МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(Дипломная работа)

На тему «Разработка системы информационной безопасности для регионального телекоммуникационного провайдера»

Исполнитель_____ Хижнякова Ксения Александровна
(подпись) (фамилия,имя,отчество)

Руководитель_____ Козлов Юрий Викторович
(подпись) (фамилия,имя,отчество)

«К защите допускаю»
Заведующий кафедрой _____ Лепешкин Олег Михайлович
(подпись) (фамилия,имя,отчество)

«____»_____20___г.

Санкт-Петербург

2026

МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

«УТВЕРЖДАЮ»
Заведующий кафедрой
_____ Лепешкин Олег Михайлович
(подпись) (фамилия, имя, отчество)
« _» _____ 20___ года

Задание на выпускную квалификационную работу

студенту Хижняковой Ксении Александровне
(фамилия, имя, отчество)

1. **Тема** «Разработка системы информационной безопасности для регионального телекоммуникационного провайдера» приказом ректора Университета
   от «__» _____20___года, № _____
2. **Срок сдачи законченной работы «___» _____20___ года**
3. **Исходные данные к выпускной квалификационной работе:**

Структура организации регионального телекоммуникационного провайдера, нормативно-правовая база, необходимость комплексной системы защиты информации.

4. **Перечень вопросов, подлежащих разработке (краткое содержание работы:**

Введение. Актуальность темы, цели и задачи ВКР
Глава 1. Теоретические основы построения системы информационной безопасности (наименование главы)
Глава 2. Анализ и оценка информационной безопасности на примере регионального провайдера (наименование главы)
Глава 3. Разработка проекта системы информационной безопасности для регионального провайдера (наименование главы)
Заключение. Выводы по работе в целом. Оценка степени решения поставленных задач.Практические рекомендации.

5. **Перечень материалов, представляемых к защите:**

□ Пояснительная записка; □ Схема «Структурная схема ЦОД»
(наименование схемы)

6. Дата выдачи задания: «___» _____ 20___ года

Руководитель выпускной квалификационной работы

_____ _____

(должность, ученая степень, ученое звание, фамилия, имя, отчество) (подпись)

Задание принял к исполнению «__»_____ 20___ года

Студент _____ _____

(фамилия, имя, отчество, учебная группа) (подпись)

РЕФЕРАТ

Дипломная работа: 89 с., 12 рис., 6 табл., 7 приложений, 45 источников литературы.

РАЗРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ РЕГИОНАЛЬНОГО ТЕЛЕКОММУНИКАЦИОННОГО ПРОВАЙДЕРА.

Объект исследования: деятельность публичного акционерного общества «Телеком», которое осуществляет услуги регионального телекоммуникационного провайдера.

Предмет исследования: система информационной безопасности данного предприятия.

Цель работы: разработка комплекса мероприятий для повышения уровня защищенности ПАО «Телеком».

В дипломной работе проводится анализ нормативно-правовой базы Российской Федерации в области информационной безопасности, рассмотрены современные угрозы и уязвимости, характерные для телекоммуникационных сетей. Выполнено исследование организационной структуры и информационной инфраструктуры предоставленной компании, проведена классификация обрабатываемой информации и анализ возможных каналов утечки данных.

Разработан комплекс организационных и технических мер защиты информации. Сформирована целевая архитектура системы информационной безопасности.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В последние годы в результате масштабной цифровизации компаниям из совершенно различных сфер деятельности приходится функционировать в условиях стремительного развития цифровых технологий, что также сопровождается увеличением количества угроз информационной безопасности и высокими требованиями к защите информационных активов. В особенности это относится к современным телеком-операторам, региональным провайдерам, так как телекоммуникационные сети являются ключевым элементом цифровой инфраструктуры регионов, который обеспечивает обмен информацией между населением, бизнесом и государственными организациями. Рост количества передаваемых данных, активное внедрение облачных сервисов, развитие сетей доступа приводят к необходимости роста требований и создания комплексных систем информационной безопасности. Данные системы должны обеспечивать не только защиту данных, но и бесперебойность предоставления услуг и устойчивость к внешним и внутренним угрозам, таким образом соответствуя трем главным аспектам информационной безопасности – конфиденциальности, доступности и целостности.

Актуальность выбранной темы для выпускной квалификационной работы определяется растущим количеством общемировых угроз информационной безопасности, в том числе успешно проведенных массовых и целевых атак на инфраструктуры, и подтверждается статистикой отраслевых компаний. Так, согласно исследованию Positive Technologies, в 2025 году около 20 процентов всех успешных атак являлись успешными массовыми атаками на организации, при этом количество жертв исчислялось десятками и тысячами [34]. Также стоит обратить внимание на то, что чаще всего жертвами массовых атак были госучреждения и промышленность. Это обуславливалось геополитической значимостью, высокой ценностью хранимых данных, а также относительно незрелыми процессами информационной безопасности. По данным аналитического отчета компании «Инфосистемы Джет», около 50 процентов предприятий в промышленном секторе обладали низким уровнем зрелости

процессного управления информационной безопасности [37]. Базовые меры защиты автоматизированных систем управления технологическими процессами (далее – АСУ ТП), предусмотренные нормативными документами, часто были реализованы формально, в результате чего данные меры стали недостаточными для противодействия атакам. Это постепенно привело к тому, что требования регуляторов начали ужесточаться. Так, в 2025 году ужесточились требования к критической информационной инфраструктуре (далее – КИИ) и обработке персональных данных, в том числе стало обязательным внедрение отечественного программного обеспечения (далее – ПО). Также теперь требуется использовать оборудование, которое сертифицировано Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК).

В 2025 году злоумышленники активно использовали для массовых и целевых атак вирусное программное обеспечение (далее – ВПО), RAT (ВПО для удаленного управления), а также шпионское ПО и шифровальщики [34]. Массовые атаки эволюционировали от самых простых сценариев до сложно обнаруживаемых и адаптивных. Таким образом, злоумышленники все чаще стали применять более изощренные техники, например, ботнеты с гибкой логикой, обфускацию кода или программируемое создание вредоносных файлов. В результате применения таких способов зловредная активность легче маскируется, сигнатуры реже детектируются системами обнаружения и атаки удается масштабировать до момента реакции на них. Это ведет к тому, что грань между массовыми и целевыми атаками становится все менее четкой, деятельность злоумышленников становится автоматизированной.

Самыми частыми последствиями, с которыми приходится сталкиваться жертвам атак – утечки конфиденциальной информации. Помимо прямых последствий, массовые атаки также порождают ряд системных проблем: происходит многократное увеличение нагрузки на защитные механизмы и команды реагирования. В результате появления множества инцидентов происходит перегрузка команд реагирования, что затрудняет своевременное выявление и отражение угроз. Так как для телекоммуникационных операторов

нарушение конфиденциальности, целостности и доступности может привести к значительному ущербу, существует необходимость проектирования и внедрения эффективной системы информационной безопасности в сетевую архитектуру регионального телекоммуникационного провайдера, работающего в условиях ограниченных ресурсов, но высокой критичности инфраструктуры.

Объектом исследования является деятельность некого условного публичного акционерного общества (далее – ПАО) «Телеком», которое осуществляет услуги регионального телекоммуникационного провайдера. Предметом исследования выступает система информационной безопасности данного предприятия, то есть архитектурные, организационные и технические меры обеспечения информационной безопасности.

Целью работы является разработка комплекса мероприятий для повышения уровня защищенности ПАО «Телеком», учитывающего актуальные угрозы, нормативные требования и специфику функционирования сетевой инфраструктуры. Комплекс обязан включать в себя подбор технических средств (в том числе межсетевые экраны, системы предотвращения вторжений, средства контроля доступа, решения для мониторинга и корреляции событий безопасности) и их внедрение, а также организационные меры.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать теоретические аспекты построения систем информационной безопасности для предприятий, осуществляющих услуги регионального телекоммуникационного провайдера;
2. Исследовать особенности функционирования сетевой инфраструктуры операторов связи, определить современные угрозы;
3. Изучить действующую нормативно-правовую базу и актуальные стандарты и требования в области информационной безопасности критической инфраструктуры;
4. Выполнить анализ текущего состояния системы информационной безопасности для ПАО «Телеком», произвести анализ сетевой архитектуры,

выявление уязвимостей и определение соответствия действующим нормативным требованиям;

5. Разработать комплекс мероприятий для повышения уровня защищенности ПАО «Телеком», включающий подбор и обоснование внедрения технических средств, а также организационных мер;

6. Оценить влияние предложенных мероприятий на уровень информационной безопасности предприятия.

Гипотеза исследования заключается в предположении, что применение комплексного архитектурного подхода к обеспечению информационной безопасности регионального телекоммуникационного провайдера позволит повысить устойчивость сетевой инфраструктуры к актуальным угрозам с помощью подходящих средств обеспечения информационной безопасности, обеспечит прозрачность процессов, сократит время реагирования на инциденты, обеспечит выполнение нормативных требований и подготовит компанию к проверкам регуляторов.

Методами исследований, использованными в процессе работы над выпускной квалификационной работой, являются: анализ научно-технической литературы и нормативных документов, метод сравнительного анализа, аналитический метод, методы системного и архитектурного моделирования, методы моделирования угроз, элементы риск-ориентированного подхода.

Степень разработанности проблемы подтверждается наличием научных публикаций, посвящённых вопросам архитектуры сетевой защиты, проектирования систем информационной безопасности и обеспечения устойчивости операторской инфраструктуры, однако практические аспекты адаптации подобных решений к условиям региональных телекоммуникационных компаний изучены недостаточно.

Научная новизна состоит в уточнении подходов к проектированию системы защиты телекоммуникационной инфраструктуры регионального провайдера с учётом комплексного совмещения организационных и

архитектурных мер, а также в формулировании требований к системе информационной безопасности на основе актуальной модели угроз.

Практическая значимость заключается в возможности применения разработанных рекомендаций и проектных решений в деятельности региональных операторов связи, а также в создании методологической основы для построения защищенной системы.

Нормативно-правовая база для исследовательской работы должна включать в себя федеральные законы и подзаконные акты Российской Федерации в области защиты информации и критической инфраструктуры. Также необходимо произвести работу с сопутствующими нормативными документами и учитывать национальные стандарты и примеры методических документов в исследуемой сфере [35].

Выпускная квалификационная работа состоит из введения, трех глав, заключения и списка используемой литературы, а также приложений.

В первой главе рассматриваются цели, задачи и теоретические аспекты построения систем информационной безопасности, а также подходы к защите телекоммуникационной инфраструктуры.

Вторая глава содержит анализ текущего состояния информационной безопасности в условном ПАО «Телеком», рассматриваются угрозы, классифицируются активы, оценивается уровень защищенности инфраструктуры компании и выявляются направления совершенствования.

Третья глава включает процесс модернизации проекта системы информационной безопасности, предложенные технические и организационные меры, архитектуру системы защиты и оценку эффективности внедрения комплекса решений.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В первой главе освещаются основополагающие принципы разработки системы информационной безопасности, также рассматривается история исследуемого вопроса. Обосновывается выбор технологий, используемых для обеспечения информационной безопасности.

В разделе 1.1 раскрываются теоретические основы информационной безопасности. В разделе 1.2 определены программные и аппаратные средства, необходимые для решения поставленных задач, а также представлен краткий обзор существующих решений для обеспечения информационной безопасности систем. В разделе 1.3 описана документация, используемая в практической части исследовательской работы.

1.1. Сущность, цели и задачи системы информационной безопасности

Сам термин информации является относительно широким, поэтому его необходимо конкретизировать в рамках данной исследовательской работы для выполнения поставленных задач. Обычно информацию определяют как некий набор сведений, который не зависит от формы представления. Информация является объектом отношений между юридическими, физическими лицами и государством. Информацию обязательно защищать.

Согласно Федеральному закону № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3], информацию по категории доступа можно разделить на общедоступную информацию и информацию с ограниченным доступом. В зависимости от порядка предоставления информация делится на:

1. Информацию, которую можно свободно распространять;
2. Информацию, которая должна предоставляться только по соглашению сторон;
3. Информацию, которая должна быть представлена в соответствии с законами;
4. Информацию, которую не разрешается распространять.

Обеспечение безопасности информации, в том числе и в компьютерных системах, требует сохранения её целостности, доступности и конфиденциальности. Целостность информации заключается в поддержании её существования в неискаженном, неизменном виде по отношению к её исходному состоянию. Доступность информации – это свойство, характеризующее способность информации быть беспрепятственно доступной для пользователей, которые обладают правами на эту информацию. Конфиденциальность информации – это принцип, который гарантирует, что право доступа к информации есть только у уполномоченных лиц или систем, имеющих на это право.

Система информационной безопасности должна быть комплексом мер, направленных на обеспечение информационной безопасности информационных ресурсов и информации, которую они обрабатывают. Меры включают в себя организационные, технические, программные и правовые, и в результате они все должны быть направлены на обеспечение конфиденциальности ресурсов и информации, целостности информации и доступности ресурсов, устойчивого и безопасного функционирования ресурсов. Эти три аспекта являются ключевыми целями для каждой системы информационной безопасности. Так как в современных условиях угрозы информационной безопасности характеризуются высокой динамичностью, используемой автоматизацией атак, распределённым характером и использованием уязвимостей как технического, так и организационного характера, система информационной безопасности должна также не только предотвращать реализацию угроз, но и обеспечивать своевременное обнаружение инцидентов, минимизацию их последствий и восстановление работоспособности систем. В отличие от отдельных средств защиты, система информационной безопасности обладает комплексным характером и охватывает все уровни функционирования информационной инфраструктуры — от аппаратного и сетевого, до прикладного и организационного.

Для достижения поставленных целей системе информационной безопасности необходимо решать следующие задачи:

1. Выявление и анализ угроз информационной безопасности, которые характерны для конкретной организации и её информационной инфраструктуры;
2. Формирование и актуализация модели угроз и нарушителя с учётом специфики деятельности и изменений во внешней среде;
3. Оценка рисков информационной безопасности и определение приоритетных направлений защиты;
4. Разработка и внедрение организационных мер защиты, в том числе политики, регламенты и инструкции по обеспечению информационной безопасности;
5. Внедрение технических и программных средств защиты информации (далее – СЗИ);
6. Эксплуатация выше указанных СЗИ;
7. Организация контроля доступа, который могут получить пользователи или злоумышленник;
8. Обеспечение мониторинга событий безопасности;
9. Выявление угроз и реагирования на инциденты информационной безопасности;
10. Проведение аудита и оценки эффективности мер защиты;
11. Обеспечение обучения и повышения осведомлённости персонала в области информационной безопасности;
12. Организация резервного копирования и восстановления информации;
13. Обеспечение взаимодействия с регуляторами и выполнение требований нормативно-правовой базы.

Для телекоммуникационных организаций система информационной безопасности должна включать дополнительные задачи, которые обусловлены необходимостью обеспечения непрерывности предоставления услуг связи, высокой степенью распределённости инфраструктуры и наличием критически

важных процессов. В таких условиях система информационной безопасности становится не только комплексным решением для защиты информации, но и инструментом обеспечения отказоустойчивости и надёжности сетевой инфраструктуры.

Система информационной безопасности в компании должна быть частью общей системы управления организацией и должна быть интегрирована в процессы стратегического и оперативного управления. Эффективная система информационной безопасности обеспечивает баланс между требованиями безопасности, производительности и экономической целесообразности, что особенно важно для региональных телекоммуникационных провайдеров с ограниченными ресурсами.

Необходимо подробнее рассмотреть ранее упомянутые угрозы, с которыми приходится сталкиваться системам информационной безопасности, исходя из источника, целей злоумышленников, а также ряда других критериев.

По месту расположения угрозы делятся на внутренние, внешние и угрозы в пределах видимости. Первые связаны с уязвимостями, которые изначально заложены в системе или ее компонентах. К ним относятся уязвимости в ПО. Вторые происходят извне – например, это могут быть атаки хакеров. Третьи включают перехватывающую и прослушивающую аппаратуру. По видимости угрозы можно разделить на пассивные и активные. Пассивные угрозы незаметны, как, например, считывание конфиденциальных данных, а активные – наоборот, как повреждение данных. По доступу угрозы разделяются на несанкционированный доступ и утечку или повреждение данных. Первый связан с попыткой получения доступа к информации пользователем без необходимых для этого прав, другой происходит в результате ошибочных или неправомерных действий сотрудника с доступом. Также угрозы делятся по цели: угроза данным, программной среде, аппаратному обеспечению, поддерживающей инфраструктуре. А классификация угроз по уровню объективности включает объективные, субъективные и случайные угрозы. Объективные это технические средства излучения, субъективные угрозы включают в себя ошибки при

установке ПО и в процессе эксплуатации, к случайным же угрозам относят сбои и отказы в работе корпоративной инфраструктуры.

Перечисленные выше угрозы описаны в общей форме. Также можно рассмотреть более конкретные угрозы, которые влияют на функционирование сети «Интернет» и сети связи общего пользования, с которыми сталкиваются провайдеры. Например, это может быть угроза устойчивости функционирования. При данной угрозе работоспособность сети нарушается, если есть какая-либо неисправность в части сети. Также это может быть угроза невозможности доступа к услугам связи, которая возникает по причине аварий. В итоге обеих угроз, система приходит в такое состояние, в котором услуги связи становятся недоступными для физических и юридических лиц. Особую категорию составляют угрозы, связанные с невозможностью оказания услуг связи владельцам критически важных объектов. Такие инциденты могут повлечь не просто нарушение, но и полное прекращение функционирования объектов. Под угрозами безопасности функционирования понимаются угрозы, при реализации которых снижается или утрачивается способность противостояния несанкционированному доступу [14].

1.2. Обзор современных методов и средств защиты информации

Информационная безопасность современных телекоммуникационных сетей представляет собой комплекс мероприятий для повышения уровня защищенности, которые направлены на предотвращение несанкционированного доступа, обеспечение целостности, доступности и конфиденциальности информации. В условиях роста трафика и цифровизации услуг провайдеры сталкиваются с увеличением числа кибератак, включая DDoS-атаки, попытки взлома сетевых узлов, перехват трафика, эксплуатацию уязвимостей в сетевом оборудовании. Поэтому современный рынок информационной безопасности предлагает огромное количество решений: межсетевые экраны нового поколения (далее – NGFW), средства контроля целостности, средство для обнаружения и нейтрализации атак на конечных точках (далее – EDR), NDR, средства журналирования и мониторинга событий безопасности (далее – SIEM)

и т.д. Но человеческий фактор может оказаться решающим, и по данной причине обеспечение безопасности должно основываться на одновременном применении всего комплекса мер, предусмотренных законом и предлагаемых специалистами.

Меры защиты принято разделять на два больших класса: административные (или организационные) и технические [39]. К первым относится регламентация, документирование, аудиты инфраструктуры, разработка и внедрение политик безопасности. Важной составляющей организационных методов является распределение ролей и ответственности персонала [42, 44]. Для телекоммуникационных провайдеров, эксплуатирующих распределённую инфраструктуру, особое значение имеет формализация процессов управления изменениями, эксплуатации сетевого оборудования и взаимодействия с подрядными организациями. К другим, техническим мерам, относятся программные и программно-аппаратные комплексы (далее – ПАК). Технические меры также можно разделить на средства по уровням защиты и на дополнительные технические меры. Дополнительные технические меры помогают сопровождению средств защиты, благодаря им повышается эффективность, также именно они помогают создать систему управления информационной безопасностью (СУИБ). Рассмотрим уровни защиты, которым будут впоследствии помогать дополнительные технические меры. Уровней защиты всего пять: уровень периметра (Perimeter Layer), уровень рабочих станций (Endpoint Layer), сетевой уровень (Network Layer), уровень Интернета (Internet Layer), пользовательский уровень (User Layer) [40]. На каждом из уровней находятся конкретные средства защиты, применяемые только на этом уровне и выполняющие конкретные соответствующие уровню функции (так называемая периметральная модель защиты). Так, на уровне периметра главной целью средств защиты является сокращение площади атаки на ресурсы организации, там же производится фильтрация контента. На следующем уровне средства защиты отвечают за безопасность рабочих станций и мобильных устройств, например, предотвращая угрозы фишинга и так далее. На сетевом уровне происходит анализ трафика на предмет компрометации локальных узлов

или поведенческих аномалий [41]. К уровню Интернета относится вся активность, которая происходит вне пределов компании и обеспечивает противодействие угрозам. Уровень пользователей – это про обучение сотрудников основам информационной безопасности.

Чтобы корректно располагать технические средства защиты на уровнях, необходимо также помнить о главных векторах атаки на представленную сеть. Так, например, на корпоративную сеть векторы атаки на почту и веб, закрываются на уровне периметра. Угрозы для рабочих станций закрываются на уровне рабочих станций. В случае, если злоумышленник уже попал во внутреннюю сеть компании, противодействие ему будет осуществляться на уровне сети.

