

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет информационных
технологий и электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.03 –

Информационная безопасность
автоматизированных систем

Специализация -

Защищенные автоматизированные
системы управления

ДИПЛОМНАЯ РАБОТА

на тему

Методика обеспечения защиты АО «НПП «Рубин» от утечек
информации по беспроводным каналам передачи данных на базе
технологии Bluetooth

Студент

Гусев Александр Павлович

Руководитель

Сергеев В.О.

Нормоконтролёр

Иванов А.П.

Рецензент инженер 2 кат. АО «НПП «Рубин»

Яшин Е.В.

Работа допущена к защите (протокол заседания кафедры от

Заведующий кафедрой



С.Л. Зефиров

Работа защищена с отметкой

(протокол заседания ГЭК

от 28.06.23 № 10)

Секретарь ГЭК

А.П. Иванов

Пенза 2023

Оглавление

Введение.....	2
1. Методика обеспечения защиты АО «НПП «Рубин» от утечек информации по беспроводному каналу передачи данных на базе технологии Bluetooth.....	4
1.1 Область применения методики.....	4
1.2 Цель разработки методики.....	5
1.3 Определение угроз.....	6
1.4 Определение уязвимостей.....	8
1.5 Определение нарушителей.....	12
1.6 Описание алгоритма выбора защитных мер методики.....	12
1.7 Выбор защитных мер, используемых в методике.....	19
1.8 Выявленные наборы защитных мер в зависимости от условий функционирования организации.....	21
1.9 Описание критерия эффективности методики.....	27
1.10 Описание процедуры анализа эффективности методики.....	28
2. Проведение экспериментальных исследований методики на эффективность, оценка результатов практического исследования.....	34
3. Рекомендации по практическому применению методики.....	44
4. Вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	48
Заключение.....	52
Список использованных источников.....	55
Приложение А. Обязательное. Схема возможной утечки информации по беспроводному каналу передачи данных на базе технологии Bluetooth.....	59
Приложение Б. Обязательное. Результаты практического исследования эффективности методики.....	60

Введение

В современном информационном обществе защита конфиденциальности и целостности данных становится все более актуальной задачей. Компании, особенно те, которые работают с ограниченным доступом к информации, сталкиваются с угрозами утечки данных через беспроводные каналы передачи данных на базе технологии Bluetooth. Данная дипломная работа посвящена разработке методики, которая позволит обеспечить безопасность информации от утечек по беспроводному каналу Bluetooth на базе предприятия АО «НПП «Рубин», а также ее исследованию.

Целью было поставлено разработать в выпускной квалификационной работе методику, которая позволит обеспечить защиту АСУ АО «НПП «Рубин» от утечек информации по беспроводным каналам передачи данных на базе технологии Bluetooth. А также разработка рекомендаций для практического применения методики обеспечения безопасности информации беспроводных сетей передачи данных на базе технологии Bluetooth.

Во время разработки данной методики была определена область, в которой она будет применена, а также ее цель. Исходя из того, что АСУ АО «НПП «Рубин» является режимным предприятием, должны быть определены возможные нарушители, которые могут воспользоваться описанными при исследовании уязвимостями, тем самым создавая определенные угрозы конфиденциальности информации являющейся экономической и интеллектуальной ценностью компании.

Для достижения поставленной цели был составлен алгоритм, по которому осуществляется выбор защитных мер в зависимости от того в каких условиях функционирует организация.

Из-за необходимости определения применимости методики на АСУ АО «НПП «Рубин», была проведена процедура анализа, выявляющего эффективность методики по разработанным критериям. Для этого были

проведены экспериментальные исследования и приведены результаты практических исследований для оценки эффективности.

В целях обеспечения удобства работы с методикой специалистов по защите информации были определены влияющие на опорно-двигательный аппарат вредные психофизиологические факторы, а также методы и средства физической культуры, которые помогут снизить их воздействие. Вместе с этим были приведены рекомендации для применения методики на практике.

1. Методика обеспечения защиты АО «НПП «Рубин» от утечек информации по беспроводному каналу передачи данных на базе технологии Bluetooth

1.1 Область применения методики

Использование методики возможно на таких предприятиях как «НПП «Рубин» или в схожих с ней организациях. Данные организации используют такую методику для обработки информации, находящейся в ограниченном доступе. Информация в ограниченном доступе включает в себя не только коммерческие и государственные секреты, но также и информацию, записанную только для пользования в служебных целях или информацию о персональных данных.

Информация из ограниченного доступа описана в законе ФЗ-149. Его основной задачей является регулирование работы организаций, занимающихся сбором и созданием информации. В данном случае подразумевается информация, находящаяся в ограниченном доступе согласно законодательству Российской Федерации.

Распространение такой информации карается уголовным наказанием. Для того, чтобы обозначить какая информация является секретной, нужно обратиться к документам, описывающим права и свободы человека. Сохранение секретной информации влияет на территориальную целостность государства, влияет на беспристрастность судебной системы, кроме того, такая информация обеспечивает права и свободы граждан, она способна влиять на количество преступлений в стране и на людей, обеспечивающих порядок в стране.

Таким образом, методика, предназначенная для таких организаций как «НПП «Рубин» имеет возможность сохранить секретную информацию, тем самым создать безопасные условия для граждан страны и для служащих правопорядка.

1.2 Цель разработки методики

Разрабатываемая методика может быть использована на АО «НПП «Рубин» для защиты данных, передаваемых по каналам беспроводной связи. Также целью является помощь специалистам, работающим с информацией для разработки систем защиты от утечки данных. Такие каналы могут стать причиной утечки информации с помощью технологии Bluetooth. Соответственно необходимо использовать меры систематизированные специально для защиты информации или иных данных от утечек. Кроме того, утечка информации из-за недостаточной защищенности технологии Bluetooth может быть предотвращена благодаря определенным условиям, создающим возможность использования технологии без потери безопасности. Такая методика позволит работникам организации АО «НПП «Рубин» выявлять угрозы, влияющие на сетевую безопасность.

Современное развитие сетей происходит большими темпами, что приводит к тому, что появляются новые способы обхода блокираторов Bluetooth. Сами блокираторы также могут устаревать из-за чего необходимы новые методы защиты информации. Примером может являться случай, произошедший в 2020 году, который повлиял на проведение итогового государственного экзамена. В том году вышла новая модель телефонов «Honor» против которой стандартные глушители Bluetooth сигнала оказались бесполезными. Это привело к несанкционированным действиям со стороны людей, использующих данную модель телефона. Если такая же ситуация произошла бы на предприятиях, содержащих на своей территории секретную информацию, то это принесло бы негативные последствия для такой организации.

Соответственно целью данной методики является создание условий при которых секретная информация не сможет утечь или попасть к третьим лицам не из организации.

1.3 Определение угроз

Утечка информации является основным видом угроз возникающих при передаче данных на базе технологии Bluetooth. Кроме этой угрозы также существуют другие разновидности угроз, которые могут повлиять на информацию на предприятии. Угрозы возникают из-за того, что в современном мире все предприятия стараются переходить на электронные носители информации. Такая практика ускоряет скорость работы специалистов, но при этом влияет на безопасность всей системы. Данная ситуация приводит к выводу, что невозможно исключить из работы организации современные технологии из-за возможной потери производительности компании.

Утечка информации через Bluetooth также может осуществляться через лиц изначально не имеющих желание нарушить целостность безопасности на организации. Такие люди становятся «переносчиками» информации, к нарушителям при этом не понимая, как они передали эти данные. Соответственно сама организация должна предоставить все возможные способы защиты и не перераспределять ответственность за утечку информации на других лиц.

Если рассматривать предприятие АО «НПП «Рубин» и похожие на него организации, содержащие секретную информацию, то такими «переносчиками» могут стать клиенты данной организации, которые представляют собой государственные организации. Утечка информации происходит посредством людей участвующих в цепочке поставок, во время данной цепочки могут быть найдены слабые места, подходящие для кражи данных.

Например, клиенты могут использовать не безопасные сервисы для обмена данными, а сами сервисы могут иметь возможность подключаться к неограниченному количеству устройств, создавая не только угрозу для перехвата данных, но и ситуацию, в которой невозможно отследить источник

перехвата информации. Устройства созданные с целью защитить информацию могут устареть, а сервисы для перехвата информации становятся только новее и современнее. При условии, что невозможно постоянно обновлять устройства, блокирующие Bluetooth сигнал устройств, необходимо проводить анализ средств и анализ программного обеспечения предотвращающие вышеописанные риски. Кроме клиентов угрозу несут как соперничающие организации, так и преступные группировки с иностранной поддержкой. Группировки с иностранной поддержкой могут использовать устройства неизвестные для защищаемой организации, данную возможность также не стоит исключать.

Кроме клиентов и прочих людей, представляющих угрозу для безопасности, угрозами также считаются утечки из закрытых источников, утечки, созданные техническими путями, а также утечки из-за нелегального проникновения.

Другим видом угроз является утечка данных благодаря самим работникам организации, так как и клиенты, сотрудники могут не преднамеренно создать опасные условия. Это происходит из-за недостаточной осведомленности работника о правилах, действующих в стенах организации. Однако бывают обстоятельства, в которых сотрудники намеренно создают риски для организации, такие люди называются внутренними нарушителями. Целью внутренних нарушителей является разведка данных для других похожих организаций, которые хотят получить дополнительный доход с разработок компании. Основной сложностью в данном случае является тот факт, что таких нарушителей труднее всего выявить в организации, так как человеческий фактор даже при современных системах защиты остается одним из самых низко контролируемых. Кроме того, работник может иметь доступ к секретным данным или находиться на высокой должности из-за чего другие работники на более низких должностях не смогут контролировать действия внутреннего нарушителя.

1.4 Определение уязвимостей

Уязвимости включают в себя людей, работающих на территории, и ненадлежащая компетентность персонала. В первом случае потеря конфиденциальности информации из-за персонала может произойти если работники пройдут на место работы с устройствами, содержащими технологию Bluetooth, то есть если на контролируемой зоне появятся данные устройства. Во-втором случае персонал может быть, не осведомлен о всех правилах и требованиях, действующих на территории предприятия из-за чего, также происходит проникновение устройств на защищенную территорию.

Информация становится уязвимой из-за не совершенности программных средств, но не только программы могут стать угрозой. Сами люди, работающие в организации, могут навредить ей. Персонал, может быть, не ознакомлен со всеми правилами, действующими на территории или забыть их. Чтобы решить данную проблему необходимо наличие людей, следящих за сотрудниками организации, а также устраивающими регулярные проверки персонала и проверки рабочих мест сотрудников.

Места сотрудников должны соответствовать требованиям организации, так на рабочем месте не должно находиться устройств с Bluetooth, не должно быть найдено дубликатов документов, хранящихся на электронных носителях во избежание их попадания в руки третьим лицам.

Программное обеспечение на территории предприятия и соответственно на рабочем месте специалиста не должно содержать программ, не относящихся к работе специалиста, если в оборудовании присутствуют данные о других сотрудниках, то эти данные не должны попадать на другие устройства, не предназначенные для этих целей. Само оборудование должно проходить регулярную проверку или тестирование. Проверку должно проводить особое подразделение специалистов, подготовленное для данной деятельности.

Перечисленные факты приводят к тому, что для комфортной и безопасной работы организации начинать стоит с подбора специалистов. Подбор кадров происходит через собеседования, которые проводят люди, работающие в организации, затем необходим сбор данных о специалисте. Проводить собеседование должны именно работники организации для того, чтобы создать условия, максимально совпадающие с реальными условиями. Данные включают предыдущее место работы, данные о родственниках кандидата и прочие аспекты такие как психологический портрет кандидата и его эмоциональное состояние. Частичное автоматизирование данного процесса возможно создать если внедрить подготовленные тесты для кандидатов. Однако для конкретных случаев может потребоваться создание нового теста, например когда в организацию требуются специалисты области, ранее не работающие в компании.

