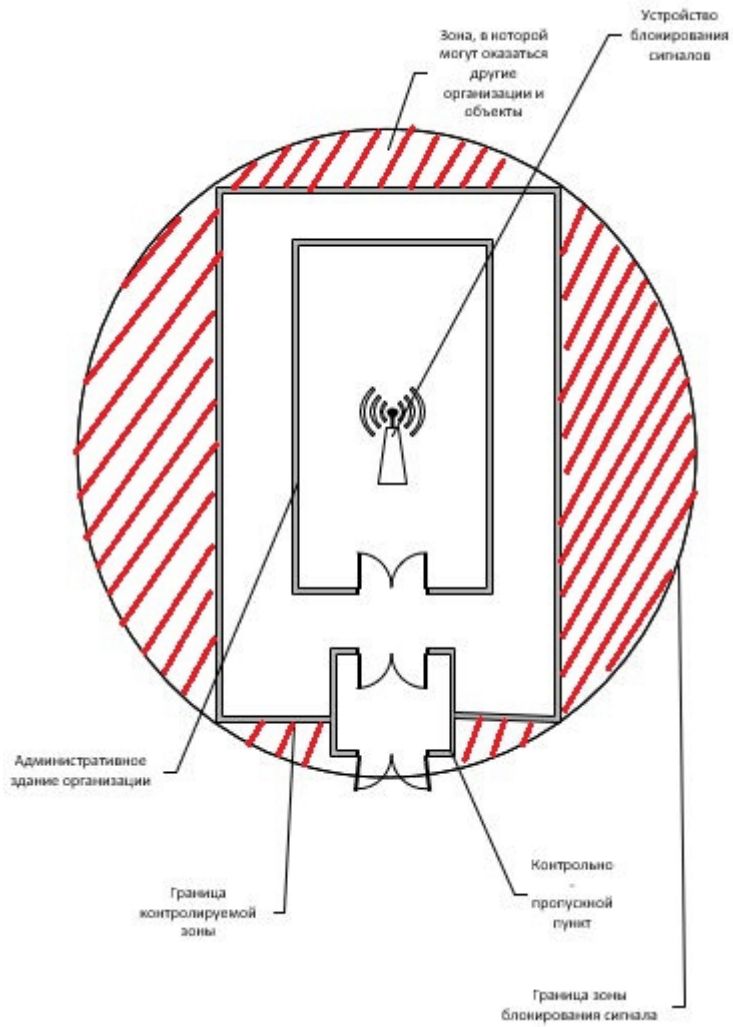

Рисунок 6 — Схема для определения возможности использования устройств блокирования работы систем мобильной связи для блокирования сигнала по всей площади организации

При условии возможности использования средств блокирования работы систем мобильной связи большего радиуса возможно использовать автоматизированный комплекс выявления и идентификации электронных устройств беспроводных связи «Цифра». Так как автоматизированный комплекс выявления и идентификации электронных устройств беспроводных связи «Цифра» позволяет обнаружить устройства большем радиусе, то не представляется возможным его использование для контроля использования устройств сотовой связи в организациях, где к границам контролируемой зоны примыкают другие организации, объекты, а также дороги общего пользования

по причине того, что данный комплекс будет обнаруживать не только устройства сотовой связи, находящиеся на территории организации, но и те, что находятся за её пределами. Таким образом, проведение проверок с использованием данного комплекса не может быть гарантированно точным.

Если при использовании средств блокирования работы систем мобильной связи не создается возможность блокирования работы систем мобильной связи за пределами территории организации, что может нарушить деятельность других организаций, социально-значимых объектов, а также привести к неудобствам людей, то необходимо использовать устройства блокирования работы систем мобильной связи малого радиуса действия.

При условии невозможности полного блокирования работы систем мобильной связи, но, при этом, необходимости защиты всей территории от использования средств сотовой связи, необходимо также определить имеются ли пункты пропуска транспортных средств. Если таких пунктов нет, то необходимо произвести установку индивидуальных сейфов для хранения устройств сотовой связи на контрольно-пропускном пункте организации, оборудовать контрольно-пропускные пункты металлодетекторами, а также внести изменения в Должностные инструкции охранника организации для работы с данными металлодетекторами и ознакомление с ними охранников под роспись.

Если такие пункты есть, то, помимо мер, принятых для организаций, у которых нет пунктов пропуска транспортных средств, должна быть произведена установка индивидуальный сейфов для хранения устройств сотовой связи водителей данных средств, а также их пассажиров на пункте пропуска транспортных средств на территорию организации.

Если же защите подлежат только помещения, в которых обрабатывается информация ограниченного доступа, то необходимо установить индивидуальные сейфы для хранения средств сотовой связи около входов в

такие помещения для хранения устройств сотовой связи работающего там персонала, а также иных допущенных в них лиц.

Если при использовании средств блокирования работы систем мобильной связи создается возможность блокирования работы систем мобильной связи за пределами территории организации, что может нарушить деятельность данной организации, других организаций, социально-значимых объектов, а также привести к неудобствам людей, то необходимо отказаться от использования устройств блокирования работы систем мобильной связи малого радиуса действия в пользу экранирования помещений, в которых обрабатывается информация ограниченного доступа.

Если при использовании средств блокирования работы систем мобильной связи не создается возможность блокирования работы систем мобильной связи за пределами территории организации, что может нарушить деятельность данной организации, других организаций, социально-значимых объектов, а также привести к неудобствам людей, то необходимо применять устройства блокирования работы систем мобильной связи малого радиуса действия.

При условии отсутствия других организаций, объектов, а также дорог общего пользования в радиусе действия возможно использовать автоматизированный комплекс выявления и идентификации электронных устройств беспроводных связи «Цифра». Так как автоматизированный комплекс выявления и идентификации электронных устройств беспроводных связи «Цифра» позволяет обнаружить устройства большем радиусе, то не представляется возможным его использование для контроля использования устройств сотовой связи в организациях, где к границам контролируемой зоны примыкают другие организации, объекты, а также дороги общего пользования по причине того, что данный комплекс будет обнаруживать не только устройства сотовой связи, находящиеся на территории организации, но и те, что находятся за её пределами. Таким образом, проведение проверок с использованием данного комплекса не может быть гарантированно точным.

Для всех предыдущих вариантов выбора защитных мер, в зависимости от численности персонала, необходимо создать структурное подразделение или назначить должностное лицо, осуществляющее контроль за использованием устройств сотовой связи на территории организации. Если численность персонала небольшая, то стоит назначить должностное лицо от руководства. При условии большего количества персонала необходимо создать отдельное структурное подразделение осуществляющее контроль за использованием устройств сотовой связи на территории организации.

Также для всех предыдущих вариантов выбора защитных мер руководству организации необходимо разработать приказ для руководителей всех структурных подразделений, в которых существует запрет на использование средств сотовой связи, по надзору за использованием средств сотовой связи работниками данных подразделений.

После определения всех необходимых защитных мер следует оценить стоимость их реализации, после чего необходимо сравнить стоимость реализации данных защитных мер с оценкой максимально возможных финансовых затрат на реализацию мер защиты от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных. Если стоимость реализации выбранных защитных мер превышает максимально возможные финансовые затраты, то следует заново определить выбор защитных мер в соответствии с Рекомендациями по практическому применению методики.