Теперь рассмотрим, на каких же уровнях какие конкретно технические средства защиты принято использовать. Так, на уровне сетевого периметра используются не только такие современные средства защиты, как NGFW, но и используются системы обнаружения и предотвращения вторжений (далее – IDP/IPS). Также на данном уровне принято настраивать фильтрацию трафика посредством списков управления доступом (далее – ACL), средства защиты от DDoS-атак, SIEM, межсетевые экраны прикладного уровня (далее – WAF). На уровне рабочих станций используются программные меры – антивирусное ПО, EDR. На сетевом уровне используются средства, способные произвести сегментацию сети и изоляцию критически важных узлов, а также использовать криптографические средства: внутренние NGFW, системы контроля и управления доступом к сети (далее – NAC), системы обнаружения аномалий сетевого трафика (далее – NDR), средства работы с неструктурированными данными (далее – DCAP-системы), сканеры уязвимостей. На уровне Интернета есть средства URL- и контентной фильтрации, а также программные продукты, защищающие организации от утечек конфиденциальной информации (далее DLP-системы). На пользовательском уровне располагаются системы управления идентификацией и доступом (далее – IAM), средства многофакторной аутентификации (далее – MFA), средства контроля пользовательских сессий.

Стоит также заметить, что в последние годы широкое распространение получили архитектурные подходы, ориентированные на отказ от традиционной периметральной модели защиты. К таким подходам относятся такие концепции, как, например, модель сетевой безопасности, объединяющая облачные инструменты защиты и сетевые технологии в один пакет услуг (Secure Access Service Edge или, если кратко, SASE), также предполагающая непрерывную проверку доверия и централизованное управление доступом к ресурсам. Но для телекоммуникационных операторов внедрение подобных подходов требует адаптации с учётом требований по отказоустойчивости, производительности и нормативного регулирования, поэтому концепция нулевого доверия (Zero Trust), которая будет использоваться в практической части исследовательской работы, более подходящая.

В целом, любую систему информационной безопасности необходимо строить комплексно, чтобы у специалиста информационной безопасности была возможность выполнения трех основных технических задач:

1. Как можно раньше обнаружить и предотвратить атаку;
2. Как можно быстрее обнаружить и локализовать успешную атаку;
3. После остановки атаки провести детальный анализ произошедшего.

Именно многоуровневый подход с использованием различных решений информационной безопасности позволяет реализовать надежную защиту.

1.3. Нормативно-правовая база и стандарты в области информационной безопасности

Значительную роль в построении системы информационной безопасности играют нормативные документы. Они демонстрируют не только конкретные требования, регулирующие сферу информационной безопасности, но и то, как планируется развивать направление информационной безопасности в ближайшем будущем с учетом событий в настоящем. Так, в распоряжении Правительства Российской Федерации от 24.11.2023 «О стратегии развития отрасли связи Российской Федерации на период до 2035 года», сделан акцент на том, что количество инцидентов информационной безопасности не только

растет, но и их техническая структура усложняется и скоординированность атак повышается, это является также одной из причин актуальности данной исследовательской работы [10]. Также нельзя забывать Федеральный закон № 172-ФЗ «О стратегическом планировании в РФ», который регулирует целеполагание, прогнозирование и программирование развития отраслей, включая инфраструктуру цифровой экономики, обеспечивая их соответствие национальным интересам и технологической безопасности [7].

Для определения терминологии информации в предыдущем подразделе был использован Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 24.07.2025) «Об информации, информационных технологиях и о защите информации», также в нем раскрываются принципы правового регулирования в сфере информации и подобное [3]. Для работы с авторизацией в личные кабинеты пользователей, которые будут использоваться в примере регионального провайдера, чтобы пользователи могли ознакомиться со всей необходимой им информацией, будет также необходимо обратиться к данному закону.

Федеральный закон № 126-ФЗ «О связи» от 07.07.2003 устанавливает правовые основы деятельности в сфере связи в стране, регулируя создание и эксплуатацию сетей, использование радиочастотного спектра, предоставление услуг электросвязи и почтовой связи, а также права и обязанности операторов связи и пользователей, обеспечивая защиту интересов сторон, конкуренцию, и интеграцию в мировые сети [6].

Федеральный закон № 152-ФЗ «О персональных данных» является одним из ключевых нормативных правовых актов для сферы информационной безопасности [5]. Его требования обязательны к выполнению всеми организациями, осуществляющими обработку персональных данных в рамках своей деятельности. Закон устанавливается правовые основания обработки персональных данных, в том числе включая необходимость получения согласия субъектов на обработку. Также необходима регистрация организации в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор). Определение Роскомнадзора

как федеральной службы по надзору в сфере связи описано в Постановлении Правительства РФ от 16.03.2009 № 228 (ред. от 03.07.2025) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» [12]. Роскомнадзор также осуществляет лицензирование деятельности по технической защите конфиденциальной информации согласно Постановлению Правительства РФ от 03.02.2012 № 79 (ред. От 27.12.2024) «О лицензировании деятельности по технической защите конфиденциальной информации», с помощью оценочного листа, который утвержден Приказом ФСТЭК России от 28.12.2021 № 206 «Об утверждении формы оценочного листа, в соответствии с которым ФСТЭК России проводит оценку соответствия соискателя лицензии или лицензиата лицензионным требованиям при осуществлении деятельности по технической защите конфиденциальной информации» [11, 17]. Для того, чтобы корректно производить документирование работы с персональными данными, необходимо учитывать «Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональный данных»» Роскомнадзора.

В телекоммуникационном провайдере может производиться работа с коммерческой информацией. Обычно это относится к базам данных или составленным контрактам, а также к данным, которые предоставляют организации клиенты. Важно обращать внимание на то, как именно данные хранятся и обрабатываются, а также как соблюдается ли тайна связи и возможна ли передача данных гос. органам по запросу. Тема коммерческой тайны поднимается в Федеральном законе от 29.07.2004 № 98-ФЗ «О коммерческой тайне» [4]. Для того, чтобы разграничивать доступ внутри организации, необходимо обратиться к «Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка)» (утв. приказом ФСТЭК России от 02.06.2020 № 76) [24].

В том случае, если провайдер является субъектом КИИ, то его деятельность также должна регулироваться законодательно с учетом этого. В Федеральном законе № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» обсуждены задачи и требования к объектам КИИ (информационные системы или системы управления субъектов КИИ) [2]. Региональный интернет-провайдер, предоставляющий услуги связи, может и не относиться к субъектам КИИ. Он может являться объектом КИИ в том случае, если его информационные системы (ИС) значимы для функционирования таких ключевых отраслей, как транспорт, здравоохранение и другие. Решение о принадлежности принимает сам провайдер по критериям 187-ФЗ и приказам ФСТЭК. Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 28.08.2024) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрировано в Минюсте России 26.03.2018 N 50524) и Приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (с изменениями и дополнениями), где описаны требования к созданию и функционированию систем безопасности значимых объектов КИИ [20, 19]. Также стоит учитывать Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 07.11.2025) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» для определения критериев значимости [13].

Значительное место в нормативном регулировании вопросов информационной безопасности также уделену некоторому количеству приказов ФСТЭК, которые необходимы для работы с системами информационной безопасности. В частности, Приказ № 21 «Об утверждении Состава и содержания

организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» определяет обязательные требования, используемые в работе с персональными данными, включая перечент организационных и технических мер. К данным мерам относится идентификация и аутентификация субъектов и объектов доступа. А также определены действия, проводимые над событиями безопасности: регистрация и учет [23].

Требования к обеспечению защиты информации в автоматизированных системах управления производственными процессами (АСУ ТП) установлены Приказом ФСТЭК России от 14.03.2014 № 31 (ред. от 15.03.2021) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» зарегистрировано в Минюсте России 30.06.2014 № 32919) [18].

Деятельность, которую необходимо включать в план мероприятий информационной безопасности, описано в Постановлении Правительства РФ от 12 февраля 2020 г. № 126 «Об установке, эксплуатации и о модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования» [15]. В план мероприятий должны быть включены планируемые даты ввода в эксплуатацию (модернизации) узлов связи операторов связи с указанием мест их размещения, количество планируемых каналов передачи данных с указанием их технологии и пропускной способности, планируемая дата начала установки технических средств противодействия угрозам, сведения о среднестатистической и максимальной загрузке каналов, к которым планируется подключать технические средства противодействия угрозам.

В целом требования по защите сетей описаны в Приказе Министерства информационных технологий и связи РФ от 9 января 2008 г. № 1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации» [22]. Там говорится о том, что необходимо для защиты от несанкционированного доступа к программным средствам узлов связи сетей фиксированной телефонной связи, сетей подвижной радиосвязи, сетей подвижной радиотелефонной связи, сетей подвижной спутниковой радиосвязи, сетей передачи данных, сетей телеграфной связи.

Также отдельно стоит рассмотреть тему использования криптографии. Деятельность Федеральной службы безопасности (далее – ФСБ) регламентируется Федеральным законом от 03.04.1995 № 40-ФЗ (ред. От 28.12.2025) «О федеральной службе безопасности» [8]. Указанный нормативный правовой акт определяется правовой статус, основные задачи и пределы полномочий организации. Порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных средств криптографической защиты (шифровальных средств), описан в Приказе Федерального агентства правительственной связи и информации (ФАПСИ) при Президенте РФ от 13 июня 2001 года № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» [21]. В целом требования к криптографической защите информации описаны в Приказе ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством

Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [23].

Приказ ФСТЭК России от 12.01.2023 № 3 «Об утверждении форм документов, используемых Федеральной службой по техническому и экспортному контролю в процессе лицензирования деятельности по технической защите конфиденциальной информации, и признании утратившими силу приказа ФСТЭК России от 17 июля 2017 г. № 134 и внесенных в него изменений» описывает то, как в задокументированном виде должны выглядеть сведения о помещении, устанавливаемых средствах зашиты и так далее.

Регламентация процедуры установки, эксплуатации и модернизации в инфраструктурной сети оператора связи, который оказывает услуги по предоставлению доступа к «Интернет», описана в Постановлении Правительства РФ от 30 августа 2025 года № 1333 «Об утверждении Правил установки, эксплуатации и модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории РФ информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования» [16].

Виды угроз для сетей и регламент их определения описаны в Постановлении Правительства РФ от 27 октября 2025 года № 1667 «Об утверждении Правил централизованного управления сетью связи общего пользования» [14]. Методика оценки угроз безопасности описана в «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021) [31].

Аспекты безопасности описаны в ГОСТ Р 57149-2016/ISO/IEC Guide 51:2014 «Аспекты безопасности. Руководящие указания по включению их в стандарты» [27]. Для работы специалисты информационной безопасности также постоянно обращаются к другим стандартам ГОСТ. В ГОСТ Р 51897-2021 «Менеджмент риска» есть базовая лексика для формирования общего понимания понятий и терминов в области менеджмента риска среди организаций [26]. Более узко вопросы управления рисками рассматриваются в ГОСТ Р ИСО/МЭК 27005-

2010 «Менеджмент риска информационной безопасности», который ориентирован на идентификацию, анализ и оценку рисков [29]. В ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» определены основные процессы, которые влияют на снижение числа уязвимостей в ПО [30]. С практическими аспектами построения и внедрения системы информационной безопасности можно ознакомиться в ГОСТ Р ИСО/МЭК 27002-2021 «Методы и средства обеспечения безопасности» [28].

Оценка рисков и формирование модели угроз выполнены с учетом Банка данных угроз безопасности информации ФСТЭК России.

Стоит обратить внимание на то, что несоблюдение закона нарушениями в области информационной безопасности ведут к штрафам, приостановке деятельности или уголовной ответственности. Так, необходимо ознакомиться со следующими документами:

1. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 29.12.2025) (с изм. и доп., вступ. в силу с 20.01.2026) [9];
2. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ (ред. от 29.12.2025) (с изм. и доп., вступ. в силу с 09.01.2026), в том числе Статья 13.11 КоАП устанавливает ответственность за нарушения в области персональных данных [1];
3. Постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» [25].

Для того, чтобы ознакомиться с мерами ответственности, которая последует за нарушением законодательства сферы информационной безопасности, можно прочитать «Трудовой кодекс РФ», «Гражданском кодексе РФ» и другие документы.

Необходимо отметить, что нормативные требования постоянно изменяются и необходимо своевременно узнавать о любых изменениях и

подстраивать свои системы информационной безопасности согласно им. Так, в мае 2025 года требования к КИИ и обработке персональных данных ужесточились. К основным изменениям относится обязательное импортозамещение ПО и оборудования на сертифицированные ФСТЭК России средства.

ГЛАВА 2. АНАЛИЗ И ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ РЕГИОНАЛЬНОГО ПРОВАЙДЕРА

Во второй главе представлен анализ текущего состояния информационной безопасности условного регионального телекоммуникационного провайдера ПАО «Телеком».

В разделе 2.1 приведена характеристика объекта исследования, в том числе произведено описание актуальной сетевой топологии. В разделе 2.2 выполнен анализ функционирующей системы обеспечения информационной безопасности, выявлены реализуемые меры защиты и определены их недостатки. В разделе 2.3 проведена оценка рисков на основе модели угроз, сформированной с учетом специфики деятельности оператора.

2.1. Организационно-техническая характеристика организации и ее информационной инфраструктуры

Региональный оператор связи ПАО «Телеком» (далее – провайдер) предоставляет своим клиентам цифровые услуги и сервисы на территории субъекта Российской Федерации – Ленинградской области. Географический охват включает в себя административный центр и прилегающие муниципальные районы. Предоставляемые услуги: интернет-доступ, а также корпоративные VPN. Поддерживаются технологии Gigabit-capable Passive Optical Network (далее – GPON), Metro Ethernet. В компании числится более тысячи сотрудников, включая сетевых инженеров и специалистов ИБ. Услуги предоставляются десяткам тысяч абонентов (частным лицам), а также небольшому количеству бизнесов.

Рассмотрим организационную структуру провайдера (рисунок 1).

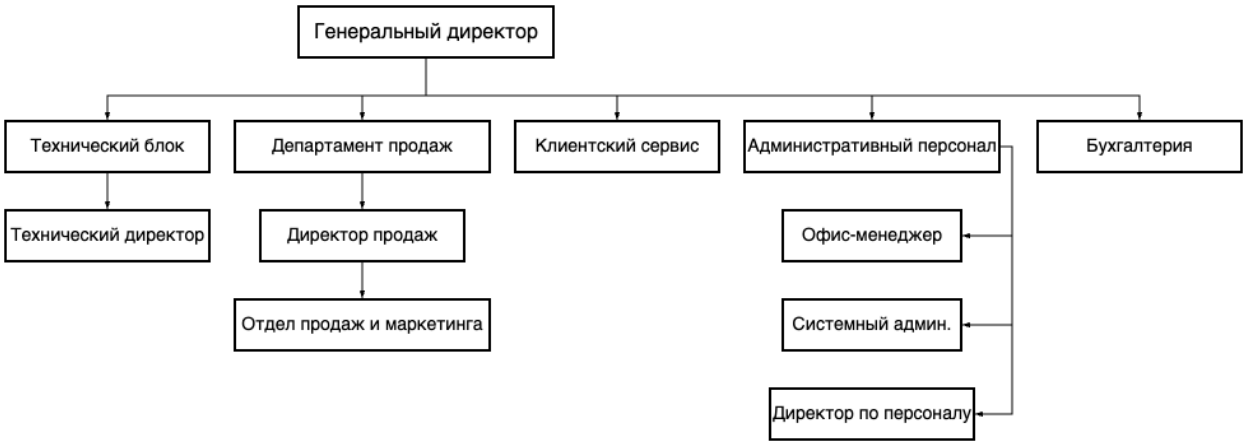

Рисунок 1 – Организационная структура

Организационная структура регионального интернет-провайдера в данном примере довольно проста. Она включает в себя технический блок (который под руководством технического директора делится на техническую поддержку и отдел специалистов, отвечающих за сети и инфраструктуры), департамент продаж и маркетинга, бухгалтерию, клиентский сервис, а также административный персонал. Используется упрощенная иерархия, чтобы была возможность быстро реагировать на запросы клиентов и внедрять изменения, опираясь на собственную локальную сеть и закупая трафик у более крупных операторов [36].

Рассмотрим подробнее деятельность некоторых отделов и подотделов. Техническая поддержка отвечает за подключение и обслуживание клиентов, производит устранение неполадок, подключение новых абонентов, работу с заявками. Специалисты отдела сетей разворачивают сети и управляют оборудованием (маршрутизаторами и коммутаторами). Отдел продаж проводит работу с частными клиентами и заключение договоров. Маркетинг отвечает за продвижение услуг, локальные рекламные компании.

Информационные потоки внутри компании обеспечивают процесс предоставления услуг связи, взаимодействие с абонентами, учет финансово-хозяйственной деятельности и техническую эксплуатацию сети. Информационные потоки между подразделениями носят как операционный, так и управленческий характер.

Рассмотрим схему информационных потоков организации (рисунок 2).

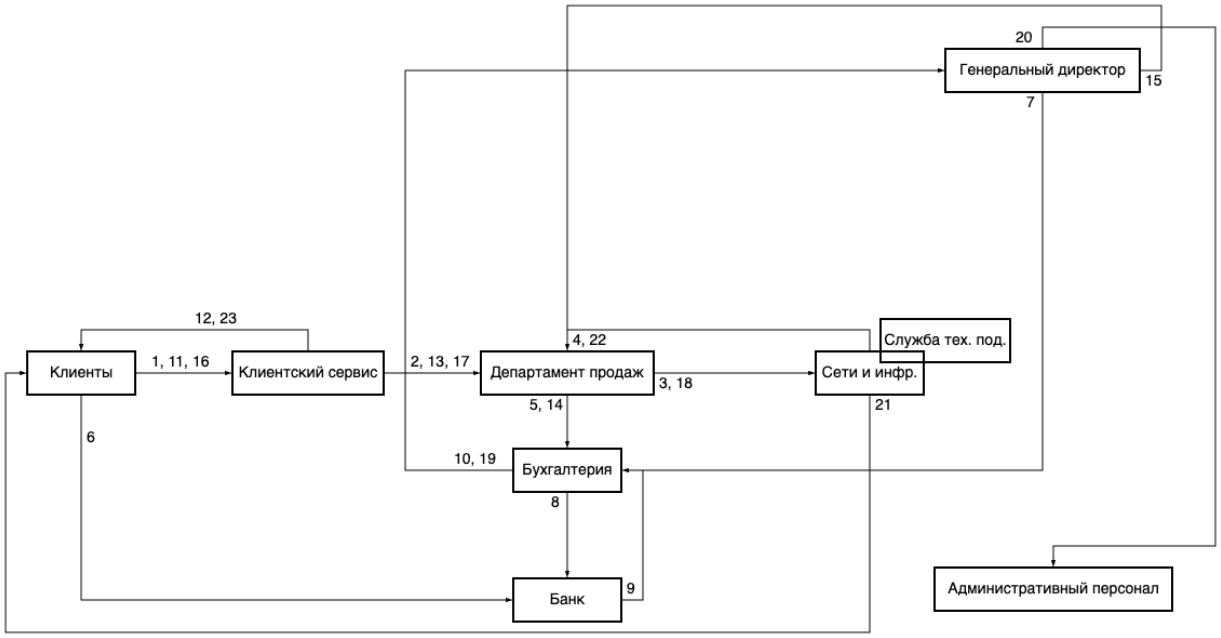

Рисунок 2 – Информационные потоки

Схема информационных потоков сопровождается таблицей (таблица 1), в которой приводится их описание и анализ.

Таблица 1 – Описание информационных потоков

Номер информационного потока	Наименование	Описание
1 2 3	Заявка на подключение абонентов	Клиент через клиентский сервис запрашивает подключение Интернета для своей сети. Через отдел продаж заявка поступает в технический блок.

Продолжение таблицы 1

4	Обратная связь о предоставляемых услугах	Технический отдел возвращает информацию о сроках выполнения работ.
5	Оплата, договоры	Обсуждение тарифов и условий оплаты.
6	Оплата услуг	Проводится оплата услуг клиентом в банк.
7	Запрос финансовой отчетности	Руководство запрашивает финансовый отчет в бухгалтерии.
8 9 10	Передача финансовой отчетности	Бухгалтерия запрашивает у банка информацию по состоянию банковской операции. Банк передает информацию о состоянии счета. Бухгалтерия предоставляет финансовую отчетность руководству.