Специалисты имеют несколько профилей подготовки, выбирать профиль стоит исходя из требований организации. Специалисты должны иметь высшее образование, допускается прохождение дополнительных образовательных курсов от университета. После поступления на работу специалисты должны пройти дополнительное обучение позволяющее разобраться в принципах работы организации. Дополнительное обучение также включает в себя объяснение новой методики или нововведений.

Обучение может проходить два этапа. На первом этапе только поступившие на работу сотрудники проходят обучение основам работы на конкретном предприятии, узнать или повторяют способы защиты данных и только после это они имеют право приступить к работе. Второй этап обучения делится на постоянно-регулярное обучение и на не постоянное обучение. В первом случае каждый работник после трех лет работы в организации должен проходить проверку на уровень знаний и умений, а также на профессиональные способности, подтверждающие его квалификацию.

Второй вариант обучения производится после появления в организации новых требований, аппаратов или программного обеспечения, с которым

должны ознакомиться как новые специалисты, так и уже опытные рабочие. Второй вариант также применяется если политика организации претерпевает изменения или в штате сотрудников появляются рабочие служащие в новых областях информационной безопасности. Первый и второй вид обучения сопровождается тестом, показывающим уровень усвоения новых знаний и требований.

После всех видов обучения работники должны проходить инструктажи, в которых рассказывается о методах безопасности на организации в случае непредвиденных ситуаций. Такие инструктажи не являются регулярными, выполняются они только после разрешения руководящих лиц организации. Основной причиной проведения инструктажей являются ситуация являющиеся опасными либо для информации на территории предприятия, либо для сотрудников компании.

После обучения работники должны быть предупреждены о возможных наказаниях если будут выявлены какие-либо нарушения безопасности организации. Данными действиями должны заниматься люди из службы безопасности. Сотрудники безопасности Российской Федерации считают, что грамотный подбор специалистов является одним из необходимых критериев подбора.

После тщательного отбора кандидатов, будущие работники обязаны будут ознакомиться с трудовым договором и поставить на нем свою подпись, сигнализирующую о том, что работник обязуется выполнять все пункты договора, а также сигнализирующую о том, что работник знает о возможных наказаниях, включающих понижение, увольнение и снижение зарплаты в случае невыполнения тех или иных аспектов договора.

Договор должен включать в себя информацию о правилах безопасности работы на территории объекта, включающие в себя право на защиту своих личных данных, право главы организации на обработку персональных данных работника, право главы организации на передачу информации о работнике третьим лицам.

Договор также должен включать правила о запрете на распространение и разглашение информации работником, находящейся под грифом «секретно». В договоре обязана присутствовать информация о наличии испытательного срока, продолжительность которого может составлять от трех месяцев. Во время испытательного срока работник должен проявить себя, во-первых, как способный работник, во-вторых, он должен подкрепить доказательствами или действиями свою возможность хранить секретную информацию. Также испытательный срок может помочь уже действующим работникам организации выявить потенциальных внутренних нарушителей.

Уменьшить уязвимости организации также можно с помощью руководителей предприятия, которые должны выдать в пользование в рабочее время секретную информацию только тем сотрудникам, которые получили официальное разрешение. Доступ к официальным секретным документам осуществляется, основываясь на сфере деятельности работника по защите информации. Это делается для того, чтоб все работники на территории не имели доступ ко всей информации. Создание таких условий приведет к тому, что работники не имеющие дополнительные полномочия не будут знать всю информацию, а значит шанс утечки данных будет снижен.

После всех мер предпринятых для выявления уязвимостей стоит использовать поощрения сотрудников для создания комфортной атмосферы в коллективе, которая также влияет на сохранность информации. К таким поощрениям относится повышение зарплаты, квартальные премии или надбавки за долгую службу. Выбор работника, который получит премию производится исходя из его знаний, из проверок, проходивших во время его работы, из данных по квартальным отчетам. Также стоит поощрить работника если тот предложил новые методы и способы защиты информации. Кроме премий финансовых также можно использовать поощрения в виде дополнительного отпуска или повышения по службе, награждение сотрудника премиями или грамотами за работу.

1.5 Определение нарушителей

Типы нарушителей приведены в таблице 1.

Таблица 1 – Типы нарушителей.

№ п/п	Тип	Цель угрозы
1	Соперничающие организации	Получение выгоды
2	Преступная группировка	Получение данных о уязвимости компании и использование их для получения денег
3	Службы с иностранной поддержкой	Получение информации способной нанести ущерб экономике, политике или иным сферам государства.

1.6 Описание алгоритма выбора защитных мер методики

Изображение алгоритма выбора защитных мер можно увидеть на рисунке 1.

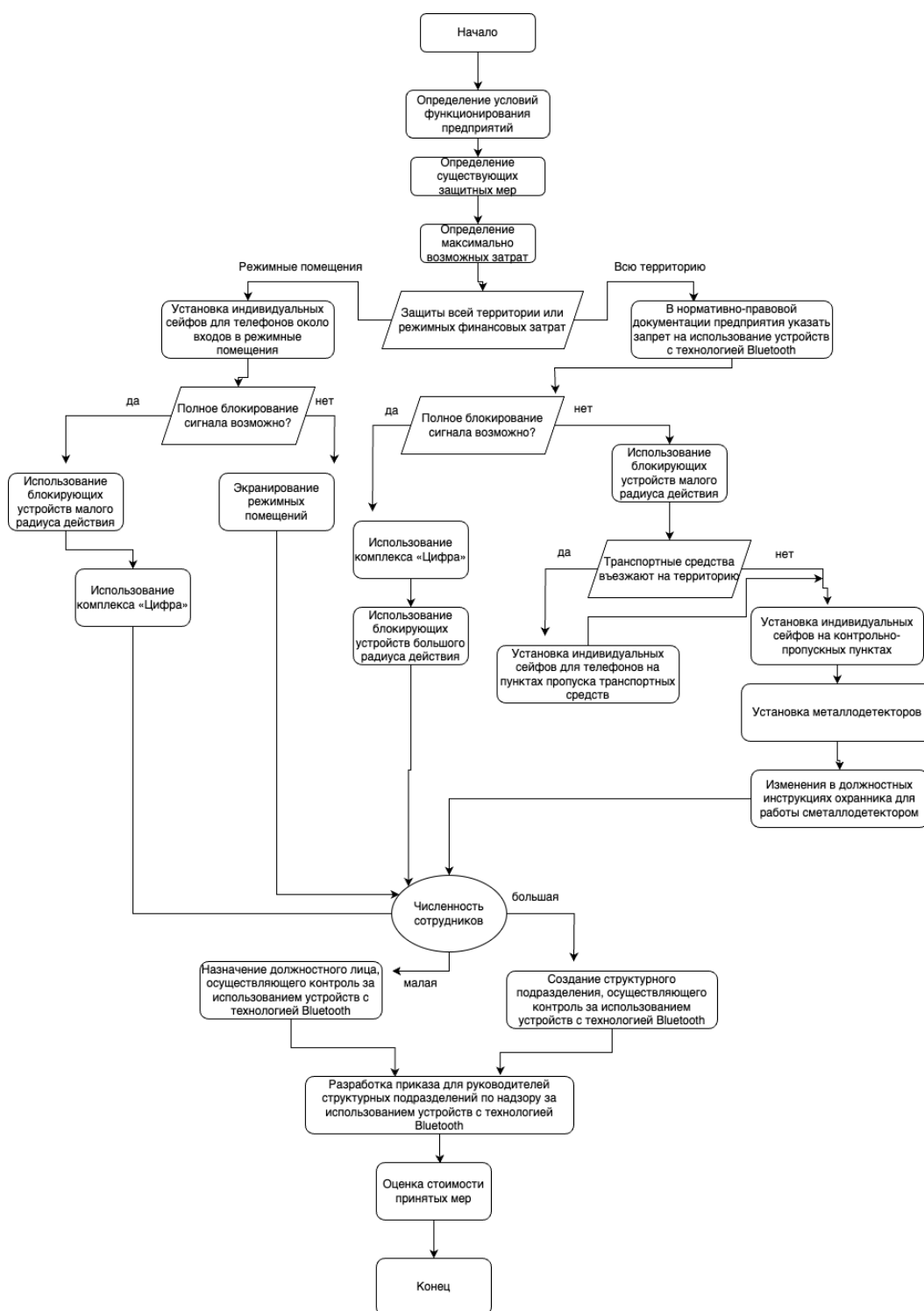


Рисунок 1 – Алгоритм выбора мер защиты

Для того чтоб анализ мер безопасности возможно было провести необходимо для начала составить анализ, который будет включать в себя все условия и факторы влияющие на работу организации, а также проверить эффективность уже существующих мер безопасности. Существующие меры безопасности описаны в разделах под названием «защитные меры», которые

применяются для защиты данных от утечки на АО «НПП «Рубин». Отдельно описаны также меры защиты информации от утечки на базе технологии Bluetooth.

После того как будут рассмотрены все меры защиты и определены все условия необходимые для функционирования, следующим этапом является оценка мер защиты и условий функционирования. Данная оценка включает в себя на финансовую сторону данных мер, а именно финансовые издержки связанные с использованием технологии Bluetooth.

Следующим этапом необходимо выявить какая область должна быть защищена, должна ли быть защищена вся территория организации или требуется защита только определенных помещений. Определяется территория, для которой будет создана защита обычно по тому, где будет происходить обработка информации с ограниченным доступом. После того как будет выбрана территория, для которой будут применяться защитные меры, данная территория должна быть включена в необходимые правовые документы.

После того, как территория внесена в правовые документы, она должна быть обеспечена общей отменой применения устройств, содержащих технологию Bluetooth. Если невозможно обеспечить полный запрет на использование устройств с Bluetooth, то в таком случае необходимо использование устройств с функцией блокировки Bluetooth, которые способны блокировать сигнал на всей необходимой территории. Схема, которая показывает данную способность представлена на рисунке 2.

Существует вариант, при котором устройства, блокирующие Bluetooth, могут помешать людям или персоналу, находящемуся за пределами организации использовать технологию Bluetooth. Такая ситуация может привести к тому, что другие организации и обычные граждане будут испытывать неудобства, а социально важные объекты станут удобными для их работников. Для того, чтобы исключить все возможные последствия от такой блокировки работы технологии Bluetooth, следует использовать устройства,

которые могут регулировать радиус своего действия или устройства с определенным, подходящим для данной организации радиусом действия.

Однако, если организация может позволить себе использовать блокирующие устройства с широким радиусом действия, организация должна использовать именно их. Такая ситуация происходит, когда необходимая для защиты территория не граничит с другими организациями, которым не требуется блокировка Bluetooth устройств.