5.8 Выявленные наборы защитных мер в зависимости от условий функционирования организации

Если необходимо защищать от использования средств сотовой связи лишь помещения, в которых обрабатывается информация ограниченного доступа, возможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за

пределами территории организации, а также при малой численности работников организации, должны быть приняты следующие защитные меры:

— установка индивидуальных сейфов для хранения устройств сотовой связи возле режимных помещений;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— использование автоматизированного комплекса выявления и идентификации электронных устройств беспроводных связи «Цифра»;

— назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Если необходимо защищать от использования средств сотовой связи лишь помещения, в которых обрабатывается информация ограниченного доступа, возможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, а также при большой численности численности работников организации, должны быть приняты следующие защитные меры:

— установка индивидуальных сейфов для хранения устройств сотовой связи возле режимных помещений;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— использование автоматизированного комплекса выявления и идентификации электронных устройств беспроводных связи «Цифра»;

— создание структурного подразделения, осуществляющего контроль

за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Если необходимо защищать от использования средств сотовой связи лишь помещения, в которых обрабатывается информация ограниченного доступа, невозможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, а также при малой численности работников организации, должны быть приняты следующие защитные меры:

— установка индивидуальных сейфов для хранения устройств сотовой связи возле режимных помещений;

— экранирование помещений, в которых запрещено использование устройств сотовой связи;

— назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Если необходимо защищать от использования средств сотовой связи лишь помещения, в которых обрабатывается информация ограниченного доступа, невозможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, а также при большой численности работников организации, должны быть приняты следующие защитные меры:

— установка индивидуальных сейфов для хранения устройств сотовой связи возле режимных помещений;

— экранирование помещений, в которых запрещено использование устройств сотовой связи;

— создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Если необходимо защищать от использования средств сотовой связи всю территорию организации, невозможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, с проездом транспортных средств на территорию организации, а также при малой численности работников организации, должны быть приняты следующие защитные меры:

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— установка индивидуальных сейфов для хранения устройств сотовой связи на пункте пропуска транспортных средств на территорию организации;

— установка индивидуальных сейфов для хранения устройств сотовой связи на контрольно-пропускном пункте организации;

— оборудование контрольно-пропускных пунктов металлодетекторами;

— внесение поправок в Должностные инструкции охранника организации и ознакомление с ними охранников;

— назначение должностного лица от руководства организации,

осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Если необходимо защищать от использования средств сотовой связи всю территорию организации, невозможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, с проездом транспортных средств на территорию организации, а также при большой численности работников организации, должны быть приняты следующие защитные меры:

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— установка индивидуальных сейфов для хранения устройств сотовой связи на пункте пропуска транспортных средств на территорию организации;

— установка индивидуальных сейфов для хранения устройств сотовой связи на контрольно-пропускном пункте организации;

— оборудование контрольно-пропускных пунктов металлодетекторами;

— внесение поправок в Должностные инструкции охранника организации и ознакомление с ними охранников;

— создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей

структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Если необходимо защищать от использования средств сотовой связи всю территорию организации, невозможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, без возможности проезда транспортных средств на территорию организации, а также при малой численности работников организации, должны быть приняты следующие защитные меры:

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— установка индивидуальных сейфов для хранения устройств сотовой связи на контрольно-пропускном пункте организации;

— оборудование контрольно-пропускных пунктов металлодетекторами;

— внесение поправок в Должностные инструкции охранника организации и ознакомление с ними охранников;

— назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Если необходимо защищать от использования средств сотовой связи всю территорию организации, невозможно использование средств блокирования

работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, без возможности проезда транспортных средств на территорию организации, а также при большой численности работников организации, должны быть приняты следующие защитные меры:

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— установка индивидуальных сейфов для хранения устройств сотовой связи на контрольно-пропускном пункте организации;

— оборудование контрольно-пропускных пунктов металлодетекторами;

— внесение поправок в Должностные инструкции охранника организации и ознакомление с ними охранников;

— создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Если необходимо защищать от использования средств сотовой связи всю территорию организации, возможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, а также при малой численности работников организации, должны быть приняты следующие защитные меры:

— закрепление в нормативно-правовых документах организации

запрета на использование средств сотовой связи на всей территории контролируемой зоны организации;

— использование автоматизированного комплекса выявления и идентификации электронных устройств беспроводных связи «Цифра»;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия большего радиуса или использование устройств блокирования работы систем мобильной связи с секторной диаграммой направленности антенны большой дальности подавления;

— назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Если необходимо защищать от использования средств сотовой связи всю территорию организации, возможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, а также при большой численности работников организации, должны быть приняты следующие защитные меры:

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации;

— использование автоматизированного комплекса выявления и идентификации электронных устройств беспроводных связи «Цифра»;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия большего радиуса или

использование устройств блокирования работы систем мобильной связи с секторной диаграммой направленности антенны большой дальности подавления;

— создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

5.9 Описание критерия эффективности методики

Идеальным критерием эффективности данной методики является отношение информации, которая утекала по каналам сотовой связи и беспроводным каналам передачи данных с помощью средств сотовой связи до применения защитных мер из данной методики, к информации, которая утекает по каналам сотовой связи и беспроводным каналам передачи данных с помощью средств сотовой связи после применения защитных мер из данной методики за определенный период времени. Таким образом, чем больше первый показатель и чем меньше второй показатель, тем более эффективной является методика. Но данный критерий не может быть применен, так как не представляется возможным определить количество информации, которая утекает из организации по каналам сотовой связи и беспроводным каналам передачи данных за определенный период, как до применения методики, так и после.

Поэтому необходимо воспользоваться критерием эффективности, суть которого состоит в подсчете количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за определенный период до применения методики, а также определить возможность использования этих устройств сотовой связи на территории, на которой необходимо исключить

использование этих средств. Также необходимо произвести подсчет количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за определенный период после применения защитных мер из данной методики, а также определить возможность использования этих устройств сотовой связи на территории, на которой необходимо исключить использование этих средств. Затем необходимо составить отношение количества таких средств до применения методики к средствам после реализации методики. Если количество пронесенных устройств сотовой связи, которые также возможно использовать на территории, на которой необходимо исключить использование этих средств, после применения защитных мер из данной методики равно нулю, то данная методика считается эффективной.

5.10 Описание процедуры анализа эффективности методики

После выбора набора защитных мер необходимо создать структурное подразделение, осуществляющее контроль за использованием устройств сотовой связи на территорию организации, или назначить должностное лицо от руководства организации, осуществляющее контроль за использованием устройств сотовой связи на территорию организации, для подсчета количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за определенный период до реализации защитных мер из набора, а также определяющих возможность использования этих устройств сотовой связи на территории, на которой необходимо исключить использование этих средств.

После осуществления подсчета количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за определенный период до реализации защитных мер из набора, а также определения возможности использования этих устройств сотовой связи на территории, на

которой необходимо исключить использование этих средств, необходимо реализовывать защитные меры из набора последовательно. Параллельно с этим производится подсчет количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за определенный период до реализации защитных мер из набора, а также определяется возможность использования этих устройств сотовой связи на территории, на которой необходимо исключить использование этих средств. Для каждой реализуемой меры защиты необходимо проводить подсчет количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, а также определить возможность использования этих устройств сотовой связи на протяжении периода, равного периоду проведения подсчета до реализации мер защиты.

После реализации всех мер и проведения подсчета устройств после введения каждой из них необходимо сравнить полученные данные. Если количество пронесенных устройств сотовой связи, которые также возможно использовать на территории, на которой необходимо исключить использование этих средств, после применения защитных мер из данной методики равно нулю, то данная методика считается эффективной. В ином случае необходимо пересмотреть защитные меры.

Разработанная методика защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи приведена в приложении Д.

6 Проведение и оценка практического исследования эффективности методики и составление рекомендаций по практическому применению методики

6.1 Проведение практического исследования эффективности методики

Для проведения практического исследования эффективности методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных был выбран отдел АО «НПП «Рубин» для были реализованы защитные меры одного из наборов защитных мер данной методики. При этом были реализованы не все защитные меры из набора, а лишь те, на которые не было необходимо производить финансовых затрат. Всё практическое исследование проводилось в одном помещении АО «НПП «Рубин».