Продолжение таблицы 1

11	Передача данных для подготовки документации о реализации продукта	Клиенты передают данные для подготовки документации.
12	Передача документации о реализации	Клиент получает договор.
13 14	Утверждение документации	Договор передается в бухгалтерию на подтверждение.
15	Инструкция или запрос на оформление/обработку документов	Передача от руководства распоряжений, указаний или запросов, касающихся документационного обеспечения деятельности компании.
16 17 18	Передача данных для подготовки реализации продукта	Клиент передает всю оставшуюся необходимую информацию для предоставления услуги техническим отделом.

Продолжение таблицы 1

19	Передача документа на утверждение и подписание	После обработки документа отделом работы с документацией, документ передаётся генеральному директору для рассмотрения, утверждения, подписания.
	Передача документа в Отдел кадров для учета или реализации.	Внесение документа в кадровый учет, архивирование и обеспечение его доступности для последующего использования.
21	Практическая реализация задач, предусмотренных документом, или техническая оценка и подготовка.	Технический отдел занимается исполнением своих обязанностей в рамках договора (например, настройкой оборудования, внедрением ПО)

Продолжение таблицы 1

22	Передача документа в Отдел продаж для обработки и подготовки к передаче клиенту	Передача информации о статусе документа, условиях сделки или выполнении обязательств.
23	Продажа	Передача готовой услуги клиентам

Схема информационных потоков показывает, как происходит движение информации между отделами, подразделениями. Основное место в информационных потоках занимает формируемая вручную, или частично вручную документируемая информация.

Исходя из структуры предприятия, информационные потоки можно разделить на:

1. Информационные потоки, поступающие извне и наоборот;
2. Поток управленческой информации;
3. Поток служебной информации, перемещающейся между отделами.

К первой группе относятся информационные потоки, поступающие извне – это информация от клиентов, а также информация для клиентов – заявки, информация о сумме оплаты за заказ, сроки готовности, и прочее. Кроме основного движения потоков, имеются также внутренние потоки. Они относятся ко второй и третьей группе.

Поток управленческой информации также имеет двусторонний характер, организованный по принципу иерархии:

1. Командный и распорядительный;
2. Отчетная информация.

Источником командной информации является генеральный директор. Получателями командной информации являются подчиненные отделы. Источниками отчетной информации являются директора отделов.

Определено, что обрабатываются следующие данные: абонентские, технические, коммерческие, персональные. На основе перечисленных в таблице информационных потоков, можно выделить следующие защищаемые ресурсы организации: финансовая информация (данные об оплате услуг, финансовая отчетность), юридическая документация (договора с клиентами, приказы и распоряжения руководства), кадровые документы (данные о сотрудниках), техническая информация (технические задания, спецификации, отчёты и акты выполненных работ), коммерческая информация (предложения, договоры и другие документы, передаваемые клиентам).

К угрозам для информационных ресурсов данного провайдера относятся: утечка данных о платежных операциях, подмена финансовых документов, подделка договоров, кража или утечка персональных данных сотрудников, нарушение целостности технической документации, фальсификация актов выполненных работ, несанкционированный доступ к договорам с клиентами. Защищаемые ресурсы и угрозы будут подробнее рассмотрены в следующем разделе данной главы.

Рассмотрим общую структурную схему (другими словами – логическую схему) сети автономной системы (AS) провайдера (рисунок 3). На данной схеме отображена общая архитектура и концепт сети, главные функциональные модули, а также общий принцип работы.

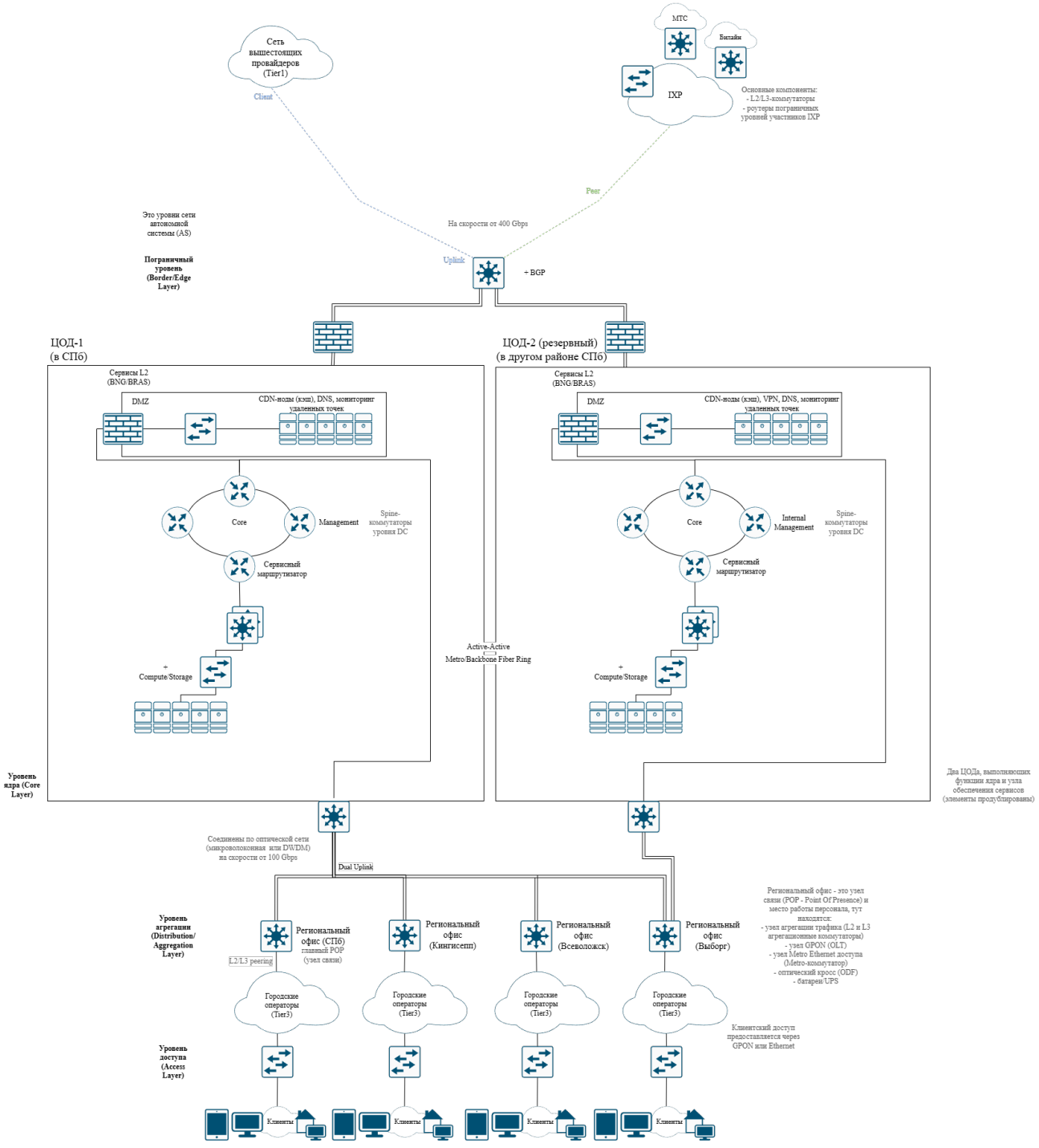

Рисунок 3 – Общая структурная схема

Согласно Трехуровневой иерархической модели Cisco (Hierarchical Network Model), которая предназначена для структурирования корпоративных сетей, схематически сеть провайдера можно разделить на три уровня: уровень доступа (Access Layer), уровень агрегации (Distribution/Aggregation Layer) и уровень ядра (Core Layer). Также иногда выделяют дополнительный пограничный уровень (Border/Edge Layer), но он не входит в базовую модель сети. Каждый уровень отвечает за конкретный процесс, уровни последовательно

связаны между собой. Таким образом, на уровне доступа происходит непосредственное подключение конечных абонентов – физических лиц и организаций, с помощью L2-коммутаторов, предоставленных провайдерами уровня Tier 3, то есть локальными или розничными (в данном случае, городскими). Городские провайдеры покупают интернет-транзит (это услуга, при которой есть обязательства одного оператора (UpLink) предоставлять глобальную связность и пропускать трафик в интересах другой сети (DownLink)) у регионального провайдера (уровень которого - Tier 2). Эта часть сети состоит в основном из свичей (Switch). На горизонте следующего уровня, уровня агрегации, располагаются региональные офисы регионального провайдера, через которые и проходит распределение трафика по городским провайдерам. В компании ПАО «Телеком» 4 региональных офиса в 4 разных городах – Санкт-Петербурге, Кингисеппе, Выборге и Всеволожске. Данные офисы выполняют роль Point-Of-Presence (POP), то есть узлов связи, где находится не только место работы персонала, работающего в компании, но и узел агрегации трафика (L2 и L3 агрегационные коммутаторы), узел GPON (OLT), узел Metro Ethernet доступа, оптический кросс (ODF), батареи/UPS. Они принимают GPON от уровня доступа, поднимают MPLS L2/L3 VPN, отдают трафик с ядро через MPLS. Региональные офисы связаны по оптической сети на скорости от 100Gbps с Центрами Обработки Данных (далее – ЦОД), которые находятся на уровне ядра данной схемы и являются ключевыми элементами инфраструктуры. В данной архитектуре два ЦОДа (основной и резервный), что является распределенным и отказоустойчивым решением. Они выполняют функции ядра и узла обеспечения сервисов, причем все ключевые сервисы продублированы. Вообще в целом центр сети оператора связи состоит из ядра, как правило, использующего технологию Multiprotocol Label Switching (MPLS), и сегментов aggregation-access сетей, которые позволяют подключать пользователей к сети. А уже на границе MPLS ядра находятся Provider Edge (PE) роутеры. Они производительнее, чем роутеры ядра (P Routers), потому как им нужно «держать» таблицу BGP. Пограничный уровень – стык сети провайдера с внешним миром. Там располагаются

маршрутизаторы и межсетевые экраны (брэндамауэры), обслуживающие внешние BGP-соединения: то есть соединяющие сеть провайдера с вышестоящими провайдерами уровня Tier 1 и точками обмена трафиком (далее – IXP). IXP является точкой обмена трафиком между равноправными участниками пиринга (в предоставленном случае, различными региональными провайдерами (МТС, Билайн)), где участники IXP располагают своим Border/Edge маршрутизаторы.

В рамках выпускной квалификационной работы разработка системы информационной безопасности будет проводиться для основного ЦОД. Так как ЦОД является ключевым элементом инфраструктуры и предназначен для размещения различных сервисов, с точки зрения информационной безопасности он относится к критическим элементам. Его недоступность влечёт отказ в предоставлении услуг.

Основной центр обработки данных (ЦОД) оператора выполняет роль активного ядра сети провайдера и центра предоставления сервисов. В нём размещаются ключевые элементы телекоммуникационной инфраструктуры, включая маршрутизаторы ядра, узлы авторизации абонентов, сервера и сервисы и многое другое. На уровне сетевой безопасности в основном ЦОД обычно обслуживаются межсетевые экраны, системы DPI, иногда CGNAT, а также пограничные маршрутизаторы, обеспечивающие взаимодействие с вышестоящими операторами, точками обмена трафиком и пиринговыми сессиями.

В целом стандартный набор сервисов, используемых интернет-провайдером, включает в себя: DHCP-сервер; DNS-сервер; один или (чаще) несколько серверов доступа (если таковые необходимы); сервер AAA (RADIUS); сервер биллинга; сервер баз данных; сервер хранения flow-статистики и биллинговой информации; сервер мониторинга сети; программно-аппаратный комплекс для сбора, накопления и хранения информации об абонентах операторов связи; устройства фильтрации трафика; сервисный шлюз Broadband Remote Access Server / Broadband Network Gateway (далее – BRAS/BNG).

Необходимо рассмотреть подробнее, за что конкретно отвечают данные сервисы. Основная задача для DHCP-сервера – выдача IP-адресов клиентам. Задача DNS-сервера – отвечать на DNS-запросы абонентов и преобразовывать их в IP-адреса. Сервер доступа представляет собой маршрутизатор, либо сервер, который обеспечивает клиентам доступ к сети Интернет. Технологии доступа различны, и провайдер сам может выбирать, что использовать (например, технологию IpoE или протоколы PPPoE, IPSec, L2TP, PPTP). AAA-сервер – это сервер идентификации пользователей, аутентификации, авторизации и аккаунтинга. Сервер биллинга (OSS/BSS) управляет учетными записями данных клиентов оператора, а именно отвечает за добавление и удаление пользователей, списание абонентской платы, изменение сведений о тарифах и многое другое. Работа данного сервера связана с сервером базы данных. Сервер хранения flow-статистики предназначен для непосредственной фиксации информации о «путешествиях» клиентов по сети Интернет. Network Management System (NMS) отвечает за управление OLT-терминалами (GPON) и коммутаторами агрегации (Metro Ethernet). Устройства фильтрации трафика, системы анализа трафика или DPI-устройства (Deep packet inspection). BRAS является ключевым оборудованием (сервер или программный комплекс) у интернет-провайдеров, которое контролирует доступ абонентов к интернету, выполняя функции авторизации (входа), учёта, назначения IP-адресов и применения тарифных планов (скорости, приоритетов трафика). СОРМ – программно-аппаратная платформа для реализации системы оперативно-розыскных мероприятий для силовых ведомств.

Число сервисов в сетях интернет-провайдеров может быть больше, это зависит как от организации сети, так и от разнообразия предоставляемых услуг (IP-телевидение, файловые ресурсы, телефония и другие). Однако существует возможность оптимизации сети, совмещение некоторых функций на одном устройстве. Например, фильтрацию, BRAS, CG-NAT, QoS, статистику можно объединить в платформе анализа трафика.

По большей части наполненность ЦОД у исследуемого провайдера не отличается от среднестатистического провайдера, предоставляющего только услуги Интернет.

Резервный ЦОД выполняет аналогичные функции, но работает в режиме Active/Active на уровне сервисов. Это предполагает наличие зеркальной вычислительной и дисковой инфраструктуры, а также дублирование основных сервисов и пограничных элементов. При этом объём и пропускная способность пограничного сегмента могут быть ниже, поскольку часть внешних подключений может оставаться привязанной к основному ЦОД. Дублирование отдельных сервисов осуществляется с учетом их специфики: кэширующие узлы CDN могут не дублироваться, системы хранения данных синхронизируются в синхронном или асинхронном режиме, узлы BNG часто работают в конфигурации Active/Active, а сервисы AAA и DHCP — в режиме Master/Master либо Master/Slave. Подсистема управления сетью (MGMT) в рамках резервного ЦОД обеспечивает аварийное восстановление (DR) и хранение резервных копий, включая офлайн и ленточные.

Два ЦОДа между собой связаны с учетом возможности прозрачного пропуска трафика второго уровня OSI (L2). Данная возможность является необходимой, потому что это поможет обеспечить отказоустойчивость, которая требуется в условиях работы ЦОДа, а также избежать блокировки каналов связи. В целом, при такой связи между ЦОДами также становится легко реализуемой масштабируемость сети. Трафик второго уровня прозрачно пробрасывается в VLAN-ах между площадками, а виртуальные ресурсы и приложения могут беспрепятственно мигрировать с одной площадки на другую, как будто они расположены в одном месте.

Рассмотрим структурную схему основного ЦОД (рисунок 4).

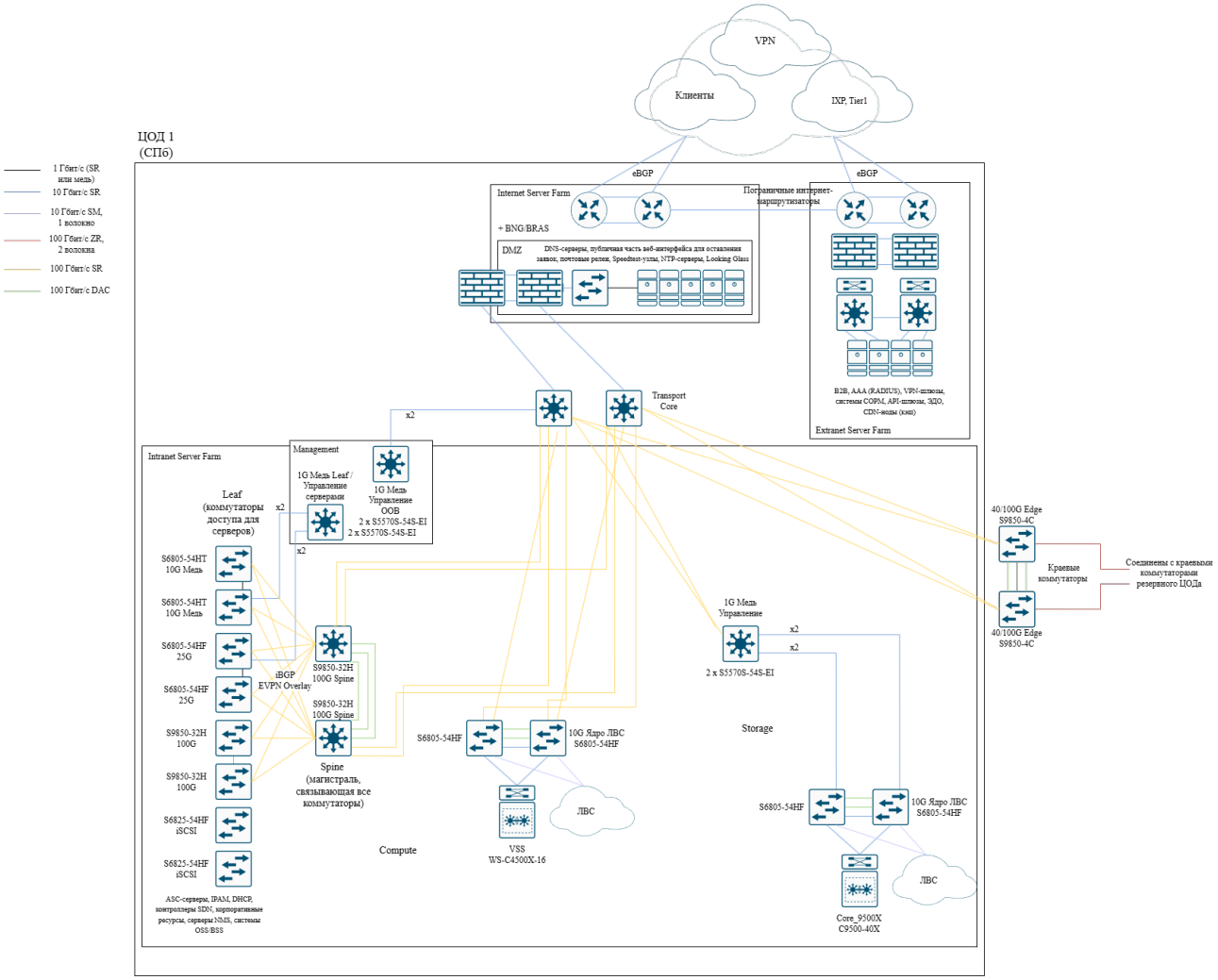

Рисунок 4 – Структурная схема ЦОД

В верхней части схемы находится пограничная зона – совокупность устройств, отделяющая недоверенную часть сети от доверенной. Там находятся маршрутизаторы, используется протокол BGP для общения с внешней сетью вышестоящих провайдеров и IXP, а также происходит фильтрация через межсетевые экраны.

Рядом с пограничной зоной можно выделить две зоны, так называемые публичную зону (Internet Server Farm), и зону взаимодействия (Extranet Server Farm). Первая содержит сервисы, которые должны быть доступны любым пользователям из глобальной сети, там же находится BRAS/BNG. Также в нее входит логически изолированный от критических ресурсов компании сегмент сети – демилитаризованная зона (далее – DMZ), в которой размещены публичные сервисы и CDN. К публичным сервисам в целом можно отнести и веб-серверы, и почтовые серверы или шлюзы, а также DNS-серверы и NTP-

серверы. Веб-серверы отвечают за работу официального сайта, личного кабинета для физических лиц (потенциальных абонентов GPON). В почтовые шлюзах происходит прием и первичная фильтрация внешней почты на спам. Используются отдельные коммутаторы, выводящие трафик по VPN-сети для связи с региональными офисами.

К зоне взаимодействия имеют доступ авторизованные партнеры, государственные органы и B2B-клиенты. Там находятся B2B-порталы управления, где расположены интерфейсы для клиентов Metro Ethernet (мониторинг L2/L3 VPN, управление SLA), а также системы COPM. Там же расположены API-шлюзы, используемые для интеграции с банками, платежными системами и вышестоящими магистральными операторами, пиринговые системы мониторинга для контроля обмена трафиком с другими сетями и системы документооборота (ЭДО).

Также стоит отметить, что основной ЦОД связан с резервным через краевые коммутаторы.