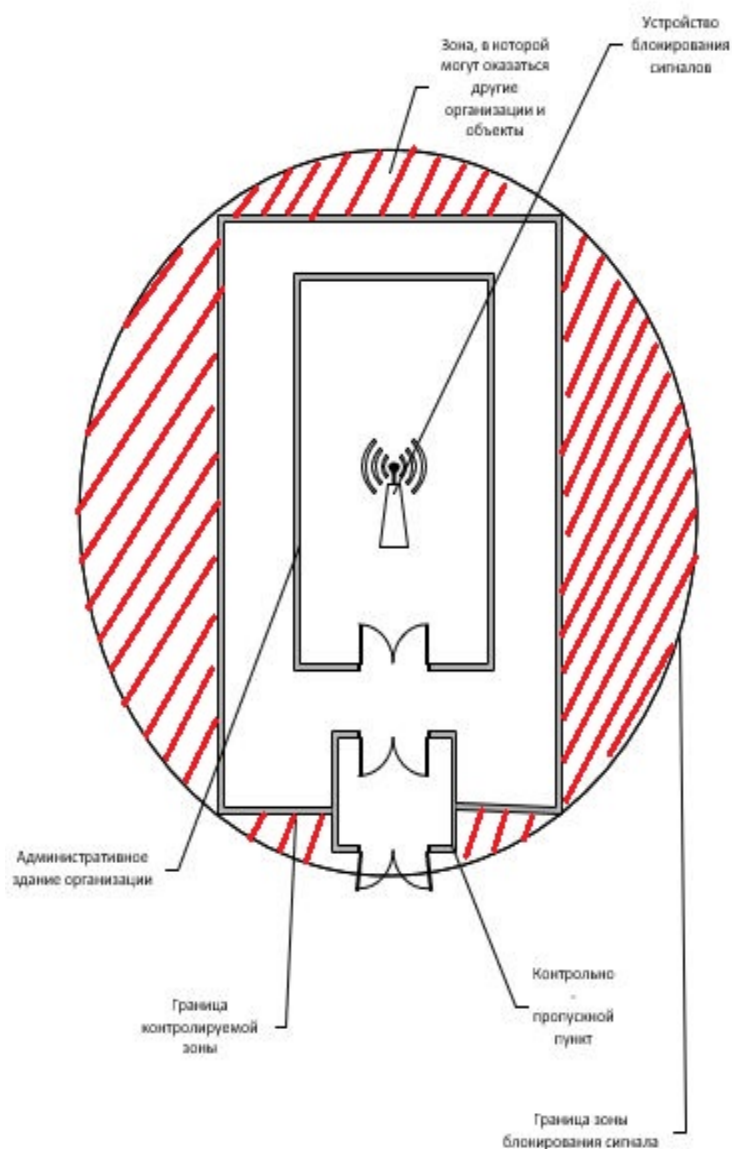


Рисунок 2 — Вариант схемы блокировки сигнала Bluetooth на планировке организации.

Средства, которые используются для блокировки Bluetooth, при этом используются с устройствами, имеющими широкий радиус, должны быть

оснащены специальным оборудованием способным автоматически находить беспроводные устройства с Bluetooth, а также блокировать их. Для достижения вышеперечисленных целей можно рассмотреть автоматизированный комплекс «Цифра». Однако также как мы описывали выше, данное устройство невозможно использовать рядом с объектами, в которых блокировка Bluetooth не предусмотрена. Это связано с тем, что устройство «Цифра» способно находить и контролировать устройства с Bluetooth на большом расстоянии. Соответственно блокировке будут подвергаться устройства как на территории под защитой от утечки информации, так и устройства, находящиеся за пределами данной территории. По этой причине использование комплекса «Цифра» не является оптимальным решением в данном вопросе, а также результаты, полученные после такой проверки, не могут считаться полностью верными.

Если присутствует риск, который влияет на работу систем других организаций, а также риск, влияющий на важные объекты социальной инфраструктуры или же если работа блокиратора может стать некомфортной для гражданских лиц, стоит отказаться от устройства с широким радиусом действия и применять устройства с меньшим радиусом или радиусом которой можно настроить под необходимые условия.

Иногда на территории организации необходимо установить контроль-пропускные пункты, через которые на территорию будет проходить транспорт. Данная ситуация может возникнуть в случае, если на всей территории должны быть условия полного блокирования Bluetooth. При условии, что установка таких пунктов по каким-либо причинам не является возможной необходимо создать условия, в которых устройства с Bluetooth будут размещаться с специально отведенных сейфов. Кроме сейфов для данных устройств возможно применение дополнительной рабочей силы, которая будет работать с металлодетекторами для дополнительной проверки лиц, проходящих на защищенную территорию. Кроме лиц также должен быть проверен и сам транспорт.

Для дополнительной защиты, которая должна быть описана в специальных требованиях и в документах самой организации, сейфы могут быть расположены не только в местах проезда автомобильной техники, но также и для персонала самого предприятия. Такие сейфы должны располагаться на входе в определенное охраняемое помещение или же на входе в само предприятие. Расположение сейфов зависит от радиуса действия зоны свободной от Bluetooth. Отдельное внимание стоит уделить персоналу, владеющему правом проходить в данные помещения.

Данные сейфы могут также называться устройствами, блокирующими работы Bluetooth с маленьким радиусом действия. Устройства с маленьким радиусом действия не смотря на свое название, также могут стать причиной неудобств для гражданских лиц и объектов инфраструктуры, особенно если эти устройства расположены около контрольно-пропускных пунктов. Для решения данной проблемы возможно использование метода экранирования помещений. При данном методе снижается интенсивность электромагнитных волн, что в свою очередь снижает электромагнитное излучение и позволяет обезопасить территорию от утечки информации.

Соблюдение всех условий, предотвращающих изменение распространения электромагнитных волн вне территории организации, то есть если граждане, городские объекты и другие не могут быть подвержены данному воздействию из-за большого радиуса действия, несущему негативные последствия для удобства перечисленных, в данном случае возможно применение устройства «Цифра». Кроме данного устройства под его характеристики и особенности использования, также подходит устройство «Сонет». «Сонет» способен также на блокировку беспроводных персональных сетей, а также на блокировку информации среди электронных устройств. Работа данного устройства осуществляется с помощью пакетной передачи данных.

Для качественной работы, соответствующей всем требованиям организации стоит выбрать человека с предприятия, который станет

ответственным за управление всеми перечисленными устройствами. Кроме того, данным вопросом должно заниматься специальное подразделение. Лица ответственные за данную работу должны выбираться в зависимости от количества лиц, задействованных в работе предприятия. Так если работников недостаточно, то следует привлекать к работе главного служащего в организации, а если число работников позволяет использовать больше одного человека, то организация должна определить группу людей ответственных за данную работу.

Работа в данной группе лиц должна быть подвержена надзору, за который отвечают лица из других подразделений. Таким образом будет создана подходящая защита на всех уровнях. Документ, регламентирующий работу или приказ разрабатывается руководством. Созданный приказ сможет регламентировать все уровни предприятия, работающего в зоне свободной от Bluetooth и соответственно простираться на все структуры.

Все условия и требования не могут быть использованы если финансовая сторона данных установок, нанимаемых работников не согласуется с возможностями предприятия. Финансовые затраты включают в себя все ресурсы отображающиеся на балансе организации под конец года. Для этого стоит рассмотреть возможности и целесообразность внедрения всех аспектов. Порядок рассмотрения финансового аспекта начинается с разработки предельно возможной суммы затрат предприятия для защиты информации от утечки с помощью Bluetooth. В случае если организация не может предоставить необходимой суммы для защиты информации, возможно перераспределение финансов в самой организации. Если невозможно перераспределение финансов, то следует выбрать необходимый минимум средств, обеспечивающий защиту информации от утечек с помощью Bluetooth.

1.7 Выбор защитных мер, использующихся в методике

Выбор защитных мер на АО «НПП «Рубин» предполагает, что меры должны включать в себя определенную организацию, подходящие техническое оснащение. Не все меры применяемые для защиты АО «НПП «Рубин» являются оптимальными, поэтому также нужно определить почему были выбраны именно такие меры.

Во-первых, следует рассмотреть, как организационные меры могут повлиять на передачу информации на защищенных территориях. Методика предлагает такие защитные меры, которые включают в себя:

1) индивидуальные сейфы. Индивидуальные сейфы, располагающиеся на тех местах, где осуществляется пропуск людей способны исключить риск попадания такого устройства внутрь охраняемого здания. Также данные сейфы могут располагаться в метрах проезда машин на территорию, это в свою очередь обеспечит сохранение конфиденциальности информации, которое может быть нарушено из-за проникновения устройств с Bluetooth через транспорт. Последним местом, где следует расположить сейфы являются индивидуальные помещения;

2) металлодетекторы. Металлодетекторы и специально подготовленные люди с ними должны располагаться там, где проходит большой поток людей;

3) поправки в инструкции. Персонал и работники, соприкасающиеся с зоной, где действует ограничение на использование Bluetooth должны быть ознакомлены со всеми необходимыми инструкциями;

4) разработка приказа. Руководство должно проводить надзор за работниками, объединенными в структуры отвечающие за сохранение информации;

5) структурное подразделение. Работники данной структуры контролируют людей, использующих технологию Bluetooth на защищенной территории;

6) должностное лицо. Оно должно быть выбрано руководителем организации с целью контроля устройств с Bluetooth;

7) запрет на устройства с Bluetooth.

Во-вторых, следует рассмотреть, как технические меры могут повлиять на передачу информации на защищенных территориях. Методика предлагает такие технические меры, которые включают в себя:

1) всенаправленные устройства блокирования. Данные устройства из-за своего радиуса подавления устройств, а также благодаря непрерывности работы большого радиуса способны создать необходимые условия для работы систем секторной диаграммы. Кроме устройств блокирования большого радиуса также возможно применение устройств с небольшим радиусом действия;

2) автоматическое распознавание устройств с Bluetooth. Такие устройства включают в себя такой аппарат как «Цифра»;

3) экранирование помещений. Позволит обеспечить безопасность охраняемой зоны.

В-третьих, следует рассмотреть, как защитные меры могут повлиять на передачу информации на защищенных территориях. Методика предлагает отказаться от использования следующих защитных мер:

1) режим контроля доступа. Недостаточное количество оснований, по которым контроль доступа следует применять. Это связано с тем, что уже применено достаточное количество защитных мер от потери конфиденциальности информации;

2) информирование за вознаграждение. Данное решение не стоит применять из-за того, что это может повлиять на коллектив, работающий в данной организации, а также такое решение принесет определенные финансовые потери.

3) звукоизоляционные в помещения. Не следует применять звукоизоляционные помещения из-за того, что все необходимые меры уже были приняты и данное решение не способно улучшить защиту организации.

4) запрет на Bluetooth устройства в смежных помещениях. В данных помещениях проводится отбор информации с ограниченным доступом. Применение данной методики не целесообразно потому, что в данных организациях уже приняты все необходимые меры защиты от утечки информации.

1.8 Выявленные наборы защитных мер в зависимости от условий функционирования организации

Наборы защитных мер должны обеспечить безопасность защиту информации в определенных условиях. Данные условия варьируются в зависимости от числа работников, от конкретного места обеспечения безопасности и от возможности или не возможности использования блокирующих систем. Таким образом, при комбинировании данных факторов получается десять условий для которых должны применяться свои меры безопасности.

Первое условие включают в себя возможность использования блокирующих устройств на территории, которая расположена за пределами организации и с маленьким числом сотрудников. В такой ситуации стоит убедиться, что режимные помещения оборудованы индивидуальными сейфами, которые могут хранить устройства с Bluetooth технологией. Кроме сейфов, которых недостаточно для создания полной безопасности предприятия из-за возможности умышленного использования или проноса данных устройств следует установить устройства, созданные специально для блокировки подобных систем, которые могут работать непрерывно, но при этом иметь небольшой радиус.

После того как будут установлены все устройства, блокирующие Bluetooth следует отследить, было ли совершено незаконное проникновение на территорию с Bluetooth устройствами, для этого используется комплекс «Цифра». Отследив все устройства с Bluetooth выше строящие члены организации должны назначить человека, задачей которого будет контроль

всех аппаратов с Bluetooth на защищенной территории. Такой работник будет подчиняться приказу, созданному руководителями предприятия. Приказ регламентирует все действия сотрудников, связанных с контролем устройств с Bluetooth на территории.

Второе условие включает в себя возможность использования устройств, подавляющих работу Bluetooth в пределах организации, но при большом числе сотрудников. В таком случае меры безопасности включают в себя использование сейфов, находящихся рядом с режимными помещениями. Также как в предыдущем условии следует использовать непрерывно действующие устройства малого радиуса блокирования Bluetooth. Комплекс «Цифра», работающий на поиск электронных устройства с беспроводной связью.