Первый этап - подсчет количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за двухдневный период до реализации защитных мер из набора, а также определение возможности использования этих устройств сотовой связи на территории, на которой необходимо исключить использование этих средств.

Всего в помещении находятся рабочие места семерых работников. У каждого работника отдела есть одно устройство сотовой связи. В момент проверки количества пронесенных устройств сотовой связи не все работники могли находиться на своих рабочих местах. Проверка осуществлялась в начале рабочего дня.

В первый день периода до реализации защитных мер из набора во время подсчета количества устройств сотовой связи на своих рабочих местах находились шесть человек из семи. У всех работников в сумме шесть устройств. Устройства всех шестерых работников могли быть ими использованы. Таким образом, все 100 процентов устройств присутствующих

работников могли использоваться.

Во второй день периода до реализации защитных мер из набора во время подсчета количества устройств сотовой связи на своих рабочих местах находились пять человек из семи. У всех работников в сумме 5 устройств. Устройства всех пятерых работников могли быть ими использованы. Таким образом, все 100 процентов устройств присутствующих работников могли использоваться. Данные за первый этап практического исследования приведены в таблице 2.

Таблица 2 — Данные за первый этап практического исследования

№ дня исследования	Количество присутствующих работников	Количество устройств сотовой связи работников не в ящике	Количество устройств сотовой связи, доступных для использования	Процент устройств сотовой связи, которые могли быть использованы
1	6	6	6	100
2	5	5	5	100

Второй этап — установка индивидуальных сейфов для хранения устройств сотовой связи. Для реализации данной защитной меры был использован ящик, в который работники складывали свои устройства сотовой связи. Также было проведено информирование работников о запрете использования средств сотовой связи. После реализации данных мер был проведен подсчет количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за двухдневный период до реализации защитных мер из набора, а также определена возможность использования этих устройств сотовой связи на территории, на которой необходимо исключить использование этих средств.

В первый день второго этапа во время подсчета количества устройств сотовой связи на своих рабочих местах находились семь человек из семи. В

ящике для устройств сотовой связи было шесть устройств. Одно устройство могло быть использованным. Таким образом, 14 процентов устройств присутствующих работников могли использоваться.

Во второй день второго этапа во время подсчета количества устройств сотовой связи на своих рабочих местах находились шесть человек из семи. В ящике для устройств сотовой связи было четыре устройства. Два устройства могли быть использованы. Таким образом, 33 процента устройств присутствующих работников могли использоваться. Данные за второй этап практического исследования приведены в таблице 3.

Таблица 3 — Данные за второй этап практического исследования

№ дня исследования	Количество присутствующих работников	Количество устройств сотовой связи работников не в ящике	Количество устройств сотовой связи, доступных для использования	Процент устройств сотовой связи, которые могли быть использованы
3	7	1	1	14
4	6	2	2	33

Третий этап — введение дополнительных проверок во время рабочего дня. Они проводятся в случайное время. Также было проведено повторное информирование работников о запрете использования средств сотовой связи. После реализации данных мер был проведен подсчет количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за двухдневный период до реализации защитных мер из набора, а также определена возможность использования этих устройств сотовой связи на территории, на которой необходимо исключить использование этих средств.

В первый день третьего этапа во время подсчета количества устройств сотовой связи на своих рабочих местах находились шесть человек из семи. В ящике для устройств сотовой связи было пять устройств. Одно устройство

могло быть использованным. Таким образом, 17 процентов устройств присутствующих работников могли использоваться. Также была проведена проверка в случайное время рабочего дня. На своих рабочих местах находились четыре человека из семи. В ящике для устройств сотовой связи было два устройства. Два устройства могли быть использованными. Таким образом, 50 процентов устройств присутствующих работников могли использоваться.

Во второй день третьего этапа во время подсчета количества устройств сотовой связи на своих рабочих местах находились пять человек из семи. В ящике для устройств сотовой связи было пять устройств. Ни одно устройство не могло быть использованным. Таким образом, 0 процентов устройств присутствующих работников могли использоваться. Также была проведена проверка в случайное время рабочего дня. На своих рабочих местах находились пять человека из семи. В ящике для устройств сотовой связи было четыре устройства. Одно устройство могло быть использованным. Таким образом, 20 процентов устройств присутствующих работников могли использоваться. Данные за третий этап практического исследования приведены в таблице 4.

Таблица 4 — Данные за третий этап практического исследования

№ дня исследования	Тип проверки	Количество присутствующих работников	Количество устройств сотовой связи работников не в ящике	Количество устройств сотовой связи, доступных для использования	Процент устройств сотовой связи, которые могли быть использованы
5	Регулярная проверка	6	1	1	17
	Проверка в случайное время	4	2	2	50
6	Регулярная проверка	5	0	0	0
	Проверка в случайное время	5	1	1	20

Четвертый этап — установка устройства подавления систем цифровой связи и передачи данных всех стандартов «Мозаика-7К». После реализации данного мероприятия был проведен подсчет количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за двухдневный период до реализации защитных мер из набора, а также определена возможность использования этих устройств сотовой связи на территории, на которой необходимо исключить использование этих средств.

В первый день четвертого этапа во время подсчета количества устройств сотовой связи на своих рабочих местах находились шесть человек из семи. В ящике для устройств сотовой связи было шесть устройств. Ни одно устройство не могло быть использованным. Таким образом, 0 процентов устройств присутствующих работников могли использоваться. Также была проведена проверка в случайное время рабочего дня. На своих рабочих местах находились пять человека из семи. В ящике для устройств сотовой связи было четыре устройства. Ни одно устройство не могло быть использованным из-за работы устройства подавления систем цифровой связи и передачи данных всех стандартов «Мозаика-7К». Таким образом, 0 процентов устройств присутствующих работников могли использоваться.

Во второй день четвертого этапа во время подсчета количества устройств сотовой связи на своих рабочих местах находились семь человек из семи. В ящике для устройств сотовой связи было семь устройств. Ни одно устройство не могло быть использованным из-за работы устройства подавления систем цифровой связи и передачи данных всех стандартов «Мозаика-7К». Таким образом, 0 процентов устройств присутствующих работников могли использоваться. Также была проведена проверка в случайное время рабочего дня. На своих рабочих местах находились пять человека из семи. В ящике для устройств сотовой связи было пять устройства. Ни одно устройство не могло быть использованным из-за работы устройства подавления систем цифровой

связи и передачи данных всех стандартов «Мозаика-7К». Таким образом, 0 процентов устройств присутствующих работников могли использоваться. Схема размещения средств защиты информации представлена в приложении Е. Данные за четвертый этап практического исследования приведены в таблице 5.

Таблица 5 — Данные за четвертый этап практического исследования

№ дня исследования	Тип проверки	Количество присутствующих работников	Количество устройств сотовой связи работников не в ящике	Количество устройств сотовой связи, доступных для использования	Процент устройств сотовой связи, которые могли быть использованы
7	Регулярная проверка	6	0	0	0
	Проверка в случайное время	5	1	0	0
8	Регулярная проверка	7	0	0	0
	Проверка в случайное время	5	0	0	0

После восьми дней практическое исследование было завершено.

6.2 Оценка результатов практического исследования эффективности методики

Для оценки практического исследования эффективности методики был построен график данного исследования, который приведен в приложении Ж.

По оси X координат расположены тип и день проверки, когда по оси Y координат расположен процент устройств, которые возможно использовать, от общего числа устройств, которые были принесены работниками. Красной линией на графике практического исследования эффективности методики

отмечена линия тренда изменения процента устройств, которые возможно использовать, от общего числа устройств, которые были принесены работниками, на протяжении всего периода проведения практического исследования эффективности методики.