Всю нижнюю площадь структурной схемы занимает внутренняя доверенная зона (Intranet Server Farm). Это «мозг» провайдера, полностью изолированный от прямого доступа из интернета. Здесь сосредоточено управление критической инфраструктурой Metro Ethernet и GPON. К сервисам относится OSS/BSS, а также NMS, используется IPAM для учета и управления адресным пространством IP. Тут же находятся некоторые корпоративные ресурсы.

В контексте ЦОД внутренняя инфраструктура традиционно делится на три фундаментальных компонента: Compute (сервера, выполняющие вычисления), Storage (системы, где хранятся данные) и Network (сеть).

В данном ЦОД есть система хранения данных (далее – СХД), что является буквально физическим воплощением уровня Storage. В той зоне находятся специализированные устройства (дисковые массивы), которые обеспечивают хранение и доступ к данным для серверов. Совокупность серверов, которые обрабатывают информацию, является воплощением Compute. Многочисленные

серверы представляют собой терминальное оборудование информационной инфраструктуры машинного зала (далее – машзал) ЦОДа. По разным направлениям они взаимодействуют с локальной вычислительной сетью (далее – ЛВС) и СХД, находясь между ними.

ЛВС, представленная на схеме в нескольких местах, является частью уровня Network. Она обеспечивает связь между серверами и внешним миром, а также часто служит транспортом для связи Compute со Storage. Также выделена отдельная платформа управления, которая отделена от сервисного трафика.

Архитектура центральной части схемы построена на основе архитектуры Spine – Leaf. Также используются отдельные Leaf для Storage и Compute.

Двухуровневая архитектура, называемая также децентрализованной ячеистой (mesh) или Spine – Leaf архитектурой, применена при построении локальной сети ЦОДа. В этой архитектуре каждый коммутатор нижнего уровня, так называемый Leaf, соединен выделенной неблокируемой связью с каждым коммутатором верхнего уровня (Spine). Основное достоинство архитектуры Spine – Leaf заключается в том, что при обмене данными между двумя произвольно взятыми серверами трафик проходит только через один коммутатор верхнего уровня Spine и задержка сигнала становится предсказуемой и согласованной.

Таким образом, выигрыш по ключевому параметру времени задержки достигается резким увеличением количества связей для обмена данными между отдельными узлами.

Архитектура Spine – Leaf является продуктом естественного развития классических подходов к построению физического и транспортного уровня информационной инфраструктуры ЦОДа. Благодаря существенному снижению задержки передачи сигнала она имеет широкие перспективы практического применения при условии использования на физическом уровне сети волоконной оптики. Причем реализовать архитектуру Spine – Leaf можно на известной элементной базе, новых разработок не требуется.

Модернизация на физическом уровне сводится к установке дополнительного центрального кросса, наличие которого значительнотувеличивает эксплуатационную гибкость физического уровня информационной инфраструктуры машзала ЦОДа. Двойное сокращение средней длины кабелей сборки несколько упрощает развертывание линейной части информационной проводки.

Главный недостаток архитектуры Spine – Leaf – удвоение количества оптических претерминированных сборок на физическом уровне. Поэтому ее применение ужесточает требования к планированию кабельных трасс с учетом перспектив развития ЦОДа.

В целом, ядро сети реализовано как Spine уровень фабрики, архитектура в данном случае, как часто используется в последние годы, стала плоской, так как фабрика расплющена и роли размазаны.

Аппаратная часть информационной системы машинного зала ЦОДа – это комплекс компьютерного и сетевого оборудования, а также дополняющей его информационной проводки (таблица 2).

Таблица 2 - Оборудование

Устройство /Оборудо-вание	Описание	Назначение	Пример конфигурации	Кол-во
BGP Border Router	Высокопроизводительный L3 маршрутизатор	eBGP с Tier1 / IX, фильтрация, communities, RTBH	100G Uplinks, Full View, RPKI, FlowSpec	2

Продолжение таблицы 2

Border Switch (L2/L3)	Коммутатор агрегации Border	Подключение к DMZ	10/24/100G, LACP	2
CGNAT / UG Appliance	Аппаратный CGNAT / Universal Gateway	NAT444, Port Control, logging	40-80 Гбит/с, 5M+ сессий	2
NGFW	Межсетевой экран	Отслеживает сетевые пакеты, блокирует или разрешает их прохождение	UserGate NGFW	2
DMZ Service Switch	L3-коммутатор для DMZ	Подключение CGNAT,FW,DNS Отделение сегмента сети - для размещения публичных сервисов	10/25/40G	2
RADIUS-сервер	Сервер аутентификации	Аутентификация абонентов	FreeRADIUS	2
BRAS/BNG Router	Абонентский шлюз	Управление сессиями широкополосных абонентов, авторизация/учет трафика	1M+ сессий	2 (с резервированием)

Продолжение таблицы 2

BNG Access Switch	L3/Metro Switch	Подключение Metro/OLT	QinQ, VLAN, LACP	2
DHCP-сервер	Сервер адресации	IPv4	Redundant DHCP	2
Metro Core Switch	L3 агрегация	MetroE, DIA, VLAN	10/25/100G	2
OLT	GPON OLT	Терминация PON	16-32 PON портов	2-4
OSS/BSS Server	Сервер биллинга	Учет трафика/услуг	PostgreSQL, API	2
NMS Server	Мониторинг сети	SNMP	Zabbix	2
Log Server	Логирование	CGN/AAA/BNG logs	100ТБ	2
Management Switch	OOB управление	Управление оборудованием	1G, isolated	2
Compute Server	Универсальный сервер	AAA, DHCP, NMS, BSS	2xCPU, 128-256 GB RAM	4-6
Storage Server	Сервер хранения	Логи, биллинг, резерв	200 ТБ RAW	2
Console Server	Сервер доступа	Аварийный доступ	RS232/RSB	1
Time Server	NTP/PTP	Синхронизация	GPS/NTP	1
Рабочие станции (ПК)	Компьютеры для сотрудников (бухгалтерия и т.д.)	Работа сотрудников	ПК с оперативной памятью 8 ГБ и SSD 256 ГБ	от 50 шт.

Также необходимо ознакомиться с общей таблицей программного обеспечения организации (таблица 3).

Таблица 3 – Программное обеспечение

Категория ПО	Описание	Пример
Сетевое и маршрутизационное ПО	Встроенные ОС маршрутизаторов и коммутаторов	MikrotikRouterOS
Абонентский доступ	Аутентификация абонентов, DHCP-based доступ	Mikrotik BNG, Accel-PPP, Kea DHCP
Операционные системы серверов	Аутентификация и учет, сбор сессий и трафика и т.д.	FreeRADIUS, SQL-based
Биллинг и клиентские сервисы	Учет услуг и платежей, работа с клиентами, личный кабинет, оплата	CRM, YooKassa
Операционные системы компьютеров	Обеспечение работы рабочих станций	Windows 11
Антивирусное ПО	Защита от угроз	Kaspersky, ESET, Dr.Web
Firewall Software	Управление межсетевым экраном	PfSense
ПО для резервного копирования	Бэкапы данных	Acronis, Veeam Backup
Веб-сервер	Для размещения сайтов	Nginx, Apache
Клиентское ПО сотрудников	Работа сотрудников	Microsoft Office, LibreOffice

Продолжение таблицы 3

Корпоративные коммуникации	Программы для взаимодействия и совместной работы сотрудников	Битрикс24, Контур.Толк
Система автоматизации документооборота	Учет, бухгалтерия	1С:Предприятие

В рамках данной работы была рассмотрена структурная схема ЦОД регионального провайдера.

Детализация на уровне L2/L3 не приводится. Все межзональные взаимодействия реализованы на L3, маршрутизация выполняется динамическими протоколами. L2 используется только в зоне доступа.

Провайдер обеспечивает круглосуточное функционирование сети с высокими требованиями к доступности и непрерывности предоставления услуг. Нарушения работы ЦОД, сетевых узлов или сервисов авторизации потенциально приводят к значительным репутационным и экономическим потерям. Таким образом, объект исследования характеризуется сочетанием распределенной архитектуры, критичных сервисов и высокой зависимости бизнес-процессов от функционирования телекоммуникационной сети.

Провайдер функционирует на основе лицензий в области телематических услуг и услуг передачи данных в соответствии с законодательством Российской Федерации. Предоставление услуг «Интернет» является основной деятельностью компании и формирует её ключевые бизнес-процессы, зависимые от стабильного функционирования сетевой инфраструктуры и сервисов управления.

2.2. Анализ существующей системы защиты информации и применяемых мер безопасности

Для телекоммуникационного оператора высоким уровнем критичности обычно обладают процессы предоставления услуг связи, функционирования сетевых сегментов, маршрутизации трафика, авторизации и управления абонентами, а также взаимодействия с корпоративными и государственными заказчиками. Нарушение доступности данных процессов может привести к невозможности выполнения обязательств перед клиентами и государственными органами, что формирует финансовые и репутационные риски. К критическим активам относятся: маршрутизаторы ядра, BRAS/BNG, DNS-серверы, системы биллинга и CRM, инфраструктура OLT/ONT. Процессы обработки конфиденциальной информации выражены слабее, поскольку провайдер не является оператором значительных массивов персональных данных; однако в корпоративных сегментах возможны случаи передачи критичных данных клиентов.

Анализ текущего состояния информационной безопасности у исследуемого провайдера показывает, что используется разделение по сегментам сети, настроена отказоустойчивость и резервирование главных устройств, грамотно размещены Compute/Storage, есть выделенные сети управления.

К потенциально спорным моментам относятся:

1. Для защиты используется только NGFW на границе;
2. Отсутствует полноценная система мониторинга событий безопасности (SIEM);
3. Отсутствует решение Sandbox для проверки файлов;
4. DDoS-защита также представлена только фильтрацией на граничных маршрутизаторах;
5. Политика управления доступом документирована частично;
6. Контроль уязвимостей проводится нерегулярно;
7. Обучение сотрудников проводится эпизодически.

Объект защиты в исследуемом случае – это информационная инфраструктура ЦОД регионального телекоммуникационного провайдера, которая включает в себя: сервисную зону (BNG/BRAS, AAA, DHCP, RADIUS), вычислительную и серверную инфраструктуру (OSS/BSS, биллинг, БД), сеть управления и эксплуатации (NMS, OOB). Границы системы с внешней стороны – это абоненты, интернет, IX, партнеры. Границы системы с внутренней стороны – персонал компании, администраторы, подрядчики.

Активы являются потенциальными мишенями для злоумышленников. В рассматриваемой инфраструктуре целью атаки могут стать рабочие станции, серверы, сетевое оборудование, база клиентов, системы учёта, объекты коммерческой тайны (таблица 4).

Таблица 4 - Активы

Актив	Описание	Критичность
Персональные данные абонентов	ФИО, адреса, договоры	Высокая
Учетные данные	Логины, пароли	Высокая
Биллинг	Данные о трафике и платежах	Критическая
Сеть доступа	GPON, Metro Ethernet	Высокая
Сервисы доступа	AAA, DHCP	Критическая
Репутация компании	Доверие клиентов	Критическая
Доступность услуг	Интернет, VPN	Критическая
Конфигурация сети	Конфигурация на маршрутизаторах и коммутаторах	Высокая

При успешной атаке на любой из активов бизнес понесет значительные убытки и это повлияет на работу организации.

Высокоценные активы необходимо также проанализировать на уязвимости.

Рассмотрим виды уязвимостей, которые преобладают в исследуемом провайдере. К организационным относится низкая подготовка сотрудников, отсутствие регламентов по информационной безопасности, редкие бэкапы и мониторинг логов. Технические: старые версии сервисов и приложений.

Для того, чтобы произвести оценивание вероятности того, что угрозы будут реализованы, используется конкретная шкала. Согласно данной шкале есть низкая вероятность, при которой реализация угрозы считается маловероятной, есть средняя вероятность, при которой для реализации необходимы уязвимости в системе, а также есть высока вероятность. При высокой вероятности угроза легко реализуема и широко используется на практике. Оценив вероятность того, что злоумышленники воспользуются перечисленными уязвимостями, можно сделать вывод, что вероятность эксплуатации таких уязвимостей в современных условиях крайне высока. Для провайдера это означает риск полной потери контроля над инфраструктурой.

Оценим вероятность по категориям. Организационные уязвимости обладают критической вероятностью, так как человеческий фактор остается основной причиной инцидентов (около 70% всех случаев) и в целом низкая подготовка сотрудников делает компанию идеальной мишенью для фишинга, количество которого в РФ выросло в 4 раза за последний год. Отсутствие регламентов и логов также делает нахождение злоумышленника в сети сложно заметным. Без мониторинга логов невозможно вовремя обнаружить атаку или провести расследование. Редкие бэкапы повышают вероятность того, что компания выплатит выкуп при атаке шифровальщика, так как восстановить данные иными способами будет невозможно. Технические уязвимости обладают высокой вероятностью, потому что использование устаревшего ПО и сервисов считается довольно частым способом входа в систему для хакеров, так как они используют базы известных уязвимостей (CVE) для поиска систем, которые не обновлялись. Для эксплуатации публично известных уязвимостей требуется минимальная квалификации нарушителя. Уязвимости с самыми высокими

рисками нужно устранять в первую очередь с помощью комплексных мер защиты.

Определим потенциальный ущерб от успешного использования уязвимости хакерами. Обычно ущерб может оцениваться как низкий (локальные нарушения без существенного влияния на деятельность организации), средний (нарушение работы отдельных сервисов, утечки данных ограниченного характера) и высокий (отказ критически важных сервисов, компрометация информационной системы, значительные финансовые и репутационные потери). Первым необходимо рассмотреть финансовый ущерб. Он связан с прямыми потерями, например, возможна выплата выкупа за расшифровку данных, возможны расходы на восстановление инфраструктуры (оборудование, оплата труда специалистов), возможны штрафы от регуляторов за утечку персональных данных (ПДн) клиентов. К косвенным потерям относится репутационный ущерб и потеря доверия клиентов, что ведет к их массовому оттоку. Следующим является операционный ущерб. Он связан с полным параличом работы, так как атаки шифровальщиков или уничтожение данных могут полностью остановить предоставление услуг связи. Также расследование будет усложнено по причине отсутствия мониторинга логов и регламентов. К юридическому ущербу относится уголовная ответственность, возможная при крупных утечках ПДн или критических инцидентах, судебные иски от клиентов. Клиенты, чьи данные утекли, могут подать коллективные иски с требованием компенсации морального вреда. Ущерб от такого комплекса уязвимостей оценивается как критический и необратимый. Речь идет не просто о сбое в работе, а о существовании бизнеса как такового.

Для провайдера актуальны несколько типов нарушителей: внешний нарушитель с низким уровнем возможностей, внешний профессиональный нарушитель, внутренний нарушитель (так называемые инсайдеры).

Рассмотрим их подробнее. Внешний нарушитель с низким уровнем обладает следующими возможностями: доступ только к абонентскому сегменту, генерация сетевого трафика, попытки обхода ограничений. Он не имеет

легитимного доступа к инфраструктуре, его возможными целями является получение бесплатного доступа, проведение DDoS атаки и компрометация сервисов. Внешний профессиональный нарушитель обладает более профессиональными знаниями и его возможности включают использование ботнетов, использование автоматизированных средств атак, атаки на BGP, DHCP, DNS. Его цели: отказ в обслуживании, подмена маршрутов, кража данных. Внутренний нарушитель обладает возможностями доступа к сети управления, к конфигурациям, к базам данных. Целью может быть как саботаж или злоупотребление привилегиями, так и кража данных. Также встречаются и непреднамеренные нарушители, появление которых связано с различными причинами. Это могут быть ошибки администрирования, некорректные настройки или простой человеческий фактор [32].

Из перечисленных активов и уязвимостей, а также на основании Банка данных угроз ФСТЭК и анализа архитектуры сети можно вывести следующие угрозы безопасности активов, разделив их по зонам инфраструктуры.

Угрозы абонентской и сервисной зоны:

- УБИ.125: Несанкционированное подключение к беспроводной сети.

Суть угрозы заключается в том, что злоумышленник может получить доступ к беспроводной сети, минуя процедуры проверки подлинности.

- УБИ.126: Имитация легитимного беспроводного клиента или точки доступа.

Угроза связана с возможностью внедрения поддельных устройств беспроводного доступа, в результате чего злоумышленник перехватывает информацию, которая не была для него предназначена.

- УБИ.008: Повторное использование или восстановление учетных данных.

Суть данной угрозы заключается в том, что она реализуется при компрометации аутентификационной информации пользователя. В результате у злоумышленника есть доступ к данным пользователя и функциям системы, а пользователь оказывается в неведении.

- УБИ.127: Совершение подмены действий пользователя путём обмана.

Угроза основана на манипулировании пользователем, вследствие чего нарушитель может выполнять действия от его имени.

- УБИ.128: Подмена личности доверенного пользователя.

Реализация угрозы приводит к тому, что злоумышленник маскируется под легитимного субъекта доступа.

- УБИ.130: Незаметное искажение информации, которая хранится на сетевых ресурсах.

Заключается в скрытом изменении информации, которая размещена на сетевых хранилищах, из-за чего пользователи могут быть введены в заблуждение.

- УБИ.140: Нарушение доступности сервисов.

Данная угроза проявляется в блокировании доступа законных пользователей к ресурсам системы вследствие резкого увеличения объема сетевых соединений.

- УБИ.098: Выявление доступных сетевых портов и сервисов.

Угроза заключается в возможности анализа состояния портов системы, из-за чего злоумышленник может определить потенциальные точки атаки.

- УБИ.100: Использование ошибок настройки механизмов аутентификации.

В рамках данной угрозы нарушитель может получить доступ к системе ьез прохождения штатной процедуры идентификации за счет эксплуатации некорректной работы средств аутентификации.

- УБИ.152: Блокирование доступа путем удаления учетных данных.

Реализация угрозы приводит к лишению доступа легитимных пользователей за счёт сброса их аутентификационной информации.

- УБИ.213: Компрометация многофакторной аутентификации.

Связана с обходов механизмов многофакторной защиты.

- УБИ.170: Несанкционированные шифрование данных

В результате реализации угрозы доступ к информации может быть утрачен, так как она будет криптографически преобразована.

- УБИ.174: Фарминг.

Угроза заключается в незаметном перенаправлении пользователя на поддельный интернет-ресурс, чтобы таким образом получить доступ к защищаемой информации.

- УБИ.190: Заражение вредоносным файлом при посещении веб-ресурсов.

Реализуется при автоматической загрузке и установке вредоносного кода на пользовательское устройство при его серфинге сети.

- УБИ.201: Утечка данных автозаполнения браузера.

Использование встроенных функций автозаполнения может привести к компрометации учётных данных пользователя и их последующему неправомерному использованию

- УБИ.027: Искажение вводимой и выводимой на периферийные устройства информации.

Угроза проявляется в подмене данных, отображаемых на периферийных устройствах, что может привести к дезориентации и введению пользователей в заблуждение.

- УБИ.175: Фишинг.

Сущность угрозы состоит в получении конфиденциальной информации путём убеждения пользователя добровольно передать защищаемые сведения.

- УБИ.041: Межсайтовый скриптинг (XSS).

Угроза заключается во внедрении вредоносного кода в веб-ресурсы системы, что позволяет воздействовать на пользователей или перехватывать данные.

- УБИ.042: Межсайтовая подделка запросов (CSRF).

Реализация угрозы возможна при принуждении пользователя к выполнению нежелательных действий посредством перехода по специально сформированным ссылкам.

- УБИ.181: Перехват одноразовых кодов подтверждения.

Данная угроза позволяет злоумышленнику получить контроль над критически важными пользовательскими операциями в режиме реального времени

- УБИ.074: Несанкционированное получение учетных данных.

Угроза связана с извлечением аутентификационной информации из оперативной памяти вычислительных устройств.

Угрозы DMZ и вычислительной инфраструктуры:

- УБИ.019: Подмена данных в DNS-кеше.

Угроза проявляется в изменении записей доменных имён, что позволяет перенаправлять сетевой трафик через контролируемые нарушителем узлы.

- УБИ.185: Несанкционированная корректировка параметров настройки средств защиты информации.

Реализация угрозы приводит к ослаблению механизмов безопасности за счёт изменения их конфигурации без соответствующих полномочий.

- УБИ.187: Воздействие на управляющую среду средств защиты

Угроза связана с вмешательством в программную среду управления средствами защиты информации и изменением их режима работы

- УБИ.173: Массовая рассылка сообщений через веб-сервер.

Данная угроза заключается в использовании веб-ресурсов для распространения нежелательной информации без согласия владельца сервиса.

- УБИ.172: Распространение вредоносного ПО через электронную почту.

Угроза реализуется при доставке вредоносных программ пользователям посредством заражённых электронных сообщений.

- УБИ.111: Утечка данных через скрытые каналы передачи.