Также при таких условиях работы организации следует формировать структурное подразделение, работающее с Bluetooth устройствами, которое способно контролировать данные устройства, если они были найдены на территории. Задачей руководителей организации в таких условиях является создание подходящих структурных организаций, а также создание приказа, включающего в себя все меры предпринимаемые для защиты информации на территории организации. Основной частью такого указа должна стать возможность устанавливать контроль за применением Bluetooth.

Третье условие содержит в себя такие факторы как невозможность применения устройств, блокирующих Bluetooth на территории организации. За пределами организации не должно создаваться помех, мешающих обычным гражданам или иным организациям, в которых допускается использование Bluetooth, при этом на самой организации, защищенной от использования Bluetooth в распоряжении, находится недостаточное или малое число сотрудников. При таком условии используются такие защитные меры как индивидуальные сейфы, которые находятся в режимных помещениях и которые могут хранить устройства с Bluetooth технологией.

Использование сейфов поможет предотвратить проникновение устройств с Bluetooth через работников, однако при умышленном проникновении таких устройств на территорию стоит экранировать помещения. Вышестоящие должностные лица, находящиеся у руководящих позиций в организации, должны контролировать аппараты с Bluetooth. Сами руководители в таких условиях создают приказ, контролирующий подразделения защиты информации на территории свободной от Bluetooth. Также они осуществляют дополнительный надзор.

Четвертое условие содержит в себе такие факторы как невозможность использования блокираторов, находящихся вне территории, но при условии, что на предприятии задействовано оптимальное или большое число сотрудников. При таком условии используются такие защитные меры как индивидуальные сейфы, которые находятся в режимных помещениях и которые могут хранить устройства с Bluetooth технологией.

Использование сейфов поможет предотвратить проникновение устройств с Bluetooth через работников, однако при умышленном проникновении таких устройств на территорию стоит экранировать помещения. Также при таких условиях работы организации следует формировать структурное подразделение, работающее с Bluetooth устройствами, которое способно контролировать данные устройства, если они были найдены на территории. Задачей руководителей организации в таких условиях является создание подходящих структурных организаций, а также создание приказа, включающего в себя все меры предпринимаемые для защиты информации на территории организации. Основной частью такого указа должна стать возможность устанавливать контроль за применением Bluetooth.

Пятое условие должно включать в себя возможно проезда транспорта на территорию, при этом блокирующие устройства используются по всей территории организации, однако на организации находится недостаточное или малое число работников. При таких условиях следует использовать такие

меры защиты как нормативно-правовые документы. Данные документы подтверждают невозможность проникновения, использования и работы устройств с технологией Bluetooth на территории организации. Следует использовать непрерывно действующие устройства малого радиуса блокирования Bluetooth. В такой ситуации стоит убедиться, что режимные помещения оборудованы индивидуальными сейфами, которые могут хранить устройства с Bluetooth технологией.

Данные сейфы согласно нормативно-правовым документам располагаются на контрольно-пропускном пункте. Сами пропускные пункты должны быть оснащены специальным оборудованием, таким как металлодетекторы, а также в таких местах должны находиться специально обученные люди. Работник организации, выбранный вышестоящими лицами, должен отвечать за применение технологии Bluetooth на самой территории. Задачей руководителей организации в таких условиях является создание подходящих структурных организаций, а также создание приказа, включающего в себя все меры предпринимаемые для защиты информации на территории организации. Основной частью такого указа должна стать возможность устанавливать контроль за применением Bluetooth.

Шестое условие включает в себя особенности проезда транспорта на территорию, в которой используются блокирующие устройства Bluetooth, но при наличии достаточной или большой численности сотрудников предприятия. При таких условиях в контролируемой зоне должны действовать правовые документы, в которых запрещается использование и проникновение Bluetooth устройств на территорию. Следует использовать непрерывно действующие устройства малого радиуса блокирования Bluetooth.

В такой ситуации стоит убедиться, что режимные помещения оборудованы индивидуальными сейфами, которые могут хранить устройства с Bluetooth технологией. Также данные сейфы должны находиться не только на контрольно-пропускном пункте, но также такие пропускные пункты следует оборудовать металлодетекторами и специально обученными людьми.

Задачей руководителей организации в таких условиях является создание подходящих структурных организаций, а также создание приказа, включающего в себя все меры предпринимаемые для защиты информации на территории организации. Основной частью такого указа должна стать возможность устанавливать контроль за применением Bluetooth.

Седьмое условие включает в себя запрет на использование блокираторов за территорией предприятия, а также ограниченном передвижении транспорта на территорию, при условии количество работников мало или недостаточно. В таких случаях мерами безопасности будет использование таких мер защиты как нормативно-правовые документы. Данные документы подтверждают невозможность проникновения, использования и работы устройств с технологией Bluetooth на территории организации. Должны быть предоставлены специальные блокираторы подобных систем, которые могут работать непрерывно, но при этом иметь небольшой радиус. Также стоит убедиться, что контрольно-пропускные пункты оборудованы индивидуальными сейфами, которые могут хранить устройства с Bluetooth технологией. Также данные сейфы должны находиться не только на контрольно-пропускном пункте, но также такие пропускные пункты следует оборудовать металлодетекторами и специально обученными людьми.

После этого стоит изменить должностные инструкции для данных людей. Вышестоящие лица должны определить работника задачей которого будет контроль и осмотр устройств с Bluetooth на территории. Задачей руководителей организации в таких условиях является создание подходящих структурных организаций, а также создание приказа, включающего в себя все меры предпринимаемые для защиты информации на территории организации.

Восьмое условие включает в себя ситуацию в которой на территории организации использование блокираторов не предоставляется возможным, а также невозможно применение блокираторов вне территории организации, транспорт не имеет возможность проезжать в контроль-пропускные пункты, а число работников небольшое либо достаточное для данного предприятия. В

таком случае средствами защиты станут нормативно-правовые документы, в которых прописаны запреты, включающие запрет на устройства с Bluetooth на территории. Должны быть предоставлены специальные блокираторы подобных систем, которые могут работать непрерывно, но при этом иметь небольшой радиус. В такой ситуации стоит убедиться, что место оборудовано индивидуальными сейфами, которые могут хранить устройства с Bluetooth технологией. Данные сейфы согласно нормативно-правовым документам располагаются на контрольно-пропускном пункте. Сами пропускные пункты должны быть оснащены специальным оборудованием, таким как металлодетекторы, а также в таких местах должны находиться специально обученные люди. Работник организации, выбранный вышестоящими лицами, должен отвечать за применение технологии Bluetooth на самой территории. Задачей руководителей организации в таких условиях является создание подходящих структурных организаций, а также создание приказа, включающего в себя все меры предпринимаемые для защиты информации на территории организации.

Девятое условие включает в себя, во-первых, возможность использование блокираторов, во-вторых, блокираторы могут работать в пределах территории предприятия, а в-третьих, количество работников мало либо недостаточно. В данном случае защита должна осуществляться таким образом, чтобы запрет на устройства с Bluetooth был определен в специальных документах. На самой территории следует использовать аппарат «Цифра», который способен находить устройства с Bluetooth. Следует установить устройства, созданные специально для блокировки подобных систем, которые могут работать непрерывно, но при этом иметь большой радиус. При этом такие устройства будут оснащены секторной диаграммой направленности антенны. Отследив все устройства с Bluetooth выше строящие члены организации должны назначить человека, задачей которого будет контроль всех аппаратов с Bluetooth на защищенной территории. Такой работник будет подчиняться приказу, созданному руководителями предприятия. Приказ

регламентирует все действия сотрудников, связанных с контролем устройств с Bluetooth на территории.

Последним десятым условием является сочетание таких особенностей как применение блокираторов за пределами и в пределах организации, при этом на территории организации находится большое или достаточное число работников, которые могут осуществлять необходимые меры безопасности. Так мерами безопасности в такой ситуации является, во-первых, использование правовых актов, в которых запрещается использовать аппараты содержащие в себе технологию Bluetooth на всей зоне. Во-вторых, аппарат с названием «Цифра» должен будет обеспечить поиск Bluetooth устройств на территории. В-третьих, блокираторы должны быть непрерывного действия, у них должна быть секторная диаграмма, они должны обеспечить блокировку устройств на большом радиусе действия, у данного устройства должны быть направленные антенны.

После подробного описания характера и качеств устройства нужного для работы в таких организациях следует отметить, что важно не только само устройство, но люди, работающие с данными аппаратами. Так люди, работающие на таких предприятиях, должны быть организованы в структурные подразделения. Сами подразделения выбираются руководителями предприятия. Основной задачей таких подразделений станет контроль за устройствами с Bluetooth технологией. И последним пунктом станет разработка приказа, который будет регламентировать действия, осуществляющие контроль использования устройств Bluetooth. Такие приказы должны быть созданы самими руководителями предприятия.

1.9 Описание критерия эффективности методики

Описание того, насколько продуктивна и производительна данная методика, стоит начать с количества информации утерянной в ходе использования такой методики или по показателям сохранения информации, передаваемой через устройства, содержащие в себе Bluetooth технологию. Из-

за особенностей методики и времени временного промежутка ее применения не представляется возможным выявить точные данные по объему информации утерянной в организации до первичного применения методики. Однако если сравнивать количество информации, пропавшей сразу после использования такой методики и объем информации, пропавший до данной методики, можно выявить эффективные и неэффективные ее аспекты. Соответственно, если утекшей количество информации после применения методики снизилось, то данная методика может считаться потенциально успешной.

Эффективность или успешность методики может быть определена после подсчета устройств, содержащих в себе технологию Bluetooth, используемых для кражи информации. Подсчет устройств должен производиться до и после внедрения новой методики. Такие устройства включают в себя устройства, найденные на защищенной территории, но использующиеся на ней при условии отсутствия блокираторов Bluetooth. Необходимо учитывать количество таких устройств до применения и после применения методики. Соответственно если на защищенной территории после применения методики нет устройств с Bluetooth, то методика является успешной.

Таким образом, критерии эффективности методики зависят от количества информации утерянной в ходе проведения методики, влияют показатели сохранения технологии. Проводить анализ стоит до и после внедрения методики, а также нужно проводить проверки в произвольное время и в специально отведенное время. Эффективной может быть только та методика, которая обеспечивает 100 процентов сохранение информации.

1.10 Описание процедуры анализа эффективности методики

Создание безопасного пространства на территории организации требует использование защитных мер, способных противостоять утечкам информации с устройств с Bluetooth. Для того, чтобы все меры используемые для сохранения безопасности работали необходимо специальное подразделение, которое создается главой организации или если количество людей

недостаточно, то за безопасностью должен следить сам руководитель организации. Такие меры безопасности могут гарантировать организации отсутствие Bluetooth устройств на территории организации. Кроме того, такие меры могут быть полезны для поиска данных аппаратов на территории, где нельзя использовать Bluetooth устройства.

Оптимальным решением вопроса о безопасности организации является постепенное внедрение мер защиты. Методичное встраивание мер позволит увидеть количество аппаратов с Bluetooth на территории, которые могут создавать помехи для сохранения информации в пределах организации. Организация защитных мер позволит проследить как в период внедрения методики меры безопасности начинают эффективно действовать для организации. Кроме этого, также стоит выявить является ли возможным применение методики в тех местах организации, где блокирующие сигнал Bluetooth устройства запрещены. Основным моментом, который позволит отследить эффективность методики является подсчет устройств Bluetooth тем, или иным путем, появившимся на территории и устройств, влияющих на безопасность информации в организации.