Данный график указывает на то, что по мере реализации мер защиты происходит падение процента устройств сотовой связи, которые могли быть использованы, от общего числа устройств, пронесенных на защищаемую территорию. Линия тренда также указывает на данную тенденцию. Но , при этом, существуют и значения, которые не соотносятся с данной тенденцией. К ним относятся значения регулярной проверки на четвертый день и случайной проверки на пятый день. Данный факт объясняется тем, что работники отдела не всегда со всей серьезностью относились к данному исследованию, а также то, что отсутствовала система дисциплинарных санкций для нарушителей запрета на устройства сотовой связи на территории отдела, где проводилось практическое исследование.

Также можно отметить постепенное падение процента устройств, которые возможно использовать, от общего числа устройств, которые были принесены работниками, по мере реализации мер защиты из набора. Это указывает на то, что возможно применение не всего набора защитных мер, а лишь определенного их числа, путем постепенного их ввода с оценкой после введения каждой меры по отдельности.

Так как количество пронесенных устройств сотовой связи, которые также возможно использовать на территории, на которой необходимо исключить использование этих средств, после применения защитных мер из данной методики равно нулю, то данная методика считается эффективной.

6.3 Рекомендации по практическому применению методики

При применении данной методики необходимо провести комплексный анализ условий функционирования организации и уже реализованных

защитных мер.

После определения условий функционирования организации проводится оценка максимально возможных финансовых затрат на реализацию мер защиты от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных.

Затем на основе полученных данных проводится выбор набора защитных мер из тех, что представлены в методике.

Если на реализацию защитных мер из выбранного набора необходимо затрать большее количество финансовых средств, чем было изначально запланировано до выбора набора, то необходимо пересмотреть набор или заменить некоторые дорогостоящие меры из набора на более дешевые. Так, при реализации защитных мер «Создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации» или «Назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации», функции создаваемых подразделений можно предоставить уже существующему подразделению по информационной безопасности или Службе безопасности организации. Также, мера защиты «Экранирование помещений, в которых запрещено использование устройств сотовой связи» может быть замещена мерой защиты «Использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса» и наоборот.

Выбранные защитные меры необходимо реализовывать поочередно. После реализации каждой меры необходимо проводить анализ эффективности и сравнивать эффективность период наблюдения после реализации данной защитной меры с периодом наблюдения после реализации предыдущей защитной меры, а также с периодом до реализации защитных мер. При достижении эффективности методики по критерию эффективности необходимо прекратить введение дальнейших мер защиты из набора.

При определении порядка реализации защитным мер из набора необходимо в первую очередь выбирать те защитные меры, на введение которых необходимы наименьшие финансовые затраты, и технические средства для которых уже имеются у организации.

Разработанные рекомендации по практическому применению методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных представлены в приложении И.

7 Вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

Работа специалиста по защите информации предполагает работу с различными техническими средствами, которые могут негативно воздействовать на организм специалиста. К таким воздействиям относятся:

— электромагнитные излучения и радиоизлучения;

— высокочастотные звуковые сигналы;

— вибрация;

— ненормированный уровень шума;

— ненормированная яркость изображения на экране мониторов и дисплеев.

Также негативное влияние на здоровье специалиста по защите информации оказывают внешние факторы, такие как:

— вид трудовой активности;

— микроклимат помещений;

— освещенность рабочего места;

— расположение органов управления и технических средств на рабочем месте по отношению к специалисту.

Воздействие вредных факторов на опорно-двигательный аппарат специалиста зависит в первую очередь от его двигательной активности в период рабочего времени. Сфера его деятельности может включать:

— длительное нахождение в помещении с высоким уровнем вибрации;

— работу, связанную с частым переносом тяжелого оборудования;

— длительное пребывание в сидячем положении.

Так, при постоянном выполнении работ в помещениях с высоким уровнем вибрации у специалиста страдает мышечная система, хрящи и связки. При

постоянной вибрации появляется мышечная усталость, их сила снижается, происходит атрофия мышц. Хрящевая ткань от вибраций становится грубее и затрудняет движения в суставах, о чем может свидетельствовать боль и отеки. Связки также становятся грубее и менее прочными, что приводит к их растяжению и разрыву.

Во время поднятия, приёма, переноса или перестановки тяжелого оборудования создается большая нагрузка на мышцы, а при неразвитой мускулатуре или поднятии очень большого веса, всю нагрузку берет на себя позвоночник. Вследствие этого возможно растяжение и разрыв мышц спины, смещение, протрузии, грыжи межпозвоночных дисков.

Если же рабочая деятельность подразумевает постоянное нахождение в сидячем положении при работе на компьютере, это может привести к развитию тоннельного синдрома запястного канала, искривлению позвоночника, остеохондрозу позвоночника шейного, грудного и поясничного отделов, застоя венозной крови в органах малого таза и ногах, что может привести к варикозу и тромбозу.

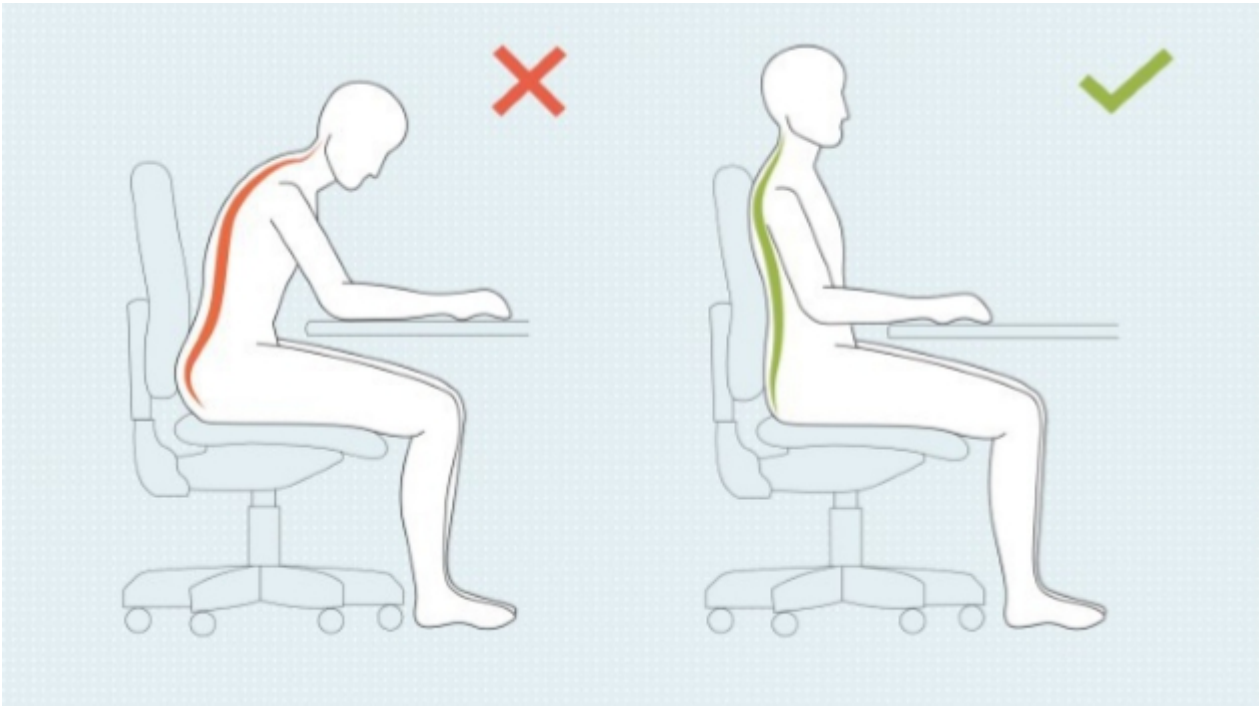

Рисунок 7 — Неправильное и правильное положение сидя

Также, помимо соблюдения правильного положения тела, для

профилактики негативных воздействий, влияющих на опорно-двигательный аппарат специалиста по защите информации рекомендуется выполнять следующие действия, направленные на разгрузку и поддержание в тонусе опорно-двигательного аппарата:

— ежедневная утренняя зарядка;

— ежедневная ходьба в среднем темпе в течение 40 минут;

— занятие активными видами спорта;

— делать небольшой перерыв через каждые 2-3 часа постоянной работы, во время которого осуществлять разминку опорно-двигательного аппарата;

— массаж.