Сущность угрозы состоит в несанкционированном выводе защищаемой информации за пределы системы обходными способами.

- УБИ.159: Принудительный веб-доступ к уязвимым компонентам.

Позволяет получить доступ к данным или функциям веб-приложений за счет ошибок в их механизмах защиты.

- УБИ.116: Получение конфиденциальной информации, которая передается в трафике.

В результате данной угрозы у злоумышленника будет доступ к данным, которые он перехватит по сети.

- УБИ.028: Несанкционированный доступ в обход.

В результате данной угрозы путем обхода средств защиты у нарушителя будет доступ к защищаемой информации.

- УБИ.136: Потеря информации.

В том случае, если работа узлов хранилища будет несогласованной, это может привести к тому, что при копировании и обработке информации она может быть удалена или утеряна.

- УБИ.176: Нарушение процессов по причине задержек во времени, которое происходит из-за долгой работы средств защиты.

По причине долгой работы в процессе обработки информации, системы могут придти в состояние отказа в обслуживании.

- УБИ.205: Нарушение работы компьютера и потеря данных из-за неправильной конфигурации установленных средств защиты.

Компьютер может работать некорректно, если средства защиты информации буду блокировать легитимный трафик.

Угрозы ядра и пограничной зоны:

- УБИ.030: Использование стандартных паролей.

Угроза проявляется в том, что злоумышленник может пройти процедуру авторизации, используя предустановленные по умолчанию учётные данные, доступные в открытых источниках

- УБИ.034: Эксплуатация слабых мест сетевых протоколов.

Суть угрозы в том, что злоумышленник может получить несанкционированный доступ к информации, передаваемой в сети, за счёт уязвимостей протоколов локальной или глобальной сети.

- УБИ.090: Незаконное создание пользовательских учетных записей.

Угроза заключается в возможности внедрения дополнительных аккаунтов злоумышленником, что открывает доступ к системе и её ресурсам.

- УБИ.088: Несанкционированное копирование защищаемой информации.

Реализация угрозы позволяет злоумышленнику получить копии конфиденциальных данных без разрешения владельца.

- УБИ.023: Модификация компонентов автоматизированной системы.

Угроза заключается в возможности изменения программных или аппаратных элементов системы, включая внедрение закладок и изменение функциональности.

- УБИ.024: Изменение режимов работы аппаратных компонентов.

Суть угрозы — несанкционированное изменение конфигурации оборудования, например, через BIOS/UEFI, что может повлиять на функционирование системы.

- УБИ.038: Истощение ресурсов хранилищ больших данных.

Угроза проявляется в блокировании доступа к данным или снижении производительности системы из-за перегрузки вычислительных ресурсов.

- УБИ.067: Несанкционированные доступ к информации.

Суть угрозы в том, что пользователь может получить доступ к информации, предназначенной для других лиц, как случайно, так и преднамеренно.

- УБИ.069: Нарушение работы каналов связи.

Угроза заключается во вмешательстве в сетевые протоколы, что может привести к сбоям или искажению данных при передаче.

- УБИ.071: Восстановление удалённых данных без разрешения

Реализация угрозы позволяет получить доступ к информации, которая была удалена, посредством прямого обращения к носителям данных.

- УБИ.073: Несанкционированный доступ к сетевому оборудованию.

Суть угрозы состоит во мешательстве в работу активного или пассивного оборудования, как физического, так и виртуального, с целью изменения его поведения.

- УБИ.057: Неконтролируемое копирование информации.

Угроза заключается в невозможности полного контроля за автоматически создаваемыми копиями информации в распределённых системах хранения.

- УБИ.084: Несанкционированный доступ к системам хранения данных.

Суть угрозы – это возможность вмешательства в работу виртуальных и физических хранилищ информации с деструктивной целью.

- УБИ.060: Неконтролируемое удаление информации хранилищем.

Угроза проявляется в удалении части данных без уведомления пользователей или администраторов, что может повлечь потерю критической информации.

- УБИ.063: Неправильное использование функционала ПО и оборудования.

Реализация угрозы возможна при использовании системных возможностей программ и устройств способами, вызывающими сбои или деструктивное воздействие на информацию.

- УБИ.192: Эксплуатация уязвимых версий ПО.

Суть угрозы – это использование злоумышленником известных уязвимостей в ПО для воздействия на систему или получение несанкционированного доступа.

- УБИ.189: Маскировка действий вредоносного кода.

Угроза проявляется в сокрытии в системе действий вредоносного ПО, что затрудняет их обнаружение и нейтрализацию.

- УБИ.104: Определение архитектуры и топологии сети.

Суть угрозы в том, что при получении злоумышленником сведений о расположении узлов и структуре сети, ему будет легче провести атаку.

- УБИ.179: Несанкционированная модификация информации.

Угроза заключается в возможности физического или программного воздействия на носители данных для изменения их содержимого без разрешения.

- УБИ.113: Перезагрузка оборудования и программных модулей.

Реализация угрозы приводит к сбросу состояния оперативной памяти или функционала устройств, вызывая временный отказ в работе.

- УБИ.103: Определение типов объектов защиты.

Суть угрозы в анализе выходных данных системы для выявления категорий информации и элементов, подлежащих защите.

- УБИ.012: Влияющее деструктивно изменение конфигурации ПО.

Угроза проявляется в вмешательстве в рабочую среду приложений с целью их разрушения или изменения функциональности.

- УБИ.015: Доступ к файлам обходными путями.

Реализация угрозы позволяет получить доступ к защищаемым каталогам и файлам с использованием нестандартных путей.

- УБИ.018: Угроза загрузки нештатной операционной системы.

Суть угрозы заключается в подмене загружаемой ОС через несанкционированное изменение настроек BIOS/UEFI, что открывает полный контроль над системой.

Угрозы сети управления:

- УБИ.031: Использование авторизационных механизмов для повышения привилегий.

Угроза проявляется в получении доступа к информации, которая должна быть доступна только тем пользователям, которые обладают большим количеством прав.

- УБИ. 007: Воздействие на программы с высокими привилегиями.

В системе злоумышленник может повысить свои права различными способами.

- УБИ.117: Перехват потоков с привилегиями.

Нарушитель имеет доступ к потоку данных, который создан приложением, обладающим большим количеством прав.

- УБИ.118: Перехват процессов с привилегиями.

Нарушитель имеет доступ к процессам, которые созданы приложением, обладающим большим количеством прав.

- УБИ.122: Повышение привилегий.

При помощи воздействия программными атаками на процессы, злоумышленник может выполнять расширение прав в системе.

- УБИ.198: Скрытая регистрация учётных записей администраторов.

Реализация угрозы возможна через скрытое создание вредоносным ПО дополнительных учётных записей с правами администратора.

- УБИ.212: Перехват управления информационной системой.

Суть угрозы в получении несанкционированного доступа к управлению системой, её ресурсами и компонентами через подмену средств централизованного контроля.

Согласно всему вышеперечисленному, получим модель угроз (приложение 1).

2.3. Классификация информационных систем и оценка рисков

Классификация объекта информатизации осуществляется на основании Руководящего документа «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) (таблица 5).

Таблица 5 – Классификация АС

Критерии классификации АС	Перечень	Описание
Перечень защищаемых информационных ресурсов	1.Финансовая информация (отчеты, счета)	Уровень конфиденциальности: 1.Коммерческая тайна

	2.Юридическая документация (договоры с клиентами) 3.Персональные данные сотрудников 4.Техническая информация (задания, спецификация)	2.Служебная информация ограниченного доступа 3.Конфиденциальная информация 4.Служебная информация

Продолжение таблицы 5

Состав пользователей	Пользователи делятся на группы (руководство, бухгалтерия, технический отдел, отдел кадров)	АС используется коллективно сотрудниками организации, многопользовательские (МП)
Матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС	1.Субъекты доступа - пользователи, группы пользователей, отделы 2. Объекты доступа - защищаемые информационные ресурсы 3. Полномочия - права доступа: чтение, запись, изменение, удаление, выполнение	
Режим обработки данных в АС	Обработка данных носит коллективный характер с определенными правами доступа	Коллективный, разграниченный доступ

Субъекты доступа	Финансовая информация	Персональные данные	Юридическая документация	Техническая информация	Коммерческая информация
Руководство	Чтение, изменение	Чтение, изменение	Чтение, утверждение	Чтение	Чтение, изменение
Бухгалтерия	Чтение, запись	Чтение	Чтение	Нет доступа	Чтение
Отдел кадров	Нет доступа	Чтение, запись	Нет доступа	Нет доступа	Нет доступа
Технический отдел (ИТ)	Чтение	Чтение	Нет доступа	Чтение, изменение	Чтение
Отдел продаж	Чтение	Чтение	Чтение, запись	Чтение	Чтение, запись
Сотрудники (общий доступ)	Нет доступа	Чтение своих данных	Чтение	Нет доступа	Нет доступа
Системный администратор (ИТ)	Полный доступ	Полный доступ	Полный доступ	Полный доступ	Полный доступ

На основании вышеуказанных критериев исследуемого провайдера можно отнести к первой группе АС. Так как АС обрабатывает информацию, которая может относиться к коммерческой тайне или персональным данным, то по уровню защищенности она относится к классу «1Д».

Также рассмотрим недостатки АС организации, на основе требований, предъявляемых в Руководящем документе Государственной технической комиссии при Президенте РФ «Автоматизированные системы защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» к классу «1Д»» (таблица 6).

Таблица 6 – Недостатки АС организации

Подсистема	Требование в РД	Состояние в АС	Недостаток
Подсистема управления доступом	Идентификация, проверка подлинности и контроль доступа субъектов: в систему	1.Матрица доступа частично определена. 2.Используются стандартные учетные записи.	1.Отсутствует формальная реализация ролей и разграничения доступа. 2.Не применяются двухфакторная аутентификация и защищенная регистрация.
Подсистема регистрации и учета	Регистрация и учет: входа (выхода) субъектов доступа в (из) систему (узел сети)	Нет данных о системах логирования и мониторинга.	Отсутствует контроль и анализ действий пользователей.

	Учет носителей информации	1.Нет данных о ведении журнала учёта носителей информации. 2.Не реализована классификация и маркировка носителей.	1.Отсутствует система учёта и регистрации носителей информации. 2.Носители не классифицируются и не маркируются.

Продолжение таблицы 6

		3.Не упоминается уничтожение или утилизация носителей информации.	3.Не описаны меры по безопасному уничтожению носителей.
Подсистема обеспечения целостности	Обеспечение целостности программных средств и обрабатываемой информации	Применяются резервные копии.	Нет средств криптографической защиты информации (КЗИ).
	Физическая охрана средств вычислительной техники и носителей информации	1.Не указаны меры физической охраны помещений, где расположены средства вычислительной техники. 2.Нет информации о системах контроля и	1.Отсутствует физическая охрана и специальные меры контроля доступа. 2.Нет ограничения на вход в помещения с

		управления доступом. 3.Не указано, ведется ли охрана и видеонаблюдение в помещениях с критической инфраструктурой.	критическим оборудованием. 3.Отсутсвует видеонаблюдение для контроля физических угроз.

Продолжение таблицы 6

	Периодическое тестирование СЗИ НСД	Не упомянуто.	Нет данных о регулярном тестировании СЗИ НСД на работоспособность.
	Наличие средств восстановления СЗИ НСД	1.Есть средства резервного копирования конфигураций СЗИ НСД. 2.План восстановления СЗИ НСД после сбоя или атаки.	2. Не разработан план восстановления работоспособности СЗИ.

Так как по результатам диагностики уровня защищенности можно сделать вывод о низком уровне зрелости процессов информационной безопасности, инфраструктура ПАО «Телеком» требует комплексной модернизации с использованием отраслевых стандартов и передовых решений в сфере информационной безопасности.

Был проведен анализ и оценка рисков информационной безопасности, для которых были использованы выявленные активы, уязвимости, а также перечень актуальных угроз из Банка данных угроз безопасности информации ФСТЭК России. При рассмотрении угроз была учтена архитектура сети а также распределение компонентов по зонам инфраструктуры.

Оценка рисков выполнена на основе качественного метода, который рекомендован ФСТЭК России и широко применяем при проектировании и анализе систем обеспечения информационной безопасности. В соответствии с данным методом уровень риска определяется как совокупная оценка вероятности реализации угрозы и возможного ущерба для организации.

В результате анализа абонентской и сервисной зоны было выявлено, что абонентская и сервисная зона характеризуется наибольшим количеством угроз с высокой и критической степенью риска. Это обусловлено прямым взаимодействием данной зоны с конечными пользователями и сетью Интернет.

К наиболее значимым угрозам относятся угрозы обхода и компрометации механизмов аутентификации (УБИ.008, УБИ.074, УБИ.181, УБИ.201), подмены доверенного пользователя и действий пользователя (УБИ.127, УБИ.128), а также угрозы фишинга и фарминга (УБИ.175, УБИ.174). Вероятность реализации данных угроз оценивается как высокая, а возможный ущерб – как высокий, что определяет критический уровень риска.

Существенную опасность представляют угрозы, связанные с беспроводными сетями, включая подключение к сети в обход аутентификации и подмену точек доступа или клиентов (УБИ.125, УБИ.126). Учитывая распространённость атак на беспроводную инфраструктуру, риск данных угроз оценивается как высокий.

Кроме того, значимыми являются угрозы внедрения вредоносного кода через веб-ресурсы и заражённые сайты (УБИ.190), межсайтового скриптинга и подделки запросов (УБИ.041, УБИ.042), а также угрозы отказа в обслуживании (УБИ.140). Реализация данных угроз может привести к нарушению доступности сервисов провайдера и утечке пользовательских данных.

В целом абонентская и сервисная зона рассматривается как основной источник инцидентов информационной безопасности, требующий приоритетного применения мер защиты.

В результате анализа зоны DMZ и вычислительная инфраструктура было выявлено, что угрозы в значительной степени связаны с функционированием публичных сервисов и серверных компонентов. Наиболее опасными являются угрозы, направленные на веб-приложения и сетевые сервисы, включая форсированный веб-браузинг (УБИ.159), перехват сетевого трафика (УБИ.116) и заражение DNS-кеша (УБИ.019). Уровень риска для данных угроз оценивается как высокий или критический, поскольку их реализация может затронуть значительное количество пользователей.

Также существенную опасность представляют угрозы утечки информации по скрытым каналам (УБИ.111), распространения вредоносного ПО через почтовые сервисы (УБИ.172). Отдельную группу составляют угрозы, связанные с особенностями функционирования систем хранения и обработки больших данных (УБИ.136, УБИ.057, УБИ.060), для которых вероятность реализации оценивается как низкая или средняя, однако возможный ущерб может быть значительным.

Таким образом, DMZ и вычислительная инфраструктура характеризуются высокой концентрацией рисков, связанных с доступностью сервисов и защитой данных.

Анализ зоны ядра сети и пограничной зоны показал, что вероятность реализации большинства угроз в данной зоне оценивается как средняя или низкая, но потенциальный ущерб от их реализации является высоким или критическим.

Наибольшую опасность представляют угрозы, которые направлены на использование уязвимых версий ПО (УБИ.192), маскирования действий вредоносного кода (УБИ.189), а также угрозы несанкционированного копирования и модификации защищаемой информации (УБИ.088, УБИ.179).

Реализация данных угроз может привести к полной компрометации информационной системы провайдера.

Существенными также являются угрозы, связанные с использованием слабостей сетевых протоколов (УБИ.034), несанкционированным доступом к сетевому оборудованию (УБИ.073) и определением топологии вычислительной сети (УБИ.104). Эти угрозы, как правило, используются нарушителем на этапе разведки и подготовки более сложных атак.

Зона сети управления характеризуется меньшей вероятностью реализации угроз, однако последствия успешной атаки в данной зоне являются наиболее тяжёлыми. Ключевыми угрозами являются угрозы повышения привилегий и воздействия на программы с высокими привилегиями (УБИ.031, УБИ.007, УБИ.122), скрытной регистрации учетных записей администраторов (УБИ.198) и перехвата управления информационной системой (УБИ.212).

Компрометация сети управления может привести к утрате контроля над средствами защиты информации и ключевыми компонентами инфраструктуры, что обуславливает необходимость применения усиленных мер защиты и строгого разграничения доступа.

Проведённая оценка рисков информационной безопасности показала, что наибольшую опасность для регионального телекоммуникационного провайдера представляют угрозы, реализуемые в абонентской и сервисной зоне, а также в DMZ, что обусловлено их высокой доступностью для внешнего нарушителя и активным взаимодействием с сетью Интернет.

Компрометация ядра сети и сети управления характеризуется меньшей вероятностью реализации, однако потенциальный ущерб от успешной атаки в данных зонах является критическим и может привести к полной утрате управляемости информационной системой и нарушению предоставления услуг связи. Полученные результаты подтверждают необходимость комплексного и зонального подхода к построению системы информационной безопасности провайдера с учётом приоритетности защиты наиболее уязвимых элементов инфраструктуры.

ГЛАВА 3. РАЗРАБОТКА ПРОЕКТА СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ РЕГИОНАЛЬНОГО ПРОВАЙДЕРА

В третьей главе представлена разработка проекта системы информационной безопасности, а также продемонстрирован частичный пример настройки технических средств защиты информации для условного регионального телекоммуникационного провайдера ПАО «Телеком».

В разделе 3.1 приведены рекомендации для улучшения состояния архитектуры информационной безопасности в компании. В разделе 3.2 выполнено оформление сопроводительных документов. В разделе 3.3 проведена финальная оценка результатов разработки проекта системы информационной безопасности.

3.1. Проектирование архитектуры информационной безопасности

На основании анализа существующей архитектуры ЦОДа информационной системы регионального телекоммуникационного провайдера, выполненного во второй главе выпускной квалификационной работы, а также с учётом выявленных уязвимостей, актуальных угроз безопасности информации и результатов оценки рисков, в рамках практической части работы разработаны предложения по доработке и совершенствованию архитектуры информационной безопасности.

Рекомендации включают в себя следующее:

1. Внедрение технических средств защиты, при настройке правил на которых для разграничения ролей и доступов должен использоваться принцип минимальных привилегий;
2. Добавление централизованной системы управления учётными записями;
3. Для критичных систем внедрение допуска по сертификатам или аппаратным токенам;
4. Настройка шифрования данных в каналах и на носителях;
5. Настройка резервного копирования и хранения копий в защищённом сегменте;

6. Также процессы обновления, мониторинга, отчётности;

7. Обновление полного комплекта документации информационной безопасности.

Анализ показал, что исходная архитектура сети в целом соответствует типовой модели оператора связи, однако в ряде сегментов отсутствует достаточная глубина защиты, а также не обеспечено полное соответствие архитектурных решений выявленным уровням риска. В связи с этим проектирование архитектуры информационной безопасности направлено не на радикальное изменение структуры сети, а на её целенаправленную корректировку за счёт внедрения дополнительных средств защиты и перераспределения функций безопасности между существующими сегментами, что перечислено ранее.

В абонентской и сервисной зоне выявлена повышенная концентрация угроз, связанных с компрометацией учетных данных, подменой пользователей, внедрением вредоносного кода и атаками социальной инженерии. В существующей архитектуре защита данной зоны в основном ограничивается базовыми механизмами аутентификации, управлением доступа и сетевой фильтрацией. В рамках проектируемой архитектуры предлагается дополнительно реализовать сегментацию абонентского трафика на уровне L2/L3, внедрить централизованные механизмы многофакторной аутентификации для доступа к сервисам самообслуживания, ввести централизованную систему управления учетными записями (AD/LDAP), настроить ролевую модель (RBAC), а также использовать средства фильтрации и анализа HTTP/HTTPS-трафика для защиты от фишинга, фарминга и межсайтовых атак, в виде специализированного межсетевого экрана WAF. Кроме того, предлагается усилить контроль беспроводного доступа за счёт отказа от небезопасных механизмов автоматической аутентификации и внедрения средств обнаружения подмены точек доступа, ввести Network Access Control (NAC) для проверки устройств перед подключением. Также необходимо пересмотреть настроенные правила на NGFW. Для централизованного

управления всеми продуктами можно использовать системы централизованного управления (Management Center).

В демилитаризованной зоне и вычислительной инфраструктуре в ходе анализа было установлено, что публичные сервисы провайдера являются потенциальной точкой входа для внешнего нарушителя. Для устранения выявленных рисков предлагается чётко разграничить функции DMZ и внутренних сегментов, ограничив сетевые взаимодействия строго необходимыми направлениями. Дополнительно тоже целесообразно внедрить WAF в данной зоне. Также рекомендуется внедрить такие средства, как IDS/IPS. Стоит рассмотреть и настройку сбора логов с маршрутизаторов, серверов, БД, домена, антивирусов, то есть добавить SIEM-систему (например, Solar JSOC, MaxPatrol SIEM, Wazuh, Qradar, UserGate Log Analyzer) [43]. Для серверных сегментов рекомендуется применение средств контроля целостности и централизованного управления обновлениями программного обеспечения [33].