Если все меры безопасности будут правильно встроены в работу системы организации, то есть если будет выявлено количество устройств Bluetooth появившихся в организации во время методики и если все меры безопасности будут внедрены в организацию, то следующим этапом можно будет сравнить все полученные данные. Оценить методику и выявить оказалась ли данная методика полезной для организации можно после того, как будет проведен подсчет найденных устройств. Эффективной методика считается только в случае полного отсутствия устройств Bluetooth, умышленно или случайно появившихся в стенах организации.

Применение данной методики возможно на таком предприятии как на АО «НПП «Рубин» или в схожих по смыслу учреждениях, где информация не должна быть доступна для каждого.

Если не использовать данную методику на АО «НПП «Рубин» и похожих предприятиях, то это может привести к потере или утечке информации через устройства содержащие технологию Bluetooth. Однако применение методики защищающей от утечки информации возможно применить, то следует определить какую цель будет преследовать данное изменение в организации предприятия. Основной целью станет защита информации, кроме этого, применение методики ограничено определенными условиями. Одним из таких условий станет внедрение руководства, обеспечивающего защиту информации от утечек с устройств с Bluetooth.

Применение методики на АО «НПП «Рубин» подразделяется на организационные меры, на меры технические, а также на меры которые по той или иной причине были отвергнуты как эффективные. Описание мер и причины отказа, также должны быть описаны, для более глубокого понимания работы методики.

Так на АО «НПП «Рубин» принимаются организационные меры, которые позволяют уменьшить или вовсе исключить появление устройств с Bluetooth на территории организации. Организационные меры насчитывают 7 основным мер защиты. Во-первых, если в организации есть места, через которые может проезжать транспорт, то в таком случае необходимо применять сейфы, внутри которых хранение устройств с Bluetooth позволит исключить возможность незаконной передачи данных третьим лицам.

Кроме самих контрольно-пропускных пунктов, данные сейфы стоит поставить рядом с режимными помещениями. Во-вторых, если установка сейфов возможна на контрольно-пропускных пунктах, то следующим этапом станет оснащение данных пунктов металлодетекторами. Грамотное использование вышеперечисленных мер позволит снизить опасные ситуации связанные с утечкой информации. Однако, недостаточно одного оборудования, также сами люди должны быть ознакомлены с оборудованием и способами его использования, для этого охранники обязаны ознакомиться с изменениями в должностных инструкциях. Сами охранники или работники,

обеспечивающие контроль за проездом автомобильной техники, должны подвергаться контролю выше стоящих подразделений. Для этого руководители от организации создают структурные подразделения, которые действуют согласно приказу, составленному самими руководителями.

Основной задачей такого структурного подразделения также является контроль использования устройств с технологией Bluetooth в стенах организации и за пределами организации. Кроме подразделений относящихся к структурному контролю устройств с Bluetooth занимается должностное лицо, выбранное руководителями. Последним пунктом методики является внедрение полного запрета на устройства с Bluetooth и их использование. Запрет должен быть подтвержден в нормативно-правовых документах.

Методика также предполагает, что организации защищаясь от утечки информации будет использовать технические меры защиты. Основными техническими мерами защиты должны быть блокирующие устройства, позволяющие непрерывно обеспечивать безопасность работы организации на всей территории. Такие устройства должны иметь большой радиус действия, а также работать с помощью секторной диаграммы.

Кроме устройств с большим радиусом, возможно также применение устройств с малым радиусом, для защиты отдельных частей организации. Как устройства с большим радиусом они должны работать непрерывно и защищать территорию от утечки информации.

После того, как все устройства с Bluetooth не смогут работать в пределах работы блокирующих устройств, можно применять аппаратный комплекс под названием «Цифра», который сможет производить поиск устройств и их идентификацию. Когда поиск устройств был успешно проведен, следующим этапом должно стать полное экранирование помещений, в которых будет производиться работа и храниться информация не должна попасть в руки злоумышленников через устройства с Bluetooth.

Все вышеприведенные меры могут защитить территорию предприятия, однако некоторые из мер могут быть излишними или не иметь достаточной

обоснованности для их применения. Меры, от которых стоит отказаться включают в себя следующие примеры:

1) режим контроля доступа. Недостаточное количество оснований, по которым контроль доступа следует применять. Это связано с тем, что уже применено достаточное количество защитных мер от потери конфиденциальности информации;

2) информирование за вознаграждение. Данное решение не стоит применять из-за того, что это может повлиять на коллектив, работающий в данной организации, а также такое решение принесет определенные финансовые потери.

3) звукоизоляционные в помещения. Не следует применять звукоизоляционные помещения из-за того, что все необходимые меры уже были приняты и данное решение не способно улучшить защиту организации.

4) запрет на Bluetooth устройства в смежных помещениях. В данных помещениях проводится отбор информации с ограниченным доступом. Применение данной методики не целесообразно потому, что в данных организациях уже приняты все необходимые меры защиты от утечки информации.

Ещё одной причиной, по которой информация с устройств Bluetooth может попасть в руки злоумышленников или быть утеряна по неосторожности персонала является Bluetooth-соединение. Данная ситуация может произойти если данные будут перехвачены злоумышленниками, с целью получения финансовой или иной выгоды для последних. Bluetooth-соединение в устройствах самой организации может быть не защищено. Перехват информации также может произойти если злоумышленники подделают передаваемые данные.

Самой часто встречающейся причиной такого перехвата данных является не осведомленность работников организации о всех требованиях необходимых для работы в зоне защищенной от Bluetooth. Работники выполняющие свои обязанности в зоне без Bluetooth устройств, могут по

неосторожности или из-за невнимательности пронести с собой данные устройства, что приведет к утечке информации. Кроме самих работников, похитить информацию с помощью Bluetooth устройств хотят различные нарушители.

2. Проведение экспериментальных исследований методики на эффективность, оценка результатов практического исследования

Меры созданные для предотвращения кражи информации должны быть не только описаны в специальных документах, но и быть проверенными на практике. Практическая проверка – это единственный вариант, при котором теоретические данные могут быть проверены практически. Если меры, предложенные для АО «НПП «Рубин» станут полезными и эффективными, то это означает их состоятельность и эффективность. Однако могут возникнуть проблемы, из-за которых проведение практической проверки станет невозможным, поэтому во избежание таких проблем было решено использовать малозатратные меры защиты.

Благодаря тому, что мы имели возможность оценить наши меры защиты на предприятии, мы провели эксперимент, который может считаться репрезентативным. Таким его делает тот факт, что все исследования могли быть детально описаны и зафиксированы. Кроме того, на предприятии имеется высокотехнологичное оборудование, сыгравшее особое значение для проверки наших теоретических наработок.

Высоко квалифицированный коллектив, многолетний опыт работы сотрудников и профессиональное оборудование, позволило создать все условия подходящие для анализа методики. Период практики в данной организации дал не только площадку для расчетов, но и опыт, который позволит в дальнейшей профессиональной жизни быть более опытным, чем другие специалисты. Рассуждая о самой разработанной методике, можно сказать, что она является эффективной и возможно для применения в похожих организациях, в которых необходимо обеспечить безопасность передачи информации через устройства с Bluetooth.

Данное практическое исследование проходило восемь дней. Был выбран именно такой промежуток времени для того, чтобы в полной мере оценить, как предложенные меры смогут повлиять на работу внутри организации, а

также увидеть, как при использовании такой методики становится проще отслеживать и блокировать устройства с Bluetooth, которые могут передавать информацию третьим лицам, не участвующим в работе организации, целью которых является незаконная утечка информации. Восемь дней были разбиты на четыре фазы, а каждая фаза для удобства была поделена на 2 дня. Времени, в которое проходила практика было достаточно для того, чтобы исполнить большинство предложенных теоретических мер.

В первый день эксперимента или на первой фазе нашего исследования необходимо выявить сколько на предприятии находится аппаратов способных тем или иным образом помешать безопасности предприятия. В рамках нашего исследования были отобраны именно аппараты, поддерживающие Bluetooth. Для этого первая фаза эксперимента была обозначена как подготовительная, за два дня были найдены все устройства, поддерживающие технологию Bluetooth, объем найденных устройств необходимо зафиксировать, для дальнейшей возможности подсчетов. Кроме того, в обязательном порядке следует выявить устройства, через которые может передаваться информация благодаря технологии Bluetooth. Выявление таких аппаратов должно проходить на территории защищенной от Bluetooth.

После оценки количества устройств с Bluetooth было выяснено, что люди, работающие на АО «НПП «Рубин» берут с собой на работу как минимум один гаджет с Bluetooth. Обозначить точное количество устройств не представилось возможным из-за того, что рабочее время сотрудников варьируется, а практика проходила в первой половине дня. Это привело к тому, что отсутствие некоторых сотрудников повлияло на точные данные о количестве устройств с Bluetooth.

Подготовительная фаза первого дня показала, что из двенадцати сотрудников данной организации на рабочем месте находились только восемь сотрудников. Различных аппаратов, содержащих в себе технологию Bluetooth, было выявлено также восемь. Анализ ситуации показывает, что данные аппараты находятся в личном использовании работников организации, а так

как защитные меры не были ещё внедрены, то все устройства потенциально могут быть источником угроз для злоумышленников.

Вторая фаза подготовки или подготовительная фаза второго дня показала, что на предприятии также не находятся все сотрудники данной организации. Исходя из выводов первого дня было выяснено, что аппараты с Bluetooth также находятся только у сотрудников в личном распоряжении. Подсчеты сотрудников, находящихся на рабочем месте, показали, что во второй день таких было десять человек. Количество людей, работающих в организации во второй день подготовительной фазы, не изменилось и также составляет двенадцать человек. Как и в первый день количество найденных аппаратов с Bluetooth равно количеству людей, находящихся на предприятии, а это значит, что было найдено десять устройств способных принести отрицательные последствия для информационной безопасности организации.

Для наглядности данных, собранных за два дня эксперимента, была составлена таблица 2.

Таблица 2 — Данные первой фазы практического исследования

День	Число работников на предприятии	Число аппаратов, поддерживающих Bluetooth, находящихся не в сейфе	Число аппаратов, поддерживающих Bluetooth, в свободном доступе	Количество аппаратов, поддерживающих Bluetooth, в свободном пользовании.
1	8	8	8	100 %
2	10	10	10	100 %

После подготовительной фазы, после которой были выделены недостатки отсутствия предложенных мер, а также описано количество устройств на предприятии, стоит переходить ко второй фазе. Во второй фазе уже стоит осуществлять внедрение защитных мер. Одной из первых мер, которые не требуют больших финансовых вложений является установка

специальных аппаратов, способных останавливать Bluetooth соединение или же сейфов.

Однако недостаточного одного факта установления данных устройств, это может не дать результата если сотрудники не будут знать о новых требованиях. Соответственно стоит провести сбор всех сотрудников, находящихся на территории и рассказать новую информацию о сейфах и их обязанностях оставлять свои устройства в данных сейфах. Такие меры позволят отследить точное количество устройств, несущих вредоносное воздействие на сохранность информации в стенах организации. Также это стало, показателем описанных в таблице 2, который показывает процент устройств, возможно принесших вредоносные последствия. Сейфы сделали возможным выявить устройства с Bluetooth на той территории АО «НПП «Рубин», где эти устройства не должны работать.

Вторая фаза состояла из двух дней. Действия первого дня ограничились вычислением количества людей в организации на момент проведения эксперимента. В первый день было выявлено девять работников, находящихся в стенах организации и соответственно десять устройств находились в сейфе. Это позволило обезопасить организацию от утечки информации, а процент устройств, оставшихся вне сейфа, составил 10 процентов, это значит, что один работник не использовал сейф.

Второй день второй фазы было выявлено, что все работники воспользовались сейфом, хранящим устройства, это означает, что процент возможной утечки информации во второй день уменьшился по сравнению с первым днем. Количество людей на рассматриваемой части предприятия составляло девять человек. Это показывает возможный потенциал методики и ее возможную эффективность.