Заключение

Современные устройства сотовой связи представляют большую опасность для организаций, в которых обрабатывается информация ограниченного доступа. Основная причина этого заключается в том, что современные устройства сотовой связи поддерживают множество стандартов беспроводной передачи данных. Соответственно данные устройства могут создавать различные каналы беспроводной передачи данных, по которым из организации может произойти утечка информации, что может нанести организации существенный финансовый ущерб. Для защиты от таких утечек необходимо применять комплекс организационных и технических защитных мер.

Основной задачей данной работы была разработка методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных, которая содержит в себе наборы организационных и технических мер для применения как в АО «НПП «Рубин», так и в организациях с отличными условиями функционирования.

В процессе выполнения выпускной квалификационной работы была подготовлена статья на тему «Обзор существующих каналов утечки информации и методов защиты информации от утечки по ним» и опубликована в сборнике «Информационные технологии в науке и образовании. Проблемы и перспективы» [20].

Были определены организационные и технические защитные меры, которые применимы в данной методике. Также был разработан алгоритм выбора защитных мер для организаций с различными условиями функционирования, по итогам выполнения которого были выявлены наборы защитных мер для организаций с различными условиями функционирования.

Для определения эффективности данной методики был сформулирован критерий эффективности и порядок проведения практического исследования

эффективности данной методики. После чего было проведено практическое исследование посредством применения защитных мер одного из наборов данной методики на отделе АО «НПП «Рубин». При анализе результатов проведения практического исследования было выявлено, что данная методика эффективна. Также по результатам практического исследования были разработаны рекомендации по практическому применению методики.

Таким образом, все пункты технического задания выполнены полностью.

Протокол проверки на оригинальность приведен в приложении К.

Список используемых источников

1 Конституция Российской Федерации : [принята всенародным голосованием 12.12.1993] [с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ] — [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения 25.02.2020).

2 Российская Федерация. Законы. О средствах массовой информации: закон РФ от 27.12.1991 №2124-1 - [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_1511/ (дата обращения: 25.02.2020).

3 Российская Федерация. Законы. О государственной тайне: закон РФ "О государственной тайне" от 21.07.1993 №5485-1 - [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_2481// (дата обращения: 25.02.2020).

4 Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации: федер. Закон Рос. Федерации от 27 июля 2006 года №149-ФЗ - [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 25.02.2020).

5 Российская Федерация. Законы. О связи: федер. Закон Рос. Федерации от 07.07.2003 №126-ФЗ - [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 25.02.2020).

6 Российская Федерация. Законы. Об обязательном экземпляре документов: федер. Закон Рос. Федерации от 29.12.1994 №77-ФЗ - [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_5437/ (дата обращения: 25.02.2020).

7 Гражданский кодекс Российской Федерации : принят Гос. Думой 21 октября 1994 - [Электронный ресурс]. Режим доступа : https://base.garant.ru/10164072/ (дата обращения: 25.02.2020).

8 Гражданско-процессуальный кодекс Российской Федерации : [принят Гос. Думой 23 октября 2002 г. : одобр. Советом Федерации 30 октября 2002г.] - [Электронный ресурс]. Режим доступа : https://base.garant.ru/12128809/ (дата обращения: 25.02.2020).

9 Уголовный кодекс Российской Федерации : [принят Гос. Думой 24 мая 1996 г. : одобр. Советом Федерации 5 июня 1996 г.] - [Электронный ресурс]. Режим доступа : https://base.garant.ru/10108000/ (дата обращения: 25.02.2020).

10 Уголовно-процессуальный кодекс Российской Федерации : [принят Гос. Думой 22 ноября 2001 г. : одобр. Советом Федерации 5 декабря 2001 г.] - [Электронный ресурс]. Режим доступа : https://base.garant.ru/12125178/ (дата обращения: 25.02.2020).

11 Налоговый кодекс Российской Федерации : [принят Гос. Думой 16 июля 1998 г. : одобр. Советом Федерации 17 июля 1998 г.] - [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_19671/ (дата обращения: 25.02.2020).

12 Семейный кодекс Российской Федерации : [принят Гос. Думой 16 июля 1998 г.] - [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_8982/ (дата обращения: 25.02.2020).

13 Российская Федерация. Законы. О Центральном банке Российской Федерации (Банке России): федер. Закон Рос. Федерации от 10.07.2002 №86-ФЗ - [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_37570/ (дата обращения: 25.02.2020).

14 UMTS и LTE частоты в России: стандарты нового поколения

[Электронный ресурс]. Режим доступа : https://gsm-repiteri.ru/umts-i-lte-chastoty-v-rossii-standarty-novogo-pokolenija (дата обращения: 30.03.2020).

15 Технология DECT [Электронный ресурс]. Режим доступа : https://radio-secure.ru/technology/dect (дата обращения: 15.04.2020).

16 Кашкаров, А.П.Электронные устройства для глушения беспроводных сигналов (GSM, Wi-Fi, GPS и некоторых радиотелефонов)/ А.П. Кашкаров. - Изд-во ДМК Пресс, 2016 — 120 с.

17 Секторные антенны - зачем они нужны [Электронный ресурс]. Режим доступа : https://kroks.ru/useful-articles/stati/sector-antennas-why-do-they-need/ (дата обращения: 20.04.2020).

18 Индикаторы электромагнитных излучений [Электронный ресурс]. Режим доступа : https://studopedia.ru/12_164773_indikatori-elektromagnitnih-izlucheniy.html (дата обращения: 20.04.2020).

19 Автоматизированный комплекс выявления и идентификации электронных устройств беспроводной связи "Цифра" [Электронный ресурс]. Режим доступа : http://www.bnti.ru/des.asp?itm=5068&tbl=04.01.01.03. (дата обращения: 20.04.2020).

20 Авдеев, С.А. Обзор существующих каналов утечки информации и методов защиты информации от утечки по ним/ С.А. Авдеев, А.П. Иванов// Информационные технологии в науке и образовании. Проблемы и перспективы. - Пенза, 2020. - С. 187-189.

Приложение А

(обязательное)