В ядре сети и пограничной зоне анализ показал недостаточную изоляцию критически важных компонентов от потенциально скомпрометированных сегментов. В рамках проектируемой архитектуры предлагается усилить пограничную защиту за счёт внедрения межсетевых экранов с функциями глубокого анализа пакетов, а также минимизировать количество точек административного доступа к сетевому оборудованию. Можно также добавить систему глубокого анализа сетевого трафика (NTA), например, PT NAD. Дополнительно рекомендуется реализовать строгий контроль конфигураций сетевых устройств, включая централизованное хранение эталонных конфигураций и регулярную проверку их целостности. Необходимо также включить шифрование данных в каналах и на носителях, настроить DLP для контроля утечек и антивирус на рабочих станциях, обеспечить резервное копирование и хранение копий в защищённом сегменте.

Особое внимание в рамках проектирования архитектуры информационной безопасности уделяется сети управления. В существующей архитектуре функции администрирования частично пересекаются с пользовательскими и

сервисными сегментами, что повышает риск компрометации средств управления. Для устранения данной проблемы предлагается логически и, при возможности, физически изолировать сеть управления, использовать защищённые каналы администрирования и внедрить средства контроля привилегированных учетных записей. Дополнительно рекомендуется реализовать централизованный аудит действий администраторов и мониторинг событий безопасности в режиме, близком к реальному времени.

Структурная схема ЦОДа с учетом рекомендаций представлена ниже (рисунок 5).

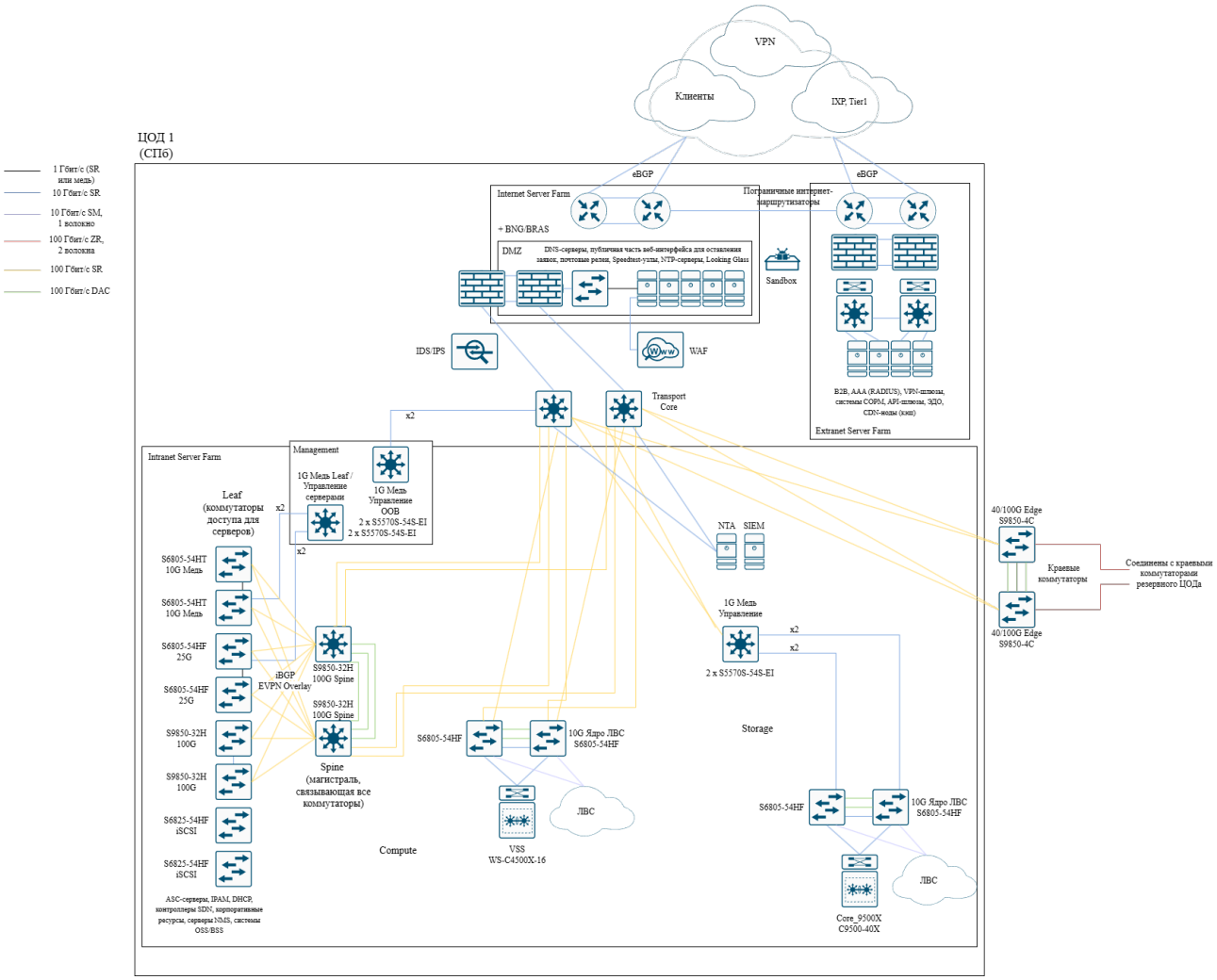

Рисунок 5 – Обновленная структурная схема

Эффективность функционирования всего комплекса мер безопасности напрямую зависит от корректности конфигурации его базовых элементов. Учитывая центральную роль межсетевого экранирования в архитектуре защиты, необходимо разобрать типичные ошибки инсталляции. К примеру, рассмотрим

наиболее частые проблемы, с которыми сталкиваются при настройке одного из главнейших средств защиты сети – NGFW, на примере UserGate NGFW.

Первая проблема: при фильтрации контента через межсетевой экран не используется дополнительный встроенный компонент “Антивирус” (рисунок 6).

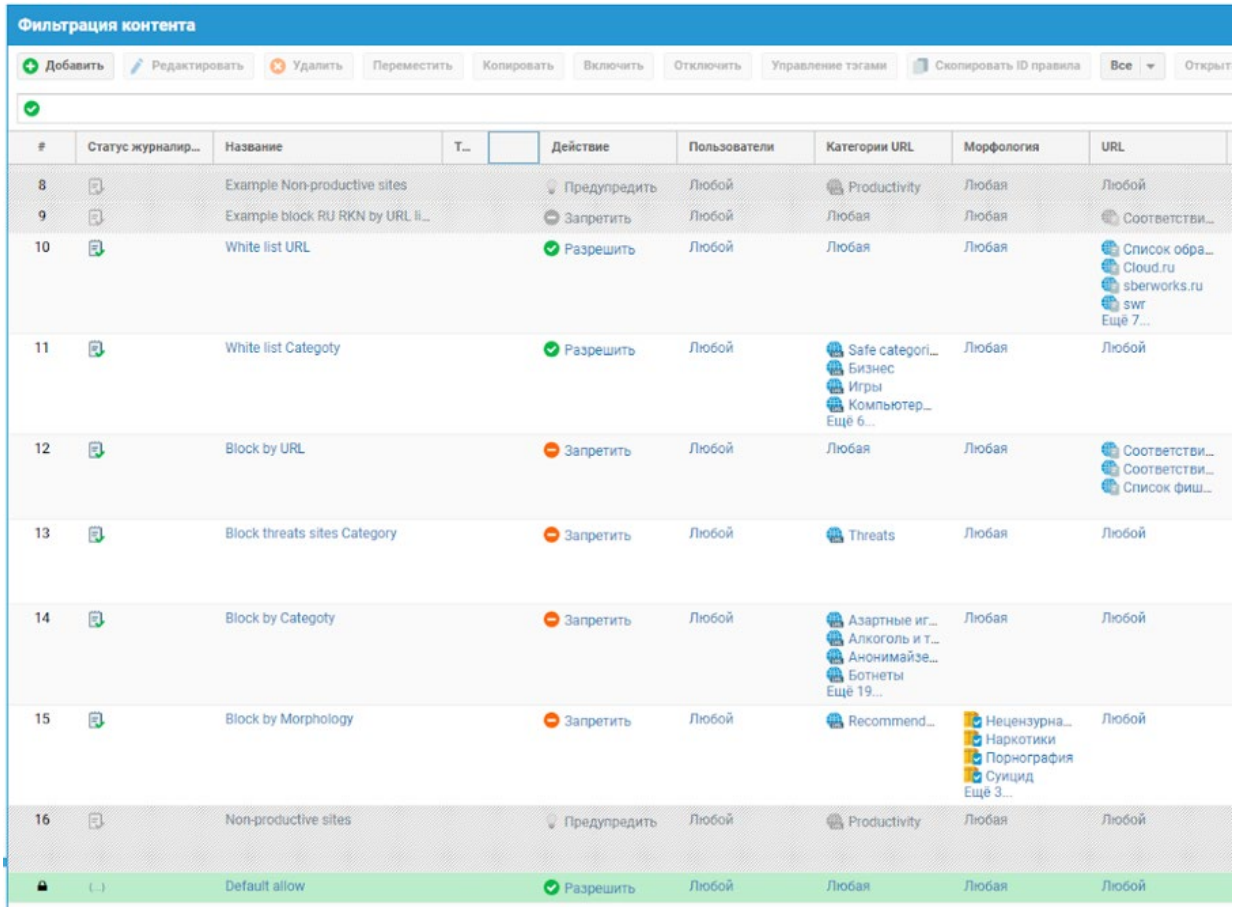

Рисунок 6 – Скриншот рабочей области UserGate NGFW

Это может привести к таким последствиям, как увеличение риска заражения, пропуск вредоносных файлов. По данной причине необходимо пересмотреть политику фильтрации контента и включить антивирус. Рекомендуется использовать данный модуль для дополнительной проверки трафика потоковым антивирусом на уровне периметра.

Вторая проблема: не используется блокировка по приложениям высокой группы угроз для зон сети, из которых есть доступ в Интернет, которую необходимо настраивать в разделе «Межсетевой экран» (рисунок 7).

Рисунок 7 – Скриншот правила

Из возможных последствий можно привести в пример подключение к ресурсам из неограниченного пула IP-адресов.

Стоит учитывать, что для корректной работы некоторых сигнатур приложений в профилях необходимо наличие сигнатур определенного протокола, в таком случае в профилях приложений рекомендуется добавлять фильтр “name = HTTP or name = SSL/TLS” (рисунок 8).

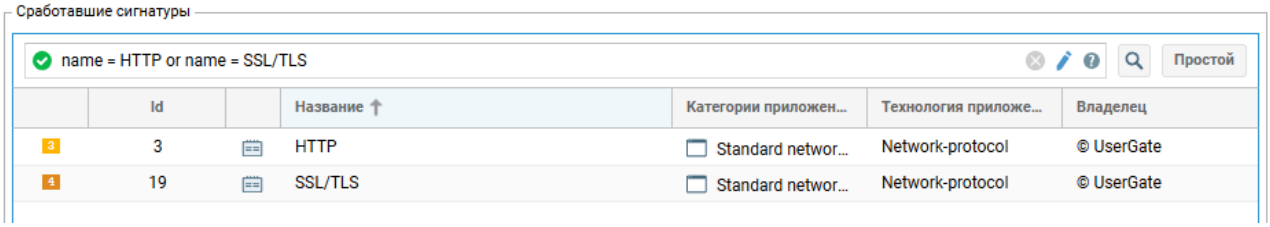

Рисунок 8 – Скриншот сигнатур

Третья проблема: отсутствует настройка регулярного экспорта конфигурации межсетевого экрана на внешние серверы для резервирования (рисунок 9).

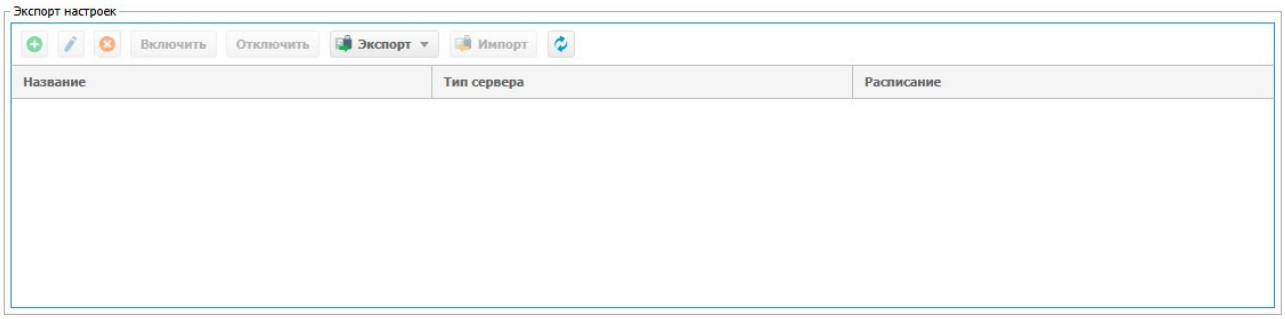

Рисунок 9 – Скриншот настроек

Возможные последствия: потеря возможности быстрого восстановления в случае аварии; риск потери конфигурации при аппаратных сбоях или инцидентах. Рекомендуется настроить периодический экспорт конфигурации на внешние серверы (FTP, SSH) по расписанию.

Четвертая проблема: не настроена проверка наличия установленных актуальных системных обновлений для используемых модулей (рисунок 10).

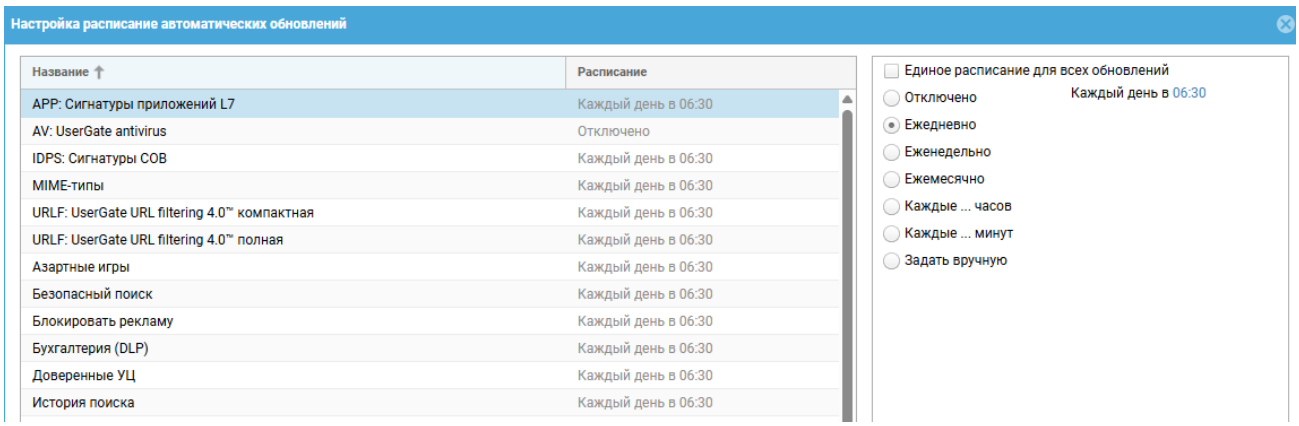

Рисунок 10 – Скриншот настроек

Также NGFW позволяет гранулированно настроить параметры защиты сети от сетевого флуда (для протоколов TCP (SYN-flood), UDP, ICMP). Грубая настройка производится в свойствах зон (раздел Настройка зон), а более точную настройку можно произвести в разделах «Правила защиты DoS» и «Профили DoS» (рисунок 11).

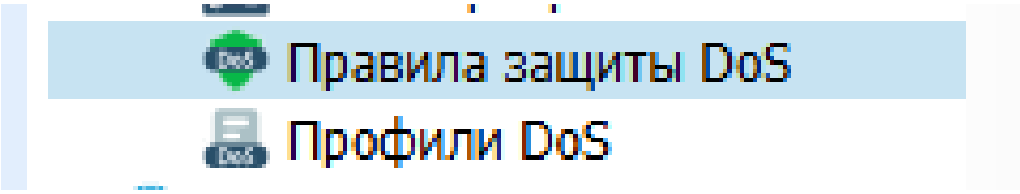

Рисунок 11 – Скриншот настроек

Рекомендуется производить настройку именно через гранулированные правила, чтобы исключить ложно положительные срабатывания для легитимного трафика.

3.2. Документация и сертификация

Эффективное функционирование системы информационной безопасности невозможно без наличия полного и актуального комплекта организационно-распорядительной, технической и эксплуатационной документации. В документации определяются ответственные лица, а также регламенты, к которым необходимо обращаться при эксплуатации систем. Также там описан порядок взаимодействий между подразделениями организации.

В рамках проектирования системы информационной безопасности регионального телекоммуникационного провайдера формируется комплект документации, охватывающий все этапы жизненного цикла системы: от

эксплуатации и администрирования до реагирования на инциденты информационной безопасности. Разработка документации осуществляется с учётом требований нормативных документов, а также сложившейся практики эксплуатации систем информационной безопасности у операторов связи.

Рассмотрим, что входит в пакет организационно-распорядительных документов:

1. Модель угроз описывает актуальные угрозы и типы нарушителей (приложение 1);
2. Положение «Политика безопасности предприятия» определяет цели, принципы и требования ИБ;
3. Положение о защите ПДн – локальный нормативный акт организации, регламентирующий порядок обработки, сбора, хранения и защиты личной информации сотрудников, клиентов и контрагентов (приложение 2);
4. Паспорт информационной системы – это сводное описание защищаемой системы;
5. Журналы учёта: средств защиты, периодического тестирования средств защиты (приложение 3), поэкземплярного учета СКЗИ (приложение 4), инцидентов;
6. Описание технологического процесса обработки конфиденциальной информации в автоматизированных системах (приложение 5);
7. Приказы о назначении группы реагирования на инциденты информационной безопасности (приложение 6);
8. Инструкция о порядке реагирования на инциденты информационной безопасности, а также на сбои и неисправности (приложение 7);
9. Инструкции по резервному копированию, реагированию, обновлению;
10. Политика управления доступом;
11. Программа по обучению персонала в области информационной безопасности.

Перечень основных документов, формируемых в рамках системы информационной безопасности, приведён в приложениях.

Использование средств защиты информации в проектируемой системе предполагает применение сертифицированных средств защиты информации в тех сегментах инфраструктуры, где осуществляется обработка критически важных данных и обеспечивается защита периметра и ядра сети. Сертификация средств защиты информации проводится в соответствии с требованиями ФСТЭК России и подтверждает соответствие заявленных функций безопасности установленным уровням доверия.

В абонентской и сервисной зоне допускается использование несертифицированных средств защиты информации при условии их применения в качестве вспомогательных механизмов и отсутствия требований по обязательной сертификации. В ядре сети, пограничной зоне и сети управления рекомендуется использовать исключительно сертифицированные средства защиты информации, обеспечивающие контроль доступа, фильтрацию сетевого трафика и защиту от несанкционированного воздействия.

Сформированный пакет документации и использование сертифицированных средств защиты информации обеспечивают формализацию процессов информационной безопасности, управляемость системы и соответствие проектируемой архитектуры требованиям нормативных документов и отраслевых стандартов. Наличие документированных процедур и подтверждённых характеристик безопасности является необходимым условием устойчивого функционирования системы информационной безопасности регионального телекоммуникационного провайдера.

3.3. Проведение заключительных работ

Завершающий этап практической реализации системы информационной безопасности регионального телекоммуникационного провайдера направлен на обеспечение устойчивого функционирования разработанной архитектуры, её интеграцию в операционную деятельность организации и формирование процессов, обеспечивающих поддержание заданного уровня защищённости на

протяжении всего жизненного цикла информационной системы. На данном этапе выполняется комплекс организационных и технических мероприятий, включающих обучение персонала, внедрение процедур реагирования на инциденты информационной безопасности, настройку процессов обновления и мониторинга, а также организацию постоянного контроля уязвимостей и конфигураций.

Одним из ключевых элементов заключительного этапа является обучение и подготовка персонала. Эффективность системы информационной безопасности в значительной степени определяется уровнем осведомлённости сотрудников и их способностью корректно выполнять установленные регламенты. В рамках внедрения системы информационной безопасности проводится дифференцированное обучение персонала с учётом выполняемых функций и уровня доступа. Для пользователей организуются обучающие мероприятия, направленные на формирование базовых навыков безопасной работы с информационными ресурсами, распознавания попыток социальной инженерии, фишинга и вредоносных воздействий. Для технических специалистов и администраторов проводится углублённое обучение, охватывающее вопросы эксплуатации средств защиты информации, реагирования на инциденты, анализа журналов событий и восстановления работоспособности систем. Результаты обучения фиксируются в установленном порядке и используются при последующей аттестации персонала.