Суммируя данные за вторую фазу исследования можно подвести итог, что все устройства были помещены в сейф, а значит возможные негативные аспекты, такие как утечка информации была предотвращена. Угроз не было обнаружено.

Данные вычисления показывают эффективность методики, однако это также значит, что можно развивать меры для защиты информации, так как если судить по первому дню второй фазы, было видно, что один работник проигнорировал меры безопасности. Данная ситуация могла сложиться из-за того, что работник мог забыть новые правила, либо человеческий фактор повлиял на исход первого дня второй фазы.

Подробное рассмотрение полученных данных показывает, что новые внедренные защитные меры, предотвращающие утечку информации с помощью устройств с технологией Bluetooth, исправно работают и обеспечивают безопасность при условии, что человеческий фактор не вредит применению методики. Это дает повод для развития или внедрения дополнительных аппаратов или средств способных предотвратить утечку информации.

Таблица 3 — Данные второй фазы практического исследования

День	Число работников на предприятии	Число аппаратов, поддерживающих Bluetooth, находящихся не в сейфе	Количество аппаратов, поддерживающих Bluetooth, в свободном доступе	Количество аппаратов, поддерживающих Bluetooth, в свободном пользовании
3	9	0	0	0 %
4	10	1	1	10 %

Третья фаза была использована для дополнительной проверки влияния человеческого фактора на безопасность работы организации. Для того, чтобы получить наиболее объективные данные во время третьего этапа все сотрудники были ещё раз проинформированы о новых правилах пользования устройств, содержащих в себе технологию Bluetooth. Такая мера позволит предостеречь возможность того, что работники забудут о новых правилах. Таким образом мы получим данные о том, что работники либо намеренно

игнорируют новое правило, либо по неосторожности нарушают их. Эти данные важны, так как это даст понимание о эффективности методики.

В первый день третьей фазы, а значит уже на пятый день эксперимента на предприятии находилось десять человек. Соответственно ожидалось, что в сейфе будет находиться десять устройств, но оказалось, что устройств способных передавать сигнал Bluetooth и нарушить безопасность на территории организации, было всего семь. Это показывает, что три человека не воспользовались сейфом и это составляет 30 процентов устройств. Такие данные были получены в тоже самое время, в какое эта проверка была проведена в предыдущие четыре дня. Затем в этот же день была проведена повторная проверка, но уже вовремя в которое работники не привыкли оставлять свои Bluetooth устройства. Эти данные показали, что из семи присутствующих сотрудников, только два человека не воспользовались сейфом, а значит 28 процентов устройств могли быть использованы для опасной для информации деятельности на территории организации.

Второй день третьей фазы, а значит уже шестой день эксперимента показал результаты, в которых из одиннадцати сотрудников на территории предприятия все одиннадцать устройств были найдены в сейфе, это означает, что не одно устройство не смогло бы навредить целостности информации на предприятии. Данная проверка проводилась в первой половине дня, когда все работники были предупреждены о необходимости использовать сейфы для сохранения конфиденциальности информации и защиты её от утечки третьим лицам.

Затем была проведена повторная проверка, в которой участвовало девять человек, так как именно столько работников находилось на предприятии в тот период. Повторная проверка проводилось вовремя, когда сотрудники не ожидали, что проверка продолжается. Такая ситуация дала возможность установить более точные данные о количестве Bluetooth устройств в защитных сейфах. По результатам проверки два устройства не

были обнаружены в сейфе, а значит 22 процента аппаратов могли нанести вред информации.

Обобщить результаты третьей фазы исследования позволит систематизация данных в таблице 4. Использование таблиц в данном случае является логичным способом суммировать наши исследования в этот период времени. Показатели не только показывает работу методики и то в каком направлении стоит развивать данную методику.

Таблица 4 — Данные третьей фазы практического исследования

Ден ь	Время проверки	Число работник ов на предприя тии	Число аппаратов, поддерживаю щих Bluetooth, находящихся не в сейфе	Количество аппаратов, поддерживаю щих Bluetooth, в свободном доступе	Количество аппаратов, поддерживаю щих Bluetooth, в свободном пользовании
5	Проверка в обычное время	10	3	3	30 %
	Проверка в нерегуляр ное время	7	2	2	28 %
6	Проверка в обычное время	11	0	0	0 %
	Проверка в нерегуляр ное время	9	2	2	22 %

Четвертая фаза эксперимента состояла из двух дней, которые были в общей сложности уже седьмым и восьмым днем эксперимента. Целью четверного дня стала установка аппарата под названием «Мозаика-7К». Данный аппарат способен создать условия, при которых все устройства, использующие Bluetooth для незаконных действий. Особенностью данного аппарата является его удобство в использовании, что позволяет снизить трудности, связанные с использованием данного аппарата. Также как в предыдущей фазе будет проведено две проверки, для получения более достоверных данных.

Первый день четверной фазы начался с выявления количества работников и аппаратов, содержащих технологию Bluetooth. Так было насчитано десять работников предприятия АО «НПП «Рубин» из двенадцати. Сейфы, установленные в организации, насчитывали также десять устройств с поддержкой Bluetooth. Это означает, что все работники ответственно подошли к введенным мерам, но кроме этого, установка нового аппарата под названием «Мозаика-7К», исключила возможность использования устройств с Bluetooth. Такие данные были получены после проверки в то время, когда люди организации ожидают ее. Вторая проверка проводилась в случайное время, она проходила уже после обеденного времени, в этот промежуток на территории находилось семь человек, и каждый работник воспользовался сейфом, хранящим Bluetooth устройства. При условии, что было использовано дополнительное оборудование в виде «Мозаика-7К» не одно устройство не могло быть использовано для передачи информации через Bluetooth.

Второй день четверной фазы является последним в данном эксперименте. На протяжении всего дня было проведено 2 проверки, первая в первой половине дня, а вторая проверка в после обеденное время. Во время первой проверки на территории находилось двенадцать сотрудников организации. Проверка сейфа показало наличие двенадцати устройств с поддержкой технологии Bluetooth. Вторая проверка показала, что в ней участвовало одиннадцать человек из коллектива, а в сейфе было также

найдено одиннадцать устройств. По мимо сейфов в последний день также использовался аппарат «Мозаика-7К».

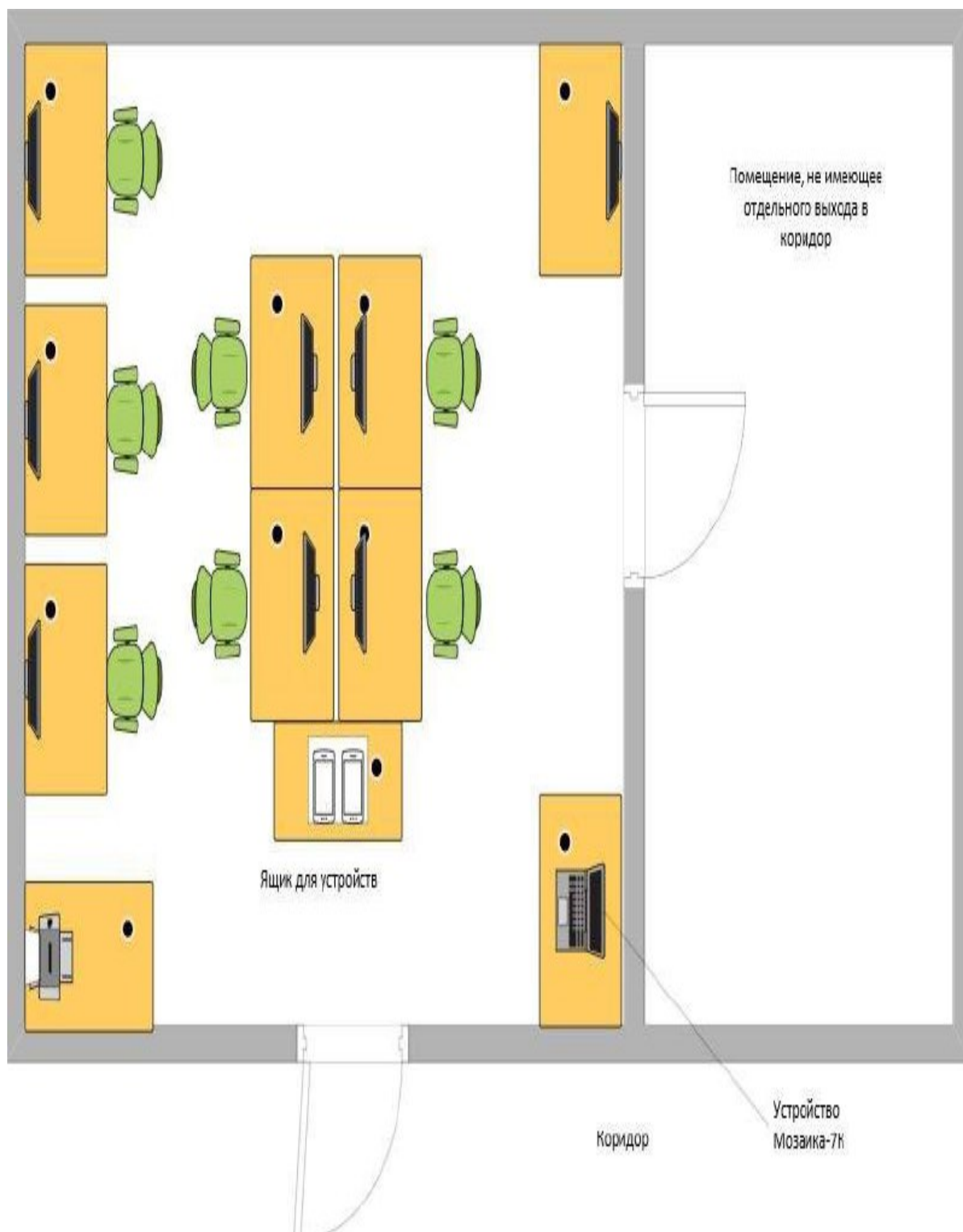


Рисунок 3 – Схема размещения средств защиты информации

На данном рисунке можно увидеть в каком порядке и как стоит расположить аппараты предназначенные для защиты информации от утечки

данных с помощью устройств с Bluetooth. Проверка всех данных позволило составить таблицу 5, в которой описан итог такой проверки.

Таблица 5 — Данные четвертой фазы практического исследования

День	Время проверки	Число работников в на предприятии	Число аппаратов, поддерживающих Bluetooth, находящихся не в сейфе	Количество аппаратов, поддерживающих Bluetooth, в свободном доступе	Количество аппаратов, поддерживающих Bluetooth, в свободном пользовании
7	Проверка в обычное время	10	0	0	0 %
	Проверка в нерегулярное время	7	0	0	0 %
8	Проверка в обычное время	12	0	0	0 %
	Проверка в нерегулярное время	11	0	0	0 %

3. Рекомендации по практическому применению методики

Практическое применение методики может показать недостатки такой методики, а это в свою очередь должно привести к новому взгляду на данную методику, который будет выражаться в создании рекомендаций. Рекомендации создаются после оценки состояния организации, то есть если после применения методики информация все же имеет возможность попасть к третьим лицам, то на это стоит обратить внимание и добавить либо новые требования, либо технологии.

Создание рекомендаций и дополнений в методику может основываться не только на данных, полученных после проведения эксперимента, но также на данных, полученных после оценки финансовой стороны организации. Возможности организации играют одну из важнейших ролей в решении по поводу внедрения методики. Расчет необходимой суммы вычисляется после того, как будет подсчитаны все возможные расходы, которые включают в себя оборудование. Оборудование может стать самой большой статьёй расходов, его настройка может потребовать приглашение дополнительных специалистов. Если учесть все эти факторы, а также учесть время, потраченное на обучение персонала, можно выяснить сколько денег потребуется для внедрения методики.