Схема возможной утечки информации по каналам беспроводной передачи данных

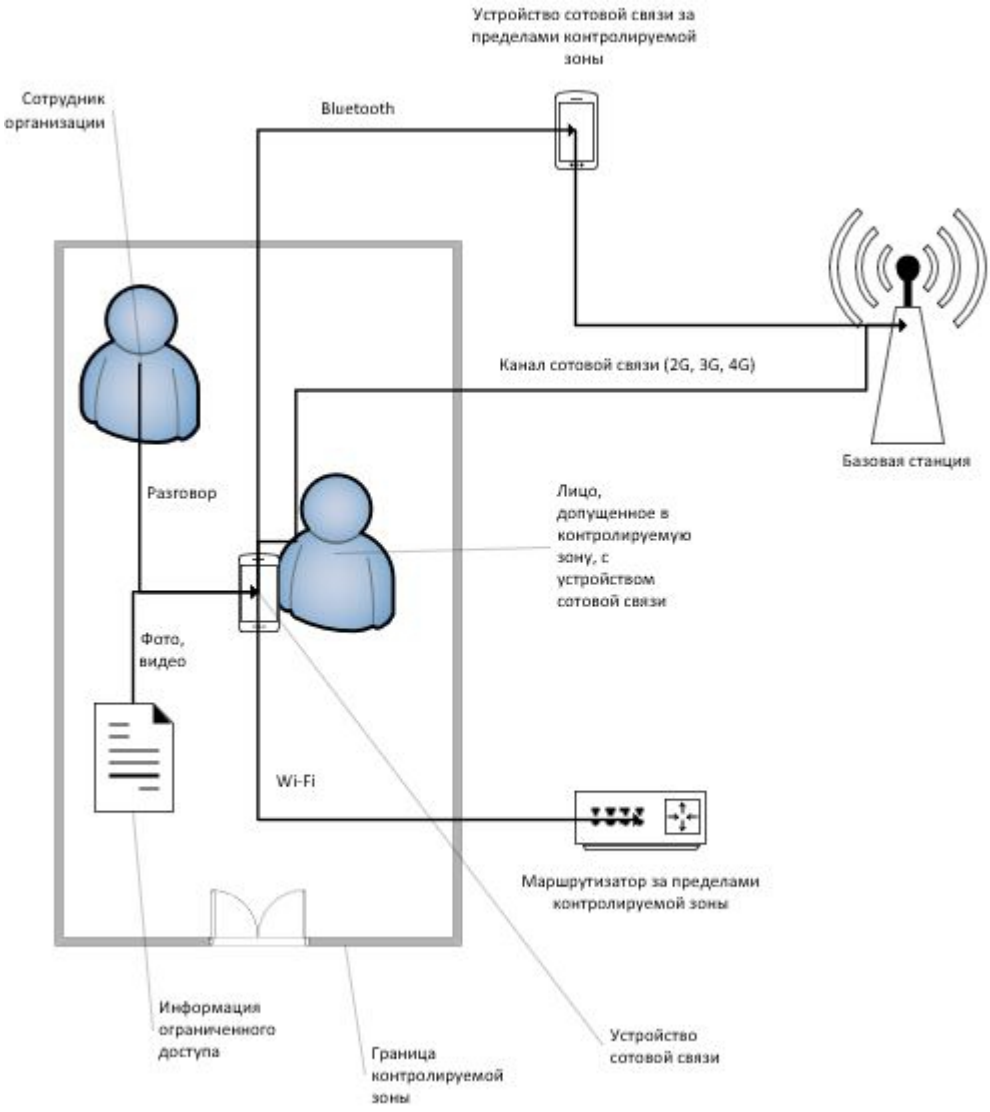

Рисунок А.1 — Схема возможной утечки информации по каналам беспроводной передачи данных

Приложение Б

(обязательное)

Перечень организационных мер, содержащихся в методике

В методике обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных содержатся следующие организационные меры:

— установка индивидуальных сейфов для хранения устройств сотовой связи на контрольно-пропускном пункте организации;

— установка индивидуальных сейфов для хранения устройств сотовой связи на пункте пропуска транспортных средств на территорию организации;

— установка индивидуальных сейфов для хранения устройств сотовой связи возле режимных помещений;

— оборудование контрольно-пропускных пунктов металлодетекторами;

— внесение поправок в Должностные инструкции охранника организации и ознакомление с ними охранников;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений;

— создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации.

Приложение В

(обязательное)

Перечень технических мер, содержащихся в методике

В методике обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных содержатся следующие технические меры:

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия большего радиуса или использование устройств блокирования работы систем мобильной связи с секторной диаграммой направленности антенны большой дальности подавления;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— использование автоматизированного комплекса выявления и идентификации электронных устройств беспроводных связи «Цифра»;

— экранирование помещений, в которых запрещено использование устройств сотовой связи.

Приложение Г

(обязательное)

Алгоритм выбора мер защиты

Рисунок Г.1 — Алгоритм выбора мер защиты

Приложение Д

(обязательное)

Методика обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи

УТВЕРЖДЕНА

приказом_____

№_____

« __ » _____20__ г.

МЕТОДИКА ОБЕСПЕЧЕНИЯ ЗАЩИТЫ АО «НПП «РУБИН» ОТ УТЕЧЕК ИНФОРМАЦИИ ПО КАНАЛАМ СОТОВОЙ СВЯЗИ И БЕСПРОВОДНЫМ КАНАЛАМ ПЕРЕДАЧИ

Содержание

Д.1 Область применения методики....73
Д.2 Цель разработки методики....73
Д.3 Выбор защитных мер, использующихся в методике....73
Д.4 Определение угроз....75
Д.5 Определение уязвимостей....75
Д.6 Определение нарушителей....76
Д.7 Выявленные наборы защитных мер в зависимости от условий функционирования организации....76
Д.7.1 Набор №1....76
Д.7.2 Набор №2....77
Д.7.3 Набор №3....78
Д.7.4 Набор №4....78
Д.7.5 Набор №5....79
Д.7.6 Набор №6....80
Д.7.7 Набор №7....81
Д.7.8 Набор №8....82
Д.7.9 Набор №9....83
Д.7.10 Набор №10....83
Д.8 Описание критерия эффективности методики....84
Д.9 Описание процедуры анализа эффективности методики....85

Д.1 Область применения методики

Данная методика предназначена для применения на АО «НПП «Рубин», а также в иных организациях, где уже осуществляется обработка информации ограниченного доступа, в том числе являющейся государственной тайной, коммерческой тайной, персональными данными, а также имеющей гриф «Для служебного пользования».

Д.2 Цель разработки методики

Целью разработки методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных является систематизация мер защиты информации от утечки по каналам сотовой связи и беспроводным каналам передачи данных, определение условий, при которых указанные защитные меры могут быть применены, а также для помощи специалистам по информационной безопасности организаций по созданию системы защиты от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных.

Д.3 Выбор защитных мер, использующихся в методике

В методике обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных содержатся следующие организационные меры:

— установка индивидуальных сейфов для хранения устройств сотовой связи на контрольно-пропускном пункте организации;

— установка индивидуальных сейфов для хранения устройств сотовой связи на пункте пропуска транспортных средств на территорию организации;

— установка индивидуальных сейфов для хранения устройств сотовой связи возле режимных помещений;

— оборудование контрольно-пропускных пунктов металлодетекторами;

— внесение поправок в Должностные инструкции охранника организации и ознакомление с ними охранников;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений;

— создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации.

В методике обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных содержатся следующие технические меры:

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия большего радиуса или использование устройств блокирования работы систем мобильной связи с секторной диаграммой направленности антенны большой дальности подавления;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— использование автоматизированного комплекса выявления и идентификации электронных устройств беспроводных связи «Цифра»;

— экранирование помещений, в которых запрещено использование устройств сотовой связи.

Защитные меры, которые не были выбраны для применения в данной

методике (с указанием причин отказа от применения):

— введение пропускного режима для персонала, транспортных средств и их водителей, а также для посетителей организации (по причине того, что в организациях, для которых может быть применена данная методика, уже ведется обработка информации ограниченного доступа, соответственно уже приняты меры защиты, устраняющие её утечку по техническим каналам);

— введение процедуры информирования за материальное вознаграждение работниками руководство об использовании устройств сотовой связи на территории организации, где их использование запрещено (по причине того, что данная мера может привести в ухудшению корпоративного климата, за чем могут последовать финансовые потери);

— обеспечение звукоизоляции помещений, в которых обрабатывается информация ограниченного доступа (по причине того, что в организациях, для которых может быть применена данная методика, уже ведется обработка информации ограниченного доступа, соответственно уже приняты меры защиты, устраняющие её утечку по техническим каналам);

— запрет на использование средств сотовой связи в помещениях, смежных с помещениями, в которых обрабатывается информация ограниченного доступа (по причине того, что в организациях, для которых может быть применена данная методика, уже ведется обработка информации ограниченного доступа, соответственно уже приняты меры защиты, устраняющие её утечку по техническим каналам).