Важным элементом заключительных работ является разработка и внедрение плана реагирования на инциденты информационной безопасности. План реагирования определяет порядок выявления, классификации, регистрации и устранения инцидентов, а также распределение ответственности между подразделениями и должностными лицами. В рамках данного плана устанавливаются процедуры первичного реагирования, изоляции затронутых сегментов, анализа причин инцидента и восстановления нормального режима функционирования информационной системы. Отдельное внимание уделяется регламенту взаимодействия между техническими подразделениями, службой

информационной безопасности и руководством организации, а также порядку документирования и анализа инцидентов с целью предотвращения их повторного возникновения.

Для обеспечения актуальности и устойчивости системы информационной безопасности в рамках заключительных работ настраиваются процессы управления обновлениями ПО и средств защиты информации. Также необходимо обязательно настроить средства NMS, которые будут помогать с учетом используемых компонентов. Необходимо также регулярно проводить мониторинг выявленных уязвимостей и выпуска обновлений. Применение обновлений осуществляется с учётом критичности компонентов и требований к доступности сервисов, что позволяет минимизировать риск нарушения работы информационной системы.

Существенное внимание уделяется организации процессов мониторинга и анализа событий информационной безопасности. В рамках проектируемой системы внедряется централизованный сбор и корреляция журналов событий от сетевого оборудования, серверов, рабочих станций и средств защиты информации. Настраиваются правила выявления аномальной активности, попыток несанкционированного доступа и иных признаков возможных инцидентов. Результаты мониторинга используются как для оперативного реагирования, так и для формирования аналитических отчётов, отражающих текущее состояние защищённости системы.

Важным элементом заключительного этапа является внедрение процессов управления уязвимостями. В рамках данного направления осуществляется регулярное сканирование информационной системы на наличие уязвимостей, анализ полученных результатов и классификация выявленных уязвимостей по степени критичности. Для уязвимостей с высоким уровнем риска разрабатываются и реализуются меры по их устранению или снижению, включая обновление программного обеспечения, изменение конфигураций или применение компенсирующих мер защиты. Процесс управления уязвимостями

носит непрерывный характер и интегрируется с процессами обновления и мониторинга.

Дополнительно в рамках заключительных работ организуется регулярный аудит конфигураций программных и аппаратных компонентов информационной системы. Аудит направлен на выявление отклонений от утверждённых эталонных конфигураций, ошибок настройки и несанкционированных изменений. Для критически важных элементов инфраструктуры предусматривается централизованное хранение и контроль конфигураций, а также периодическая проверка их целостности. Результаты аудита используются для корректировки настроек и повышения общей устойчивости системы информационной безопасности.

Для обеспечения управляемости и прозрачности процессов информационной безопасности в рамках заключительного этапа внедряется система управления информационной безопасностью. Система управления информационной безопасностью объединяет организационные и технические меры защиты, процедуры контроля и мониторинга, а также механизмы отчётности и анализа эффективности. В рамках системы управления устанавливаются показатели эффективности процессов информационной безопасности, формируются регулярные отчёты для руководства и обеспечивается возможность принятия обоснованных управленческих решений в области защиты информации.

В целом для периодической оценки можно сверяться с показателями, описанными далее.

К правилам для паролей относится: конкретная длина пароля (для пользователей – не меньше 10 символов; для администраторов – от 15 символов; для сервисных учётных записей — от 20 символов), смена парола не реже одного раза в полгода, отключение чек-бокса PNE (Password Never Expires) для всех пользователей, блокировка учетной записи после нескольких неудачных попыток ввода пароля, настроенные оповещения о блокировке учетной записи.

К правилам для учётных записей: на компьютерах у пользователей нет прав локальных администраторов, системные администраторы работают на компьютерах под обычными учётными записями , привилегированные учётные записи на МФУ отсутствуют, права администраторов подрядчикам выдаются только на время настройки и в ситуациях, когда они действительно необходимы, учетные записи администраторов разделены на три уровня ((AD Tiering) – рабочие станции/RDS серверы (T2), серверы приложений (T1), домен (T0)), и администраторы домена (T0) могут входить только на контроллеры домена, администраторы серверов приложений (T1) не могут входить контроллеры домена, администраторы рабочих станций (T2) не могут входить на контроллеры домена, серверы приложений и не имеют там привилегий.

Правила для защиты аутентификационных данных: учётные записи администраторов находятся в группе Protected Users, LAPS развернут на компьютерах и серверах [45], доступ для локальных учётных записей с административными правами по сети запрещён везде (и в домене, и на недоменных устройствах), отсутсвие SPN на учётных записях администраторов, не включенный на серверах T0 и T1 SSO, вспомогательным учётным записям запрещён интерактивный вход и RDP, на компьютерах включён Bitlocker, пароли на интерфейсах МФУ – не дефолтные и МФУ находятся в изолированном от пользователей VLAN, антивирус защищает оперативную память от дампа LSASS на серверах и компьютерах, общие пароли хранятся только в менеджере паролей.

Правила для протоколов аутентификации: LM и NTLMv1 отключены, любой исходящий с DC и Exchange NTLMv2 отключён, исходящий с исключениями на серверах и рабочих станциях NTLMv2 отключён, входящий NTLM отключён как минимум на центре сертификации, SMB Signing (серверный и клиентский) включён везде, LDAP Signing и Channel Binding включены на контроллерах домена, Extended Protection (EP) включён для Exchange и центра сертификации.

Правила для сетевых протоколов: SMBv1, LLMNR, mDNS, NetBios, WPAD PPTP отключены, IPv6 отключён на клиентских компьютерах.

Правила для сети: интерфейсы управления серверами недоступны из клиентских сетей, все сервисы, опубликованные наружу, находятся в закрытом VLAN, SMB наружу заблокирован, из VPN для пользователей доступны только нужные для работы ресурсы, Wi-Fi с доступом к корпоративным ресурсам работает только по EAP, на коммутаторах включены IPv6: ND inspection, RA Guard, DHCP Guard, First Hop Security, Source Guard, на коммутаторах включены DHCP Snooping и Dynamic ARP Inspection.

Правила для Active Directory: пользователи не могут добавлять устройства в домен, группа Pre-Windows 2000 Compatible Access пуста [38], Microsoft Exchange не входит в группу Administrators, Exchange развернут в режиме Split Permissions, Центр сертификации одобряет сертификаты только вручную (или вы в курсе, что такое ESC6, ESC8, ESC11 и настроили права на шаблоны), домен проверен PingCastle на базовые ошибки, домен проверен BloodHound на наличие путей эскалации привилегий до администратора домена, оповещения о создании новых учётных записей настроены.

Правила для 1С и базы данных: пароль на кластер 1С установлен, тестовые и временные базы также требуют пароль, 1С запущен не под локальным администратором, сервер баз данных недоступен из клиентской сети, подключение SQL-баз выполняются под выделенной учётной записью с ограниченными правами.

Правила для резервного копирования и виртуализации: система виртуализации не входит в домен, система резервного копирования не входит в домен, система хранения резервных копий не входит в домен, SMB signing включён, доступ для локальных учётных записей с административными правами по сети запрещён, вход в систему резервного копирования — через 2FA (если поддерживается), неиспользуемые службы отключены (Remote Registry, WinRM, Windows Script Host, Print Spooler)

Правила для мониторинга: система мониторинга обновляется регулярно, вход в консоль мониторинга возможен только по двухфакторной

аутентификации, выполнение произвольных скриптов на агентах запрещено, оповещения об отключении агентов на серверах настроены.

Правила обновлений и исправлений безопасности: серверы обновляются минимум раз в квартал, IPMI/iLO/iDRAC обновляются минимум раз в год, программное обеспечение на маршрутизаторах и коммутаторах обновляется минимум раз в год, клиентские ПК обновляются раз в квартал, прикладное ПО (Adobe Reader, 7zip и прочее) обновляется хотя бы раз в год, WSUS работает по https, контроллеры домена обновляются не через WSUS.

Правила для антивируса: антивирус установлен на всех компьютерах и серверах T1|T2, SRP/Applocker запрещают запуск скриптов из профиля пользователя, Powershell в профиле пользователя ограничен, VBA в Microsoft Office отключён, JavaScript в Adobe Reader отключён, настроены оповещения при обнаружении вируса.

Правила для защиты антивируса: пароль на отключение антивируса установлен, пароль на отключение агента антивируса установлен, центр управления антивирусом находится не в домене, вход на сервер управления по сети выполняется только под пользователем (доступ для локальных учётных записей с административными правами по сети запрещён), доступ к консоли управления антивирусом защищён двухфакторной аутентификацией (2FA), неиспользуемые службы отключены (Remote Registry, WinRM, Windows Script Host, Print Spooler), антивирус установлен на все серверы, публикующие ресурсы в интернет (включая недоменные и Linux-машины), также настроены оповещения мониторинга об отключении антивируса на Linux-серверах

Есть также рекомендуемая последовательность развития для систем информационной безопасности, предлагаемая лучшими практиками отрасли (рисунок 12).

Рисунок 12 – Последовательность развития

Проведение заключительных работ обеспечивает переход от проектирования системы информационной безопасности к её полноценной эксплуатации. Реализация комплекса мероприятий по обучению персонала, реагированию на инциденты, управлению обновлениями, мониторингу, контролю уязвимостей и конфигураций, а также внедрение системы управления информационной безопасностью позволяет обеспечить устойчивое и управляемое функционирование системы информационной безопасности регионального телекоммуникационного провайдера в условиях постоянно изменяющегося ландшафта угроз.

ЗАКЛЮЧЕНИЕ

Выпускная квалификационная работа посвящена разработке системы информационной безопасности для регионального телекоммуникационного провайдера с учётом актуальных угроз безопасности информации, требований нормативно-правовых документов и особенностей архитектуры сети оператора связи. Актуальность выбранной темы обусловлена высокой степенью зависимости современных телекоммуникационных компаний от устойчивости и защищённости информационных систем, а также постоянным ростом количества и сложности атак.

В ходе выполнения работы была достигнута поставленная цель – разработка системы информационной безопасности регионального телекоммуникационного провайдера, обеспечивающая снижение выявленных рисков до приемлемого уровня и соответствие требованиям действующих нормативных документов. Для достижения указанной цели в работе были последовательно решены все поставленные задачи.

В теоретической части работы была рассмотрена основная терминология, используемая в сфере информационной безопасности. Также были проанализированы актуальные угрозы, с которыми сталкиваются инфраструктуры. Была рассмотрена база по исследуемой теме с учетом нормативно-правовой документации, регламентов и методических документов. Особое внимание было уделено требованиям ФСТЭК России и особенностям их применения в телекоммуникационной отрасли. Проведённый анализ позволил сформировать теоретическую базу для последующего проектирования системы информационной безопасности и выбора адекватных мер защиты.

В аналитической части работы была исследована архитектура информационной системы регионального телекоммуникационного провайдера, выполнена идентификация защищаемых активов и уязвимостей, а также сформирован перечень актуальных угроз безопасности информации с использованием Банка данных угроз ФСТЭК России. На основании полученных данных проведена оценка рисков, позволившая определить наиболее уязвимые

зоны инфраструктуры и приоритетные направления защиты. Результаты анализа показали, что наибольшую опасность представляют угрозы, реализуемые в абонентской и сервисной зоне, а также в демилитаризованной зоне, в то время как компрометация ядра сети и сети управления характеризуется меньшей вероятностью, но критическими последствиями.

В практической части работы на основе результатов анализа и оценки рисков были разработаны предложения по доработке архитектуры информационной безопасности. Проектные решения направлены на устранение выявленных недостатков существующей архитектуры, усиление сегментации сети, внедрение дополнительных средств защиты и формирование многоуровневой системы обеспечения информационной безопасности. Особое внимание уделено защите критически важных компонентов инфраструктуры и сети управления, а также обеспечению устойчивости системы к комплексным и многоэтапным атакам.

В рамках практической реализации системы информационной безопасности были также разработаны организационные и эксплуатационные меры, включая формирование комплекта документации, определение требований к сертификации средств защиты информации и организацию заключительных работ. Были предложены мероприятия по обучению персонала, внедрению процессов реагирования на инциденты, управления обновлениями, мониторинга событий безопасности, контроля уязвимостей и регулярного аудита конфигураций. Дополнительно была сформирована система управления информационной безопасностью, обеспечивающая централизованный контроль, отчётность и непрерывное совершенствование процессов защиты информации.

Полученные в ходе выполнения выпускной квалификационной работы результаты подтверждают, что комплексный и зонально-ориентированный подход к построению системы информационной безопасности позволяет существенно повысить уровень защищённости информационной системы регионального телекоммуникационного провайдера без радикального изменения базовой сетевой архитектуры. Предложенные решения могут быть использованы

в практической деятельности операторов связи аналогичного масштаба, а также служить основой для дальнейших исследований и развития систем информационной безопасности с учётом появления новых угроз и технологий.

Таким образом, выпускная квалификационная работа является завершённым исследованием, в котором решена актуальная практическая задача, а полученные выводы и рекомендации имеют прикладную ценность и могут быть использованы при проектировании и эксплуатации систем информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Кодекс Российской Федерации об административных правонарушениях: Федеральный закон № 195-ФЗ: [Принят Государственной думой 20 декабря 2001 года]: (с изменениями и дополнениями). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный.

2. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон № 187-ФЗ: [Принят Государственной думой 12 июля 2017 года]: (с изменениями и дополнениями). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный

3. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ: [Принят Государственной думой 8 июля 2006 года]: (с изменениями и дополнениями). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный

4. О коммерческой тайне : Федеральный закон № 98-ФЗ: [Принят Государственной думой 9 июля 2004 года]: (с изменениями и дополнениями). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный

5. О персональных данных : Федеральный закон № 152-ФЗ: [Принят Государственной думой 8 июля 2006 года]: (с изменениями и дополнениями). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный

6. О связи : Федеральный закон № 126-ФЗ: [Принят Государственной думой 18 июня 2003 года]: (с изменениями и дополнениями). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный

7. О стратегическом планировании в Российской Федерации : Федеральный закон № 172-ФЗ: [Принят Государственной думой 20 июня 20014 года]: (с изменениями и дополнениями). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный

8. О Федеральной службе безопасности Российской Федерации : Федеральный закон № 40-ФЗ: [Принят Государственной думой 22 февраля 1995 года]: (с изменениями и дополнениями). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный

9. Уголовный кодекс Российской Федерации : Федеральный закон № 63-ФЗ: [Принят Государственной думой 24 мая 1996 года]: (с изменениями и дополнениями). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный

10. О Стратегии развития отрасли связи Российской Федерации на период до 2035 года : распоряжение Правительства Рос. Федерации от 24.11.2023 № 3339-р // Собрание законодательства Рос. Федерации. – 2023. – № 49. – Ст. 8839. – URL: https://www.consultant.ru/document/cons_doc_LAW_463486/ (дата обращения: 29.01.2026).

11. О лицензировании деятельности по технической защите конфиденциальной информации : постановление Правительства Рос. Федерации от 03.02.2012 № 79 // Собрание законодательства Рос. Федерации. – 2012.

12. О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций : постановление Правительства Рос. Федерации от 16.03.2009 № 228 // Собрание законодательства Рос. Федерации. – 2009.

13. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации : постановление Правительства Рос. Федерации от 08.02.2018 № 127 – Собрание законодательства Рос. Федерации. – 2018.

14. Об утверждении Правил централизованного управления сетью связи общего пользования : постановление Правительства Рос. Федерации от 27.10.2025 № 1667 // Собрание законодательства Рос. Федерации. – 2025.

15. Об утверждении Правил установки, эксплуатации и модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования сети Интернет : постановление Правительства Рос. Федерации от 12.02.2020 № 126 // Собрание законодательства Рос. Федерации. – 2020.

16. Об утверждении Правил установки, эксплуатации и модернизации технических средств противодействия угрозам устойчивости сети Интернет : постановление Правительства Рос. Федерации от 30.08.2025 № 1333 // Собрание законодательства Рос. Федерации. – 2025.

17. Об утверждении формы оценочного листа, применяемого ФСТЭК России при лицензировании деятельности по технической защите конфиденциальной информации : приказ ФСТЭК России от 28.12.2021 № 206 // Рос. газ. – 2022.

18. Об утверждении требований к защите информации в автоматизированных системах управления : приказ ФСТЭК России от 14.03.2014 № 31 // Рос. газ. – 2014.

19. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : приказ ФСТЭК России от 25.12.2017 № 239 // Собрание законодательства Рос. Федерации. – 2017.

20. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования : приказ ФСТЭК России от 21.12.2017 № 235 // Собрание законодательства Рос. Федерации. – 2017.

21. Об утверждении Инструкции об организации и обеспечении безопасности информации : приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 // Рос. газ. – 2001.

22. Об утверждении требований по защите сетей связи от несанкционированного доступа: приказ Министерства информационных технологий и связи Российской Федерации от 09.01.2008 № 1 // Рос. газ. – 2001.

23. Об утверждении состава и содержания мер по обеспечению безопасности персональных данных : приказ ФСБ России от 10.07.2014 № 378 // Рос. газ. – 2014. -

24. Требования по безопасности информации, устанавливающие уровни доверия к средствам защиты информации : утв. приказом ФСТЭК России от 02.06.2020 № 76 // Собрание законодательства Рос. Федерации. – 2020.

25. О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина : постановление Пленума Верховного Суда Российской Федерации от 25.12.2018 № 46 // Собрание законодательства Рос. Федерации. – 2020.

26. ГОСТ Р 51897–2021. Менеджмент риска. – М. : Стандартинформ, 2021.

27. ГОСТ Р 57149–2016 / ISO/IEC Guide 51:2014. Аспекты безопасности. Руководящие указания. – М. : Стандартинформ, 2016.

28. ГОСТ Р ИСО/МЭК 27002–2021. Методы и средства обеспечения безопасности информации. – М. : Стандартинформ, 2021.

29. ГОСТ Р ИСО/МЭК 27005–2010. Менеджмент риска информационной безопасности. – М. : Стандартинформ, 2010.

30. ГОСТ Р 56939–2024. Защита информации. Разработка безопасного программного обеспечения. Общие требования. – М. : Стандартинформ, 2024.

31. Методический документ. Методика оценки угроз безопасности информации : утв. ФСТЭК России 05.02.2021. – Доступ из справ.-правовой системы «КонсультантПлюс».

32. Ашманов, И. Цифровая гигиена / И. Ашманов, Н. Касперская; редактор Н. Гринчик. – Санкт-Петербург: Питер, 2024. – 400 с. – ISBN 978-5-4461-1938-7.

33. Вигерс, К. Разработка требований к программному обеспечению / К. Вигерс, Д. Битти. –3-е изд., доп. – Санкт-Петербург: БХВ-Санкт-Петербург, 2025. – 736 с. – ISBN 978-5-9909805-3-2.

34. Вяткина, А. Эволюция массовых атак и стратегия защиты / А. Вяткина. – Текст: электронный // Аналитические статьи Positive Technologies: интернет-портал. – 2025. – URL:

https://ptsecurity.com/research/analytics/evolution-of-mass-attacks-and-defense-strategy/#id1 (дата обращения: 12.12.2025)

35. Галатенко В.А. Стандарты информационной безопасности / В.А. Галатенко. - Москва: Национальный Открытый Университет ИНТУИТ, 2024. - 307 с. - ISBN 5-9556-0053-1. - URL: https://ibooks.ru/bookshelf/394542/reading (дата обращения: 9.01.2026). - Текст: электронный.

36. Гельбух, С. С. Сети ЭВМ и телекоммуникации. Архитектура и организация : учебное пособие / С. С. Гельбух. – Санкт-Петербург : Лань, 2022. – 208 с. – ISBN 978-5-8114-3474-9.

37. Защита АСУ ТП от APT-атак как часть стратегии киберустойчивости защиты. – Текст: электронный // Аналитические статьи Инфосистемы Джет: интернет-портал. – 2025. – URL: https://jetcsirt.su/analytics/zashchita-asu-tp-ot-apt-atak-kak-chast-strategii-kiberustoychivosti/?utm_source=outlook&utm_medium=press_release&utm_campaign=APCS&utm_term=smi (дата обращения: 12.12.2025)

38. Колисниченко, Д.Н. Самоучитель Microsoft Windows 11 / Д. Н. Колисниченко. – Санкт-Петербург : БХВ-Петербург, 2022. – 368 с. – ISBN 978-5-9775-6872-2.