Если складываются обстоятельства, в которых невозможно выделить достаточное количество средств, то стоит обратить внимание на уже присутствующие аппараты и аппаратные комплексы на территории организации. Комбинирование уже имеющихся технологий с дополнительным финансовыми средствами, может положительно повлиять на развитие безопасной среды в организации.

После выбора наиболее подходящего варианта из предложенных в рекомендациях и их комбинация с финансами в организации, создается оптимальный вид защитных мер. В ситуации, когда на территории предприятия нет оборудования, которым можно заменить то, что прописано в

рекомендациях и методике, а финансовый аспект не позволяет выделить приобрести новое оборудование, стоит модернизировать уже существующие рекомендации, таким образом, чтоб они были выполнимыми. Примером тому может служить ситуация в которой на территории организации нет средств для создания нового структурного подразделения и найма новых сотрудников. Составители рекомендаций должны учитывать такой вариант развития и предусмотреть возможность руководителя поручить уже существующим работникам информационной безопасности новые полномочия. Другой ситуаций может стать нехватка денег на экранирующее устройство. В таком случае стоит отказаться от экранирования и воспользоваться заменой, которой может стать блокиратор Bluetooth малого или большого радиуса.

Когда выбор средств и подсчет возможностей организации будет выполнен стоит переходить к следующему шагу, а именно введение рекомендаций в работу на территории. Внедрение должно производиться постепенно, после каждого реализованного нововведения стоит проводить анализ. Производить такие нововведения стоит до того момента пока внедрение новых методов защиты не перестанет приносить лучшие результаты.

Порядок внедрения мер строго определен финансовой стороной. Если применять сначала более дорогие варианты из методики, то это может отразиться на бюджете при этом не принести нужных результатов. Соответственно сначала стоит начать с более экономичных вариантов.

Следующие рекомендации подойдут для АО «НПП «Рубин», они разработаны специально для этой организации или похожих не неё организаций, в которых находится информация, которая не должна выходить за территорию организации, то организации, в которых могут работать работники информационной безопасности.

Рекомендации для АО «НПП «Рубин» создаются единой целью предотвращения потери данных. Данная цель включает в себя такие аспекты как защита информации от утечки и кражи через Bluetooth соединения,

включает в себя аспекты возможности применения методики. Также она акцентирует свое внимание на технике необходимой для работы специалиста, а именно на её подборе, стоимости техники и возможности комбинирования техники способствующей безопасному нахождению информации в стенах организации.

Рассматривая рекомендации для АО «НПП «Рубин» также следует обратить внимание на финансовую сторону вопроса. Предприятие не всегда способно обеспечить все необходимое для внедрения новых рекомендаций. Стоит учитывать это и быть готовым к поправкам. Например, если методика предлагает использовать устройство, блокирующее Bluetooth под названием «ЛГШ-725», которое обладает рядом преимуществ перед другими видами блокираторов, но организация не может выделить достаточно средств на ее покупку, то можно предложить более дешевые варианты. Таким вариантом может стать устройство под названием «ЛГШ-723» или «ЛГШ-716». Цена данных аппаратов в два раза меньше, чем цена предыдущего аппарата, но при этом они могут выполнять такую же функцию, как и первый.

Продолжение рассмотрения аппаратов может привести к мысли что, если выбирать между аппаратами с большим радиусом и малым радиусом, стоит выбрать аппарат большого радиуса. Большой радиус действия прибора позволит использовать только один прибор, вместо двух или трех, что станет также менее затратно для организации.

Рекомендации стоит использовать последовательно, а это означает, что если сначала использовать сейфы, которые глушат сигнал устройств с Bluetooth, а потом использовать блокираторы сигнала Bluetooth, то дальнейшие устройства и нововведения могут оказаться излишними, что также сократит расходы организации.

Таким образом, можно сказать, что методика является начальным этапом создания охраняемой зоны. Методика не может быть эффективной без её практического применения, а практическое применение не является последним этапом в разработке оптимальной по стоимости и эффективности

методики. Внедрения должны происходить постепенно, необходим анализ ситуации, а также финансовые расчеты.

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

В процессе профессиональной деятельности специалист по защите информации может столкнуться с различными психофизиологическими факторами, влияющими на опорно-двигательный аппарат, которые могут плачевно сказаться на качестве проводимой работы специалистом, а также на его здоровье. К такого рода факторам можно отнести следующие:

- продолжительное пребывание в положении сидя. Специалисту по защите информации может понадобиться много времени проводить за различной аппаратурой, при этом находясь в сидячем положении, а это может привести к различным негативным последствиям для опорно-двигательного аппарата специалиста. Наиболее подверженными участками являются мышцы спины и шеи.

Работая много времени в сидячем положении и не поддерживая правильную осанку, мышцы спины, шеи и плеч специалиста будут находиться в постоянно напряженном состоянии. Длительное нахождение мышц в неподвижном состоянии приводит к тому, что они перенапрягаются и это может вызвать неприятные ощущения и боли в этих областях.

Кроме того, малоподвижный образ жизни, связанный с длительным пребыванием в неподвижном состоянии, может способствовать развитию проблем, связанных с циркуляцией крови в организме и ухудшению общей физической формы. Это может привести к ощущению общей усталости, снижению энергии и ухудшению работоспособности специалиста.

Еще одними не мало значимыми негативными последствиями, связанными с малоподвижной деятельностью специалиста по безопасности, являются возможные проблемы с нарушением правильной циркуляции крови в организме человека, а также общее снижение физической формы;

- монотонная повторяющаяся работа. Причиной повышенного напряжения определенных групп мышц и суставов, а также возможных в последствии повреждений связок и сухожилий может стать выполнение однообразного спектра задач;

- неправильная эргономика рабочего места. Специалист по информационной безопасности может столкнуться с такой ситуацией в которой его рабочее место не будет подходить ему по эргономике. Примером может стать неправильное расположение оборудования или неправильная организация рабочего места. Кроме самого места, сам специалист во время работы может выбрать неподходящее положение, что приведет к проблемам, связанным с опорно-двигательным аппаратом.

Если составные части аппаратуры, с которой работает специалист, находятся на не комфортном расстоянии, то это может привести к болям в руках и напряжению глаз. Также, неправильно подобранная высота рабочего стола, может вызвать напряжение и болевые ощущения в мышцах спины и шеи;

- освещение. Проблемы с освещением являются частными причинами ухудшения зрения. Работа при недостаточном освещении и или работа за устройствами, создающими искусственный синий свет приводит к покраснениям глаз и к их усталости;

- психофизиологические факторы. Специалист в работе постоянно сталкивается с большим объемом задач различной сложности, которые необходимо решить в срок, это может повлечь за собой большой уровень стресса, а также привести к утомлению и сказаться на психологическом состоянии;

- воздействие электромагнитного излучения. Работа специалиста по защите информации с электронными устройствами приводит к постоянному контакту специалиста с электромагнитным излучением. Для того, чтобы снизить вредное влияние такого излучения, специалисту необходимо делать перерывы в работе или заниматься физической активностью.

Все перечисленные факторы, влияющие на физическое и психическое здоровье специалиста, показывают, что для поддержания здорового организма стоит применять все описанные ранее методы. Сочетание физических упражнений, отдыха и правильного расположения оборудования на рабочем месте способно создать все условия для комфортной работы специалиста. Кроме этого, не стоит забывать о том, что работа приносит стресс, который также влияет на работника.

Рекомендуется также регулярное посещение врача, который может на ранних стадиях заболевания опорно-двигательного аппарата назначить лечение для специалиста.

Основными моментами, на которые стоит обратить внимание специалисту являются такие состояния позвоночника как сутулость, круглая спина, плоская спина. Борьба с данными проблемами должна начинаться с упражнений. Такими упражнениями могут являться как разминка так комплекс лечебно-оздоровительных упражнений.

Для снижения воздействия вредных психофизиологических факторов на опорно-двигательный аппарат специалиста по защите информации, рекомендуется выполнять следующие упражнения:

- регулярные перерывы и физические упражнения. Для того чтобы не доводить мышцы и суставы до состояния напряжения, а также улучшить кровообращение, необходимо регулярно проводить кратковременные перерывы и совместно с отдыхом выполнять физические упражнения для растяжки;

- эргономические упражнения. Необходимо выполнять упражнения направленные на снятия нагрузки мышц спины, шеи и рук. Это поможет улучшить физическое и психологическое состояние специалиста по защите информации.

Например, растяжка спины и шеи, включая наклоны, повороты и упражнения на растяжение мышц, может помочь снять напряжение и улучшить гибкость;

- растяжка и релаксация. Практика растяжки и релаксации может помочь снять напряжение и улучшить гибкость. Это можно делать путем выполнения растягивающих упражнений и дыхательных упражнений;

- аэробные упражнения. Физические активности, такие как ходьба, бег, плавание или езда на велосипеде, способствуют улучшению общей физической выносливости, кровообращения и уменьшению стресса;

Все эти методы и средства физической культуры могут помочь снизить воздействие вредных психофизиологических факторов и поддержать здоровье опорно-двигательного аппарата специалиста по защите информации.

Заключение

В данной дипломной работе была разработана методика предприятия АО «НПП «Рубин», обеспечивающая защиту информации от утечек по беспроводному каналу передачи данных на базе технологии Bluetooth. Были рассмотрены различные аспекты методики, такие как область применения и цель разработки и заканчивая анализом эффективности методики.

В ходе разработки были определены угрозы, уязвимости и нарушители, благодаря этому получилось получить всю необходимую информацию о рисках, которые могут возникнуть в уязвимых местах предприятия. Также был подробно рассмотрен и применен алгоритм выбора защитных мер, которые применялись в данной методике.

Исходя из условий, при которых функционирует организация были выбраны наборы защитных мер, которые наиболее оптимально соответствуют требованиям и должным образом обеспечивают защиту информации. Вместе с этим был определен критерий эффективности методики, и процедура, в которой анализируется ее эффективность. Все это позволило наиболее точно оценить полученные результаты.

Были осуществлены и оценены экспериментальные исследования методики на эффективность и результаты практического исследования. Итоговые результаты стали подтверждением того, что методика работоспособна и эффективна.

В соответствии с проведенными исследованиями и анализом были сформулированы рекомендации по практическому применению разработанной методики. Данные рекомендации могут оказаться полезны для АСУ АО «НПП «Рубин» и схожих предприятий, которые работают с информацией ограниченного доступа.

Помимо этого, в работе были рассмотрены влияющие на опорно-двигательный аппарат специалистов по защите информации вредные психофизиологические факторы. Были приведены методы и средства

физической культуры, которые помогут снизить негативное воздействие этих факторов и улучшить работоспособность специалистов.

Полученные результаты имеют важное значение для работающих с конфиденциальной информацией организаций, так как данная методика может быть широко применена и способствовать сокращению возможных рисков нарушения безопасности данных. Данная методика может быть применена на практике для обеспечения сохранности и конфиденциальности информации организации, а также защититься от возможных угроз и нарушений безопасности в сфере передачи данных.

Проведенный изначально обширный анализ угроз, уязвимостей и нарушителей позволил иметь полное представление о возможных рисках и уязвимых местах. Это послужило важным этапом для разработки методики, так как он позволил точно определить основные угрозы и сфокусироваться на правильном применении соответствующих мер защиты.

В последствии описанный алгоритм выбора защитных мер помог выбрать определенные методы защиты, которые необходимо применить в данной методике. Он обеспечил систематизированный и обоснованный подход на этапе выбора мер защиты, учитывая особенности функционирования организации и требования.

В результате проведенного экспериментального исследования методики была подтверждена ее работоспособность и эффективность. Полученные результаты подтвердили, что методика позволяет обеспечить надежную защиту от утечки информации по беспроводному каналу передачи данных на базе технологии Bluetooth.