Д.4 Определение угроз

Угрозой является утечка информации информации по каналам сотовой связи и беспроводным каналам передачи данных.

Д.5 Определение уязвимостей

Единственной уязвимостью для реализации утечки информации информации по каналам сотовой связи и беспроводным каналам передачи

данных является уязвимость персонала и лиц, допущенных на территорию контролируемой зоны, который является способом появления устройств сотовой связи в пределах контролируемой зоны. Также уязвимостью является недостаточная информированность персонала об опасности утечки информации по каналам сотовой связи и беспроводным каналам передачи данных посредством устройств сотовой связи.

Д.6 Определение нарушителей

Возможные нарушители приведены в таблице Д.1.

Таблица Д.1 — Возможные нарушители

№ п/п	Вид нарушителя	Цель реализации угроз безопасности
1	Конкурирующие организации	Получение конкурентных преимуществ.
2	Преступные группы	Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
3	Специальные службы иностранных государств	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики.

Д.7 Выявленные наборы защитных мер в зависимости от условий функционирования организации

Д.7.1 Набор №1

Набор №1 применяется при условии, если необходимо защищать от использования средств сотовой связи лишь помещения, в которых обрабатывается информация ограниченного доступа, возможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, а также при малой численности работников организации, должны быть приняты следующие защитные меры:

— установка индивидуальных сейфов для хранения устройств сотовой связи возле режимных помещений;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— использование автоматизированного комплекса выявления и идентификации электронных устройств беспроводных связи «Цифра»;

— назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Д.7.2 Набор №2

Набор №2 применяется при условии, если необходимо защищать от использования средств сотовой связи лишь помещения, в которых обрабатывается информация ограниченного доступа, возможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, а также при большой численности численности работников организации, должны быть приняты следующие защитные меры:

— установка индивидуальных сейфов для хранения устройств сотовой связи возле режимных помещений;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— использование автоматизированного комплекса выявления и идентификации электронных устройств беспроводных связи «Цифра»;

— создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Д.7.3 Набор №3

Набор №3 применяется при условии, если необходимо защищать от использования средств сотовой связи лишь помещения, в которых обрабатывается информация ограниченного доступа, невозможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, а также при малой численности работников организации, должны быть приняты следующие защитные меры:

— установка индивидуальных сейфов для хранения устройств сотовой связи возле режимных помещений;

— экранирование помещений, в которых запрещено использование устройств сотовой связи;

— назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Д.7.4 Набор №4

Набор №4 применяется при условии, если необходимо защищать от использования средств сотовой связи лишь помещения, в которых обрабатывается информация ограниченного доступа, невозможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за

пределами территории организации, а также при большой численности работников организации, должны быть приняты следующие защитные меры:

— установка индивидуальных сейфов для хранения устройств сотовой связи возле режимных помещений;

— экранирование помещений, в которых запрещено использование устройств сотовой связи;

— создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Д.7.5 Набор №5

Набор №5 применяется при условии, если необходимо защищать от использования средств сотовой связи всю территорию организации, невозможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, с проездом транспортных средств на территорию организации, а также при малой численности работников организации, должны быть приняты следующие защитные меры:

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— установка индивидуальных сейфов для хранения устройств сотовой связи на пункте пропуска транспортных средств на территорию организации;

— установка индивидуальных сейфов для хранения устройств сотовой связи на контрольно-пропускном пункте организации;

— оборудование контрольно-пропускных пунктов металлодетекторами;

— внесение поправок в Должностные инструкции охранника организации и ознакомление с ними охранников;

— назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Д.7.6 Набор №6

Набор №6 применяется при условии, если необходимо защищать от использования средств сотовой связи всю территорию организации, невозможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, с проездом транспортных средств на территорию организации, а также при большой численности работников организации, должны быть приняты следующие защитные меры:

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— установка индивидуальных сейфов для хранения устройств сотовой связи на пункте пропуска транспортных средств на территорию организации;

— установка индивидуальных сейфов для хранения устройств сотовой связи на контрольно-пропускном пункте организации;

— оборудование контрольно-пропускных пунктов металлодетекторами;

— внесение поправок в Должностные инструкции охранника организации и ознакомление с ними охранников;

— создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Д.7.7 Набор №7

Набор №7 применяется при условии, если необходимо защищать от использования средств сотовой связи всю территорию организации, невозможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, без возможности проезда транспортных средств на территорию организации, а также при малой численности работников организации, должны быть приняты следующие защитные меры:

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— установка индивидуальных сейфов для хранения устройств сотовой связи на контрольно-пропускном пункте организации;

— оборудование контрольно-пропускных пунктов металлодетекторами;

— внесение поправок в Должностные инструкции охранника организации и ознакомление с ними охранников;

— назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Д.7.8 Набор №8

Набор №8 применяется при условии, если необходимо защищать от использования средств сотовой связи всю территорию организации, невозможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, без возможности проезда транспортных средств на территорию организации, а также при большой численности работников организации, должны быть приняты следующие защитные меры:

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса;

— установка индивидуальных сейфов для хранения устройств сотовой связи на контрольно-пропускном пункте организации;

— оборудование контрольно-пропускных пунктов металлодетекторами;

— внесение поправок в Должностные инструкции охранника организации и ознакомление с ними охранников;

— создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей

структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Д.7.9 Набор №9

Набор №9 применяется при условии, если необходимо защищать от использования средств сотовой связи всю территорию организации, возможно использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, а также при малой численности работников организации, должны быть приняты следующие защитные меры:

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации;

— использование автоматизированного комплекса выявления и идентификации электронных устройств беспроводных связи «Цифра»;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия большего радиуса или использование устройств блокирования работы систем мобильной связи с секторной диаграммой направленности антенны большой дальности подавления;

— назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Д.7.10 Набор № 10

Набор №10 применяется при условии, если необходимо защищать от использования средств сотовой связи всю территорию организации, возможно

использование средств блокирования работы систем мобильной связи без создания возможности блокирования работы систем мобильной связи за пределами территории организации, а также при большой численности работников организации, должны быть приняты следующие защитные меры:

— закрепление в нормативно-правовых документах организации запрета на использование средств сотовой связи на всей территории контролируемой зоны организации;

— использование автоматизированного комплекса выявления и идентификации электронных устройств беспроводных связи «Цифра»;

— использование всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия большего радиуса или использование устройств блокирования работы систем мобильной связи с секторной диаграммой направленности антенны большой дальности подавления;

— создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации;

— разработка приказа руководителя организации для руководителей структурных подразделений по дополнительному надзору за использованием устройств сотовой связи работниками данных структурных подразделений.

Д.8 Описание критерия эффективности методики

Суть критерия эффективности методики состоит в подсчете количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за определенный период до применения методики, а также определить возможность использования этих устройств сотовой связи на территории, на которой необходимо исключить использование этих средств. Также необходимо произвести подсчет количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и

беспроводным каналам передачи данных, за определенный период после применения защитных мер из данной методики, а также определить возможность использования этих устройств сотовой связи на территории, на которой необходимо исключить использование этих средств. Затем необходимо составить отношение количества таких средств до применения методики к средствам после реализации методики. Если количество пронесенных устройств сотовой связи, которые также возможно использовать на территории, на которой необходимо исключить использование этих средств, после применения защитных мер из данной методики равно нулю, то данная методика считается эффективной.

Д.9 Описание процедуры анализа эффективности методики

После выбора набора защитных мер необходимо создать структурное подразделение, осуществляющее контроль за использованием устройств сотовой связи на территорию организации, или назначить должностное лицо от руководства организации, осуществляющее контроль за использованием устройств сотовой связи на территорию организации, для подсчета количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за определенный период до реализации защитных мер из набора, а также определяющих возможность использования этих устройств сотовой связи на территории, на которой необходимо исключить использование этих средств.

После осуществления подсчета количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за определенный период до реализации защитных мер из набора, а также определения возможности использования этих устройств сотовой связи на территории, на которой необходимо исключить использование этих средств, необходимо реализовывать защитные меры из набора последовательно. Параллельно с этим производится подсчет количества пронесенных устройств сотовой связи, с

помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, за определенный период до реализации защитных мер из набора, а также определяется возможность использования этих устройств сотовой связи на территории, на которой необходимо исключить использование этих средств. Для каждой реализуемой меры защиты необходимо проводить подсчет количества пронесенных устройств сотовой связи, с помощью которых информация может утекать по каналам сотовой связи и беспроводным каналам передачи данных, а также определить возможность использования этих устройств сотовой связи на протяжении периода, равного периоду проведения подсчета до реализации мер защиты.

После реализации всех мер и проведения подсчета устройств после введения каждой из них необходимо сравнить полученные данные. Если количество пронесенных устройств сотовой связи, которые также возможно использовать на территории, на которой необходимо исключить использование этих средств, после применения защитных мер из данной методики равно нулю, то данная методика считается эффективной. В ином случае необходимо пересмотреть защитные меры.

Приложение Е

(обязательное)

Схема размещения средств защиты информации

Рисунок Е.1 - Схема размещения средств защиты информации

Приложение Ж

(обязательное)

Статистика практического исследования эффективности методики

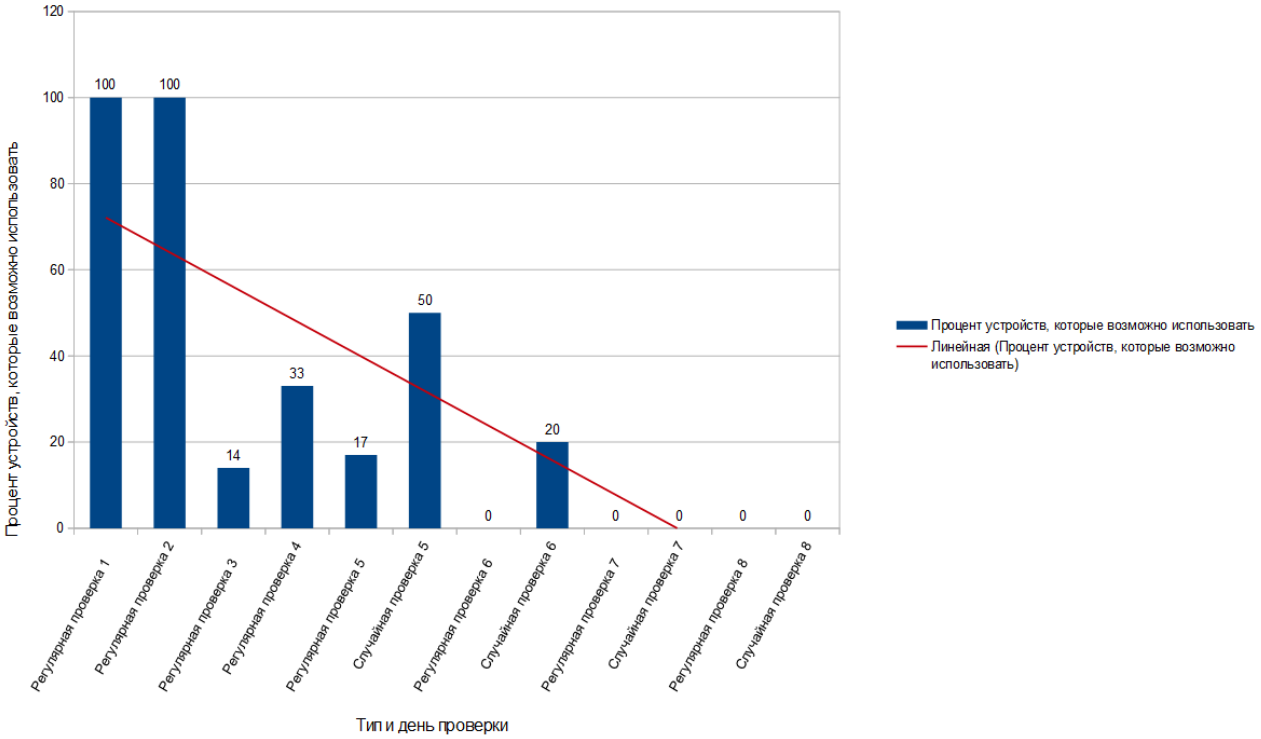

Рисунок Ж.1 — Результаты практического исследования эффективности методики

Приложение И

(обязательное)

Рекомендации по практическому применению методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных

УТВЕРЖДЕН

приказом_____

№_____

« __ » _____20__ г.

РЕКОМЕНДАЦИИ ПО ПРАКТИЧЕСКОМУ ПРИМЕНЕНИЮ МЕТОДИКИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ АО «НПП «РУБИН» ОТ УТЕЧЕК ИНФОРМАЦИИ ПО КАНАЛАМ СОТОВОЙ СВЯЗИ И БЕСПРОВОДНЫМ КАНАЛАМ ПЕРЕДАЧИ ДАННЫХ

Содержание

И.1 Область применения 92
И.2 Цель разработки 92
И.3 Рекомендации по порядку выбора защитных мер.....92
И.4 Рекомендации по реализации защитных мер.....93

И.1 Область применения методики

Данная методика предназначена для применения на АО «НПП «Рубин», а также в иных организациях, где уже осуществляется обработка информации ограниченного доступа, в том числе являющейся государственной тайной, коммерческой тайной, персональными данными, а также имеющей гриф «Для служебного пользования».

И.2 Цель разработки методики

Целью разработки методики обеспечения защиты АО «НПП «Рубин» от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных является систематизация мер защиты информации от утечки по каналам сотовой связи и беспроводным каналам передачи данных, определение условий, при которых указанные защитные меры могут быть применены, а также для помощи специалистам по информационной безопасности организаций по созданию системы защиты от утечек информации по каналам сотовой связи и беспроводным каналам передачи данных.

И.3 Рекомендации по порядку выбора защитных мер

Если на реализацию защитных мер из выбранного набора необходимо затрать большее количество финансовых средств, чем было изначально запланировано до выбора набора, то необходимо пересмотреть набор или заменить некоторые дорогостоящие меры из набора на более дешевые. Так, при реализации защитных мер «Создание структурного подразделения, осуществляющего контроль за использованием устройств сотовой связи на территорию организации» или «Назначение должностного лица от руководства организации, осуществляющего контроль за использованием устройств сотовой связи на территорию организации», функции создаваемых подразделений можно предоставить уже существующему подразделению по информационной безопасности или Службе безопасности организации. Также, мера защиты «Экранирование помещений, в которых запрещено использование устройств сотовой связи» может быть замещена мерой защиты «Использование

всенаправленных устройств блокирования работы систем мобильной связи непрерывного действия малого радиуса» и наоборот.

И.4 Рекомендации по реализации защитных мер

Выбранные защитные меры необходимо реализовывать поочередно. После реализации каждой меры необходимо проводить анализ эффективности и сравнивать эффективность период наблюдения после реализации данной защитной меры с периодом наблюдения после реализации предыдущей защитной меры, а также с периодом до реализации защитных мер. При достижении эффективности методики по критерию эффективности необходимо прекратить введение дальнейших мер защиты из набора.

При определении порядка реализации защитным мер из набора необходимо в первую очередь выбирать те защитные меры, на введение которых необходимы наименьшие финансовые затраты, и технические средства для которых уже имеются у организации.

Приложение К

(обязательное)

Протокол проверки ВКР в системе Антиплагиат