Помимо этого, в данной работе были сформулированы возможные практические рекомендации, которые АСУ АО «НПП «Рубин» и схожие организации могут использовать для применения методики на практике. Они учитывают различные условия и требования с учетом которых может функционировать организация, а также их ограниченный доступ к

конфиденциальной информации и помогают эффективно внедрить методику в практическую деятельность.

Таким образом, все пункты технического задания из ВКР выполнены полностью.

Список использованных источников

1. 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: 12.02.2023).
2. Акнорский Д. Немного о беспроводных сетях //Компьютер Price, 2003. – 89 с.
3. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка): утверждена ФСТЭК РФ от 15.02.2008:// КонсультантПлюс. Технология 3000: Версия Проф [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2015.
4. Безопасность беспроводных сетей автор Гордейчик С.В., Дубровин В.В. Издательство: Горячая линия – ТелекомISBN, 2017. – 682 с.
5. Берлин А.Н. Телекоммуникационные сети и устройства. //Интернет-университет информационных технологий - ИНТУИТ.ру, БИНОМ. Лаборатория знаний, 2008. – 319 с.
6. Беспроводная сеть своими руками автор: Ватаманюк А.И.Издательство: Питер, 2006. – 190 с.
7. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации, 2005. – 205 с.
8. Восстановления данных в беспроводной сети //iXBT URL:<http://www.ixbt.com/storage/faq-flash-p0.shtml>.
9. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2008–02–01. – М.: СтандартИнформ, 2004.– 8 с.
10. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. — М.: Изд-во стандартов, 2012. — 50 с.

11. Гулятьев А.К. Восстановление данных. 2-е изд. СПб.: Питер, 2006. – 379 с.
12. Зорин М., Писарев Ю., Соловьев П. Беспроводные сети: современное состояние и перспективы. - Connect! // Мир связи, 1999. – 104 с.
13. Зайдель И. Флэшка должна жить долго // R.LAB URL:http://rlab.ru/doc/long_live_flash.html.
14. Зорин М., Писарев Ю., Соловьев П. Радиооборудование диапазона 2,4 ГГц: задачи и возможности // PCWeek/Russian Edition, 1999. – 604 с.
15. Компьютерные сети: Многоуровневая архитектура Интернета: Перевод с английского. Автор: Куроуз Д.Ф., Росс К.В, 2000.
16. Кристиан Барнс, Тони Боутс, Дональд Ллойд, Эрик Уле, Джеффри Посланс, Дэвид М. Зенджан, Нил О'Фаррел., Защита от хакеров беспроводных сетей. - Издательство: Компания АйТи, ДМК пресс, 2005. – 480 с.
17. Меррит Максим, Дэвид Поллино., Безопасность беспроводных сетей, 2004. – 288 с.
18. Молта Д., Фостер-Вебстер А. Тестируем оборудование для беспроводных ЛВС стандарта 802.11 // Сети и системы связи, 1999. – 170 с.
19. Митилино С. Безопасность беспроводных сетей //ITC-Online, 2003.- №27 URL:<http://itc.ua/node/14109>.
20. Норенков, В.А. Трудоношин - М.: Изд-во МГТУ им. Н.Э. Баумана, 1998. – 232 с.
21. «Об информации, информационных технологиях и защите информации»: федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ: (ред. от 24.11.2014) // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2015
22. «О коммерческой тайне»: федеральный закон Российской Федерации от 29 июля 2004 №98-ФЗ: (в ред. от 12.03.14) // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2015.

23. Олифер В.Г., Олифер Н.А. Основы сетей передачи данных. //Интернет-университет информационных технологий - ИНТУИТ.ру, 2005. – 176 с.
24. Олейник Т. Беспроводные сети: современное состояние и перспективы. // Домашний ПК, 2003. – 242 с.
25. Основы построения беспроводных локальных сетей стандарта 802.11. Р. Педжман, Л. Джонатан, 2004. – 296 с.
26. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. — М.: ГТК РФ, 1992. – 39 с.
27. Сидорин Ю.С. Технические средства защиты информации: Учеб. пособие. \ Под ред. Г.А. Краюхина. – СПб.: Издательство Политехнического университета, 2005. – С.39-40.
28. Современные технологии беспроводной связи И. Шахнович
Издательство: Техносфера Год издания: 2006 Страниц: 288 ISBN: 5-94836-070-9.
29. «Специальные требования и рекомендации по технической защите конфиденциальной информации». Утверждены приказом Гостехкомиссии России от 02.03.2001 № 282. — М.: Изд-во стандартов, 2001.
30. Стенг Д., Мун С. Секреты безопасности сетей. – К.: Диалектика, 2005. – С. 96-97.
31. Хорев А.А. Способы перехвата информации, обрабатываемой техническими средствами [Электронный ресурс] / А.А. Хорев // Защита информации. Инсайд, 2008. №1. URL: http://www.insidezi.ru/pages/1_2008/index.html (дата обращения: 26.01.23)
32. Хорев, А.А. Методы и средства поиска электронных устройств перехвата информации. М.: МО РФ, 1998. – 224 с.

33. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. - К.:Издательство Юниор, 2003. – 520 с.

Приложение А

(обязательное)

Схема возможной утечки информации по беспроводному каналу передачи данных на базе технологии Bluetooth.

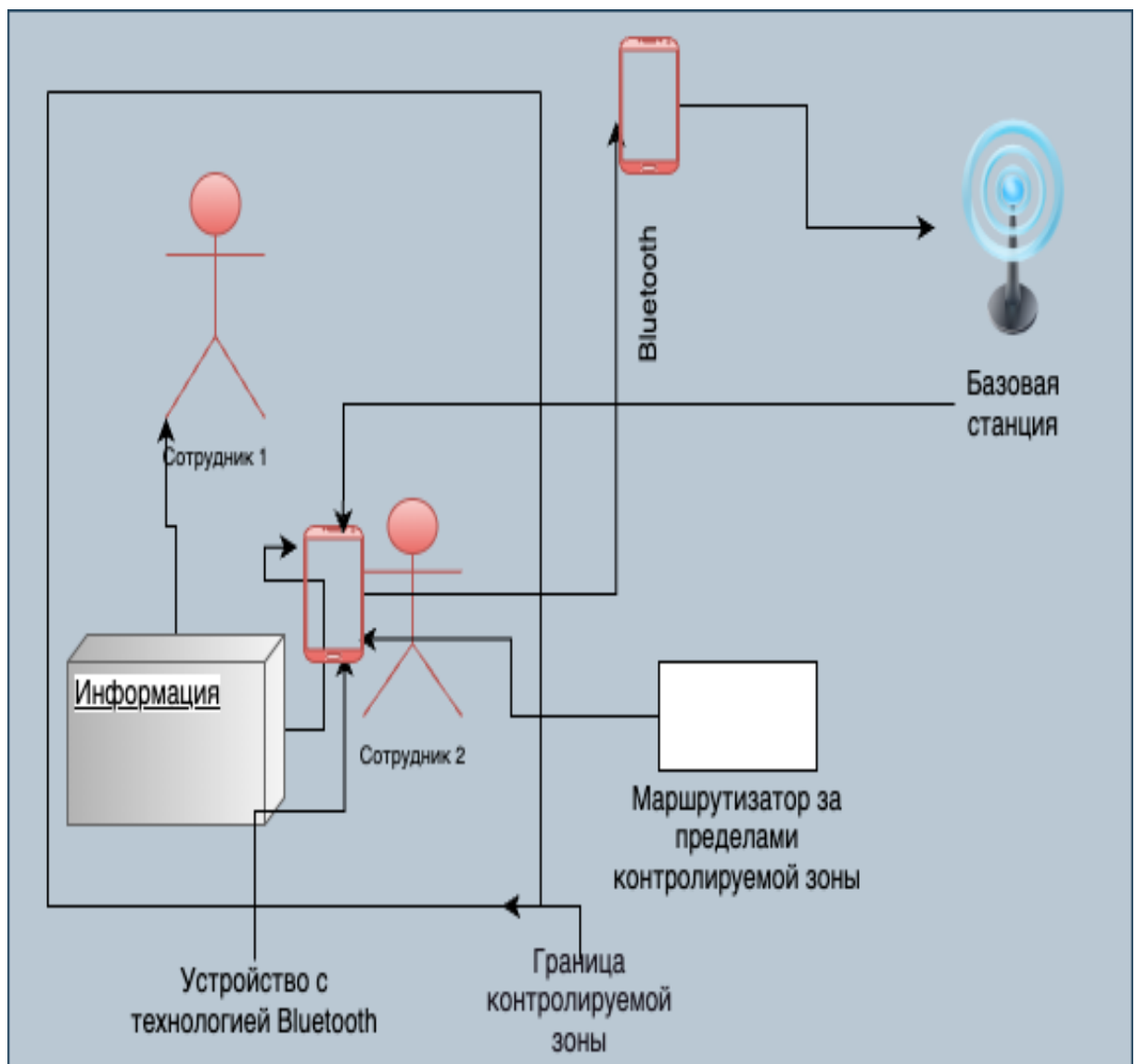


Рисунок 4 – Схема возможной утечки информации по беспроводному каналу передачи данных на базе технологии Bluetooth.

Приложение Б

(обязательное)

Статистика практического исследования эффективности методики

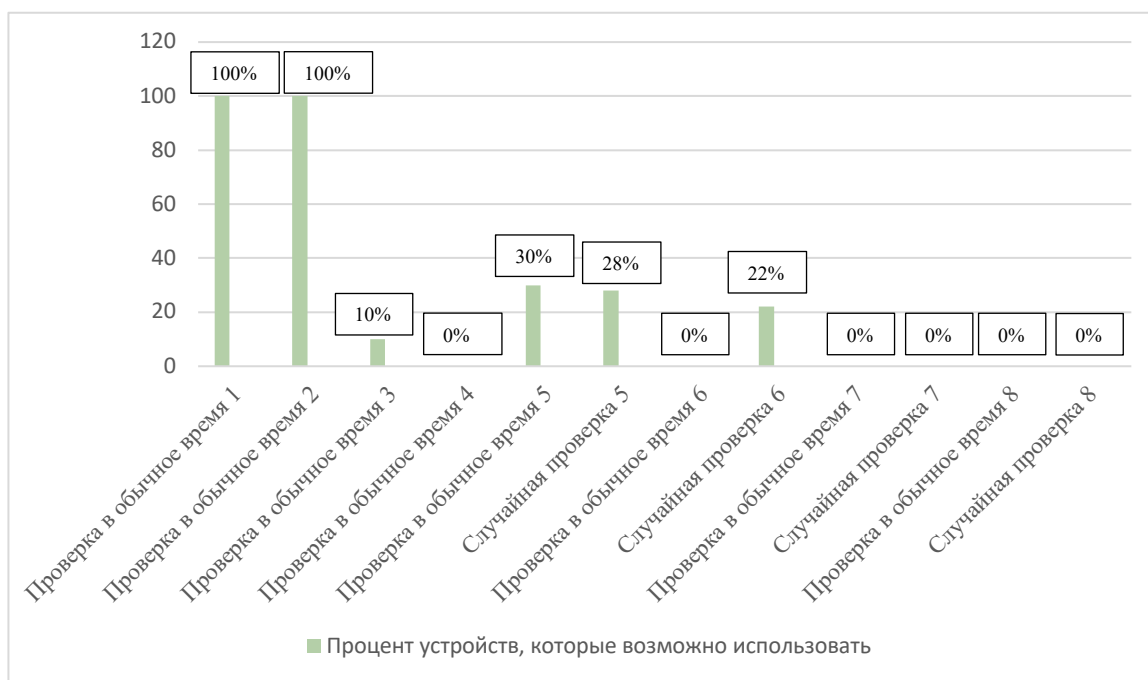


Рисунок 5 — Результаты практического исследования эффективности методики