39. Креопалов, В. В. Технические средства и методы защиты информации: учебное пособие / В.В. Креопалов. – Москва: ЕАОИ, 2024. – 278 с. – ISBN 978-5-374-00507-3. -

40. Ольков, Е. И. Архитектура защищенных сетей. Perimeter Layer: экспресс курс по основам ИБ / Е. И. Ольков – Москва: Лайдер Принт, 2023. – 186 с.

41. Ольков, Е. И. Архитектура защищенных сетей. Network Layer: экспресс курс по основам ИБ / Е. И. Ольков – Москва: Лайдер Принт, 2025. – 183 с.

42. Организационное и правовое обеспечение информационной безопасности: учебник для среднего профессионального образования / В. А. Ниесов, Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова; под редакцией Т. А.

Поляковой. — 2-е изд., перераб. и доп. – Москва: Юрайт, 2024. – 357 с. – URL: https://urait.ru/bcode/584372 (дата обращения: 25.11.2025) – ISBN 978-5-534-19107-3. – Текст: электронный.

43. Полтавцева, М. А. Безопасность баз данных : учебное пособие для вузов / М. А. Полтавцева. – Санкт-Петербург : Лань, 2024. – 356 с. – ISBN 978-5-507-49999-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/436274 (дата обращения: 5.01.2026). – Режим доступа: для авториз. пользователей.

44. Полтавцева, М.А. Организационные и правовые аспекты информационной безопасности: учебное пособие / М. А. Полтавцева – Санкт-Петербург : ПОЛИТЕХ-ПРЕСС, 2023. – 143 с. – ISBN 978-5-7422-8431-4.

45. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Н. Фимстер, Д. Уэзеролл. – 6-е изд.. – Санкт-ПетербургМоскваМинск: Питер, 2024. – 960 с. – ISBN 978-5-4461-1766-6.

ПРИЛОЖЕНИЕ

Приложение 1.

МОДЕЛЬ УГРОЗ

Безопасности информации
в информационной системе

ПРИНАДЛЕЖАЩЕЙ ПАО «Телеком»

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АВС	- антивирусные средства
АРМ	- автоматизированное рабочее место
АС	- автоматизированная система
АСЗИ	- автоматизированная система в защищенном исполнении
ГИС	- государственная информационная система
ИСПДн	- информационная система персональных данных
ЛВС	- локальная вычислительная сеть
МЭ	- межсетевой экран
ОС	- операционная система
ПДн	- персональные данные
ПМВ	- программно-математическое воздействие
ПО	- программное обеспечение
ПЭМИН	- побочные электромагнитные излучения и наводки
САЗ	- система анализа защищенности
СЗИ	- средства защиты информации
СЗПДн	- система (подсистема) защиты персональных данных
СКЗИ	- средства криптографической защиты информации
СОВ	- система обнаружения вторжений
ТС	- техническое средство
УБПДн	- угрозы безопасности персональных данных

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированная система в защищенном исполнении (АСЗИ) – автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и (или) иных нормативных документов по защите информации.

Адекватность – свойство соответствия преднамеренному поведению и результатам.

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Безопасность объекта – состояние защищенности объекта от внешних и внутренних угроз.

Безопасность информации – состояние защищённости информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации.

Блокирование информации – временное прекращение сбора, систематизации, накопления, использования, распространения, информации, в том числе её передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Встраивание криптосредства – процесс подключения криптосредства к техническим и программным средствам, совместно с которыми предполагается его штатное функционирование, за исключением процесса инсталляции.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Документированные (декларированные) возможности ПО (ТС) – функциональные возможности ПО (ТС), описанные в документации на ПО (ТС).

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Инсталляция – установка программного продукта на компьютер. Инсталляция обычно выполняется под управлением инсталлятора – программы, которая приводит состав и структуру устанавливаемого программного изделия в соответствии с конфигурацией компьютера, а также настраивает программные параметры согласно типу имеющейся операционной системы, классам решаемых задач и режимам работы. Таким образом, инсталляция делает программный продукт пригодным для использования в данной вычислительной системе и готовым решать определенный класс задач в определенном режиме работы.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационно-телекоммуникационная сеть общего пользования – информационно-телекоммуникационная сеть, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в

отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Канал атаки – среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона - это пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Криптографически опасная информация (КОИ) – информация о состояниях криптосредства, знание которой нарушителем позволит ему строить алгоритмы определения ключевой информации (или ее части) или алгоритмы бесключевого чтения.

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Модель угроз – перечень возможных угроз информации.

Нарушитель (субъект атаки) – лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Негативные функциональные возможности – документированные и недокументированных возможности программных и аппаратных компонентов криптосредства и среды функционирования криптосредства, позволяющие:

- модифицировать или искажать алгоритм работы криптосредств в процессе их использования;

- модифицировать или искажать информационные или управляющие потоки и процессы, связанные с функционированием криптосредства;

- получать доступ нарушителям к хранящимся в открытом виде ключевой, идентификационной и (или) аутентифицирующей информации, а также к защищаемой информации.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Опубликованные возможности ПО или ТС – возможности, сведения о которых содержатся в общедоступных открытых источниках (технические и любые другие материалы разработчика ПО или ТС, монографии, публикации в СМИ, материалы конференций и других форумов, информация из сети Internet и т.д.).

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Пользователь – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и(или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальная защита – комплекс организационных и технических мероприятий, обеспечивающих защиту информации от утечки по каналам побочных излучений и наводок.

Среда функционирования криптосредства (СФК) – совокупность технических и программных средств, совместно с которыми предполагается штатное функционирование криптосредства и которые способны повлиять на выполнение предъявляемых к криптосредству требований.

Средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

Средства кодирования - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

Средства криптографической защиты информации - средства шифрования, средства имитозащиты, средства кодирования, средства электронной цифровой подписи, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

Средства электронной подписи - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы – технические средства, осуществляющие обработку информации (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-

цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Угроза безопасности объекта – возможное нарушение характеристики безопасности объекта.

Угрозы безопасности информации – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при её обработке в информационной системе.

Уничтожение информации – действия, в результате которого невозможно восстановить содержание информации в информационной системе или в результате которых уничтожаются материальные носители информации.

Уровень криптографической защиты информации – совокупность требований, предъявляемых к криптосредству.

Успешная атака – атака, достигшая своей цели.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уполномоченное оператором лицо – лицо, которому на основании договора оператор поручает обработку персональных данных.

Учетность – свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.

Уязвимость - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Характеристика безопасности объекта – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами в области защиты информации и персональных данных:

[1] - Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

{ПДн} [2] - Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

{ПДн} [3] - Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119;

{ГИС} [4] - Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утверждены приказом ФСТЭК России № 17 от 11 февраля 2013 года);

{ПДн} [5] - Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом ФСТЭК России № 21 от 18 февраля 2013 года);

[6] - Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14 февраля 2008г. заместителем директора ФСТЭК России);

[7] - Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России);

[8] - Банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru);

{СКЗИ} [9] – Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утверждены руководством 8 Центра ФСБ России 31 марта 2015 года, № 149/7/2/6-432);

{СКЗИ} [10] – Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности (утверждены приказом ФСБ России от 10 июля 2014 года № 378).

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ разработан на основе нормативно-методических документов ФСТЭК России ([4]-[7]), регламентирующих порядок обеспечения безопасности ПДн.

Настоящая «Модель угроз» содержит систематизированный перечень угроз безопасности персональных данных и иной защищаемой информации при их обработке в информационной системе. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных и иной защищаемой информации, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз определяет актуальные угрозы для ИС.

Модель угроз содержит данные по угрозам безопасности персональных данных и иной защищаемой информации, обрабатываемых в ИС, связанным:

- с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ИС с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИС и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц оператора персональных данных, администраторов ИС, разработчиков ИС и их подсистем.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности ИС от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИС;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИС, в результате которого может быть нарушено их функционирование;
- контроль за обеспечением третьего уровня защищенности персональных данных и третьего класса защищенности ИС.

В Модели угроз дано обобщённое описание ИС как объекта защиты, возможных источников УБПДн, основных классов уязвимостей ИС, возможных видов неправомерных действий и деструктивных воздействий на ПДн, а также основных способов их реализации.

Угрозы безопасности ПДн, обрабатываемых в ИС, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИС. Внесение изменений в Модели угроз осуществляется также в случае внесения новых элементов в [7] и [8]. Кроме того, Модель угроз может быть пересмотрена по решению оператора ({Название организации}) на основе периодически проводимых анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений ИС, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в информационной системе.

ОПИСАНИЕ ИС

Общие сведения об информационной системе

Назначение ИС – автоматизация деятельности предоставления услуг «Интернет».

В ИС необходимо обеспечить конфиденциальность, целостность и доступность персональных данных.

В ИС обрабатываются специальные категории персональных данных более 10 000 субъектов.

Определение актуальности использования СКЗИ для обеспечения безопасности персональных данных

В ИС существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ. К таким угрозам относятся угрозы, связанные с передачей персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию.

Дополнительные объекты защиты

Согласно [9] для ИС к объектам защиты дополнительно относятся:

1) применяемые в ИС СКЗИ;
2) среда функционирования криптосредства (СФК);
3) информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
4) документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т. п., в которых отражена защищаемая информация, относящаяся к информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФК;
5) носители защищаемой информации, используемые в ИС в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;
6) используемые каналы (линии) связи;

7) помещения, в которых находятся ресурсы ИС, имеющие отношение к криптографической защите персональных данных.

Характеристики безопасности объектов угроз

В ИС необходимо обеспечить целостность, доступность и конфиденциальность защищаемой информации.

ПРИНЦИПЫ МОДЕЛИ УГРОЗ

В основе Модели угроз лежат следующие общие принципы:

1) Безопасность персональных данных и иной защищаемой информации при их обработке в информационных системах обеспечивается с помощью системы защиты информации в ИС.

2) При формировании модели угроз необходимо учитывать как угрозы, осуществление которых нарушает безопасность персональных данных и иной защищаемой информации (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

3) Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

4) Криптосредство штатно функционирует совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к криптосредству требований и которые образуют среду функционирования криптосредства (СФК).

5) Система защиты информации ИС (в том числе и СКЗИ) не предназначены для защиты информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (система защиты информации не предназначена для защиты информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

6) Нарушитель может действовать на различных этапах жизненного цикла криптосредства и СФК (под этими этапами в настоящем документе понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств криптосредства и СФК).

7) Криптографическая защита информации может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ.

8) СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ.

9) Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия.

10) СКЗИ являются как средством защиты информации, так и объектом защиты.

МОДЕЛЬ НАРУШИТЕЛЯ

В настоящем разделе определяется совокупность условий и факторов, создающих опасность нарушения характеристик безопасности возможных объектов угроз.

В данном разделе под угрозами будут пониматься атаки.

По признаку принадлежности к ИС все нарушители делятся на две группы:

Внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС;

Внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС.

Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИС, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ГИС ИС обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИС в соответствии с принятой политикой информационной безопасности.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах конкретные организационные меры, финансовые возможности и компетенцию нарушителей.

Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, не составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

средств перехвата в технических каналах утечки;

средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);

средств воздействия на источники и через цепи питания;

средств воздействия через цепи заземления;

средств активного воздействия на технические средства (средств облучения).

К внутренним нарушителям могут относиться:

администратор безопасности ИС (категория I);

администраторы конкретных подсистем или баз данных ИС(категория II);

пользователи ИС(категория III);

лица, обладающие возможностью доступа к системе передачи данных (категория V);

сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИС, но не имеющие права доступа к ним (категория VI);

обслуживающий персонал (водитель, уборщик помещений и т.п.) (категория VII);

уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС (категория VIII).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

На лиц категорий I-II возложены задачи по администрированию программно-аппаратных средств и баз данных ИС для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИС. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИС, а также к техническим и программным средствам ИС, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИС в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться

к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

К лицам категорий I-II ввиду их исключительной роли в ИС должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I-II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предположения об имеющейся у нарушителя информации об объектах реализации угроз.

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

общая информация – информации о назначении и общих характеристиках ИС;

эксплуатационная информация – информация, полученная из эксплуатационной документации;

чувствительная информация – информация, дополняющая эксплуатационную информацию об ИС (например, сведения из проектной документации ИС).

В частности, нарушитель может иметь:

данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИС;

сведения об информационных ресурсах ИС;

порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;

данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИС;

данные о реализованных в программных средствах защиты информации принципах и алгоритмах;

исходные тексты программного обеспечения ИС;

сведения о возможных каналах реализации угроз;

информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в автоматизированной информационной системе (АИС), к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об АИС, использующих эту систему

передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией о ИС и функционально ориентированных АС, включая информацию об уязвимостях технических и программных средств ИС. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИС в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными о ИС являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности, предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

Предположения об имеющихся у нарушителя средствах реализации угроз:

аппаратные компоненты средства защиты ПДн (СЗПДн);

доступные в свободной продаже технические средства и программное обеспечение;

специально разработанные технические средства и программное обеспечение.

Нарушители согласно банку данных угроз ФСТЭК России

Дополнительно в банке данных угроз ФСТЭК России определены три типа внешних и внутренних нарушителей – с низким потенциалом, со средним потенциалом и с высоким потенциалом.

Нарушители с низким потенциалом имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Также такие нарушители имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляют создание методов и средств реализации атак и реализацию атак на информационную систему.

Нарушители со средним потенциалом обладают всеми возможностями нарушителей с низким потенциалом. Имеют осведомленность о мерах защиты

информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы.

Нарушители с высоким потенциалом обладают всеми возможностями нарушителей с низким и средним потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений.

Для ИС определен нарушитель со средним потенциалом.

Обобщенные возможности источников атак

В соответствии с [9] выдвигаются предположения о наличии обобщенных возможностей у источников атак:

№ п/п	Описание возможности	Наличие возможности
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да

2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и СФК	Да
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и СФК	Да
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

Реализация угроз безопасности информации, определяемых по возможностям источников атак

Настоящий раздел сформирован в соответствии с [9], а также на основе данных нижеследующей таблицы делается вывод о необходимом классе СКЗИ для ИС в соответствии с [10].

В [9] и [10] в качестве мотивации в основном рассматриваются целенаправленные действия нарушителей, направленные на нарушение безопасности, защищаемой с помощью СКЗИ, информации или создание условий для этого (атаки). В то же время, в настоящей Модели угроз под нарушителем согласно разделу «Термины и определения» может пониматься как субъект атаки, так и физическое лицо, случайно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных. В любом случае, внешний нарушитель является субъектом атаки, случайно совершить действия по нарушению свойств

безопасности информации в ИС он не может, так как не имеет легальных прав доступа к элементам системы. В настоящей Модели угроз установлены возможности для сговора внутренних и внешних нарушителей. Сговоры, являющиеся комплексным нарушителем, объединяют в себе мотивации и возможности сговаривающихся потенциальных нарушителей. Комплексные нарушители являются субъектами атаки. Соответственно, наиболее опасным для ИС является комплексный нарушитель, совмещающий в себе целенаправленность атак на характеристики безопасности информации и возможности доступа к элементам ИС в пределах контролируемой зоны. Актуальность использования возможностей нарушителей для реализации атак определена в таблице.

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	Актуально	
1.2	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФК; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФК	Актуально	
1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФК	Актуально	

1.4	Использование штатных средств ИС, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально	
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ и СФК	Актуально	
2.2	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально	
3.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности. Доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФК, обеспечивается в соответствии с контрольно-пропускным режимом. Помещения, в которых располагаются СКЗИ и СФК, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода. Представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены

			компоненты СКЗИ и СФК, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации. Осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам. Осуществляется регистрация и учет действий пользователей. На АРМ и серверах, на которых установлены СКЗИ: - используются сертифицированные средства защиты информации от несанкционированного доступа; - используются сертифицированные средства антивирусной защиты. Дополнительно неактуальность возможности обоснована в разделе «Угрозы, связанные с недекларированными возможностями системного и прикладного программного обеспечения» настоящей Модели угроз
3.2	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности

3.2	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности
3.3	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности. Доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФК, обеспечивается в соответствии с контрольно-пропускным режимом. Помещения, в которых располагаются СКЗИ и СФК, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода.

			Представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФК, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации. Осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам. Осуществляется регистрация и учет действий пользователей. На АРМ и серверах, на которых установлены СКЗИ: - используются сертифицированные средства защиты информации от несанкционированного доступа; - используются сертифицированные средства антивирусной защиты. Дополнительно неактуальность возможности обоснована в разделе «Угрозы, связанные с недекларированными возможностями системного и прикладного программного обеспечения» настоящей Модели угроз

4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
4.3	Возможность воздействовать на любые компоненты СКЗИ и СФ	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности

В соответствии с изложенными выше предположениями о наличии возможностей у нарушителей на проведение атак и в соответствии с [10] (п. 12) в ИС должны применяться СКЗИ класса не ниже КС3.

ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящий раздел составлен в соответствии с [6], [7] и [8]. В разделе определяются актуальные угрозы безопасности персональных данных и иной защищаемой информации, не затрагивающие вопросы, связанные с применением в ИС» криптосредств.

Показатель исходной защищенности ИС

ИС имеет следующие технические и эксплуатационные характеристики:

а) Территориальное размещение ИС - локальная ИС, развернутая в пределах одного здания. Уровень защищенности - высокий.

б) Наличие соединения с сетями связи общего пользования – ИС, имеющая одноточечный выход в сеть общего пользования. Уровень защищенности - средний.

в) встроенные (легальные) операции с записями баз персональных данных – модификация, передача. Уровень защищенности - низкий.

г) разграничение доступа к персональным данным - ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн. Уровень защищенности - средний.

д) наличие соединений с другими базами персональных данных иных ИС, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИС. Уровень защищенности - высокий.

е) уровень обобщения (обезличивания) персональных данных - ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн). Уровень защищенности - низкий.

ж) объем персональных данных, которые предоставляются сторонним пользователям ИС без предварительной обработки – ИС, не предоставляющие никакой информации. Уровень защищенности - высокий.

Определение исходной степени защищенности:

№ п/п	Значение характеристики (уровень защищенности)	Количество значений	Процент значений не ниже данного уровня
1	Высокий	3	42%
2	Средний	2	71%
3	Низкий	2	-

В соответствии полученными данными устанавливается средний показатель исходной защищенности. Устанавливается значение коэффициента $Y_1=5$.

Определение последствий от нарушения свойств безопасности информации (опасность угроз)

С учетом обрабатываемых категорий персональных данных и прочих характеристик, ИС является информационной системой, для которой нарушение конфиденциальности информации, обрабатываемой в ней, может привести к негативным последствиям для субъектов персональных данных.

С учетом обрабатываемых категорий персональных данных и прочих характеристик, ИС является информационной системой, для которой нарушение целостности информации, обрабатываемой в ней, может привести к негативным последствиям для субъектов персональных данных.

С учетом обрабатываемых категорий персональных данных и прочих характеристик, ИС является информационной системой, для которой нарушение доступности информации, обрабатываемой в ней, может привести к негативным последствиям для субъектов персональных данных.

Согласно методике определения актуальных угроз, угроза имеет низкую опасность, если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных.

Согласно методике определения актуальных угроз, угроза имеет среднюю опасность, если реализация угрозы может привести к негативным последствиям для субъектов персональных данных.

Согласно методике определения актуальных угроз, угроза имеет высокую опасность, если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Согласно данным положениям для угроз частной модели, приводящих к нарушению конфиденциальности информации принимается средняя опасность.

Согласно данным положениям для угроз частной модели, приводящих к нарушению целостности информации принимается средняя опасность.

Согласно данным положениям для угроз частной модели, приводящих к нарушению доступности информации принимается средняя опасность.

Угрозы по банку данных угроз безопасности информации ФСТЭК России

В таблице приведены неприменимые к рассматриваемой ГИС «Название ИС» угрозы безопасности информации, приведено их условное обозначение в банке данных угроз ФСТЭК России, а также причины исключения данных угроз из списка рассматриваемых угроз.

№ п/п	Условные обозначения угроз, исключаемых из списка рассматриваемых угроз	Характеристика исключаемых угроз и причина исключения
1	УБИ.001, УБИ.002, УБИ.029, УБИ.038, УБИ.047, УБИ.050, УБИ.057, УБИ.060, УБИ.081, УБИ.082, УБИ.097, УБИ.105, УБИ.106, УБИ.110, УБИ.136, УБИ.146, УБИ.147, УБИ.148, УБИ.161	Из списка рассматриваемых угроз исключаются угрозы, связанные с системами распределенных вычислений (грид-системами), суперкомпьютерами и большими данными, поскольку такие технологии не применяются в рассматриваемой ИС

2		Из списка рассматриваемых угроз исключаются угрозы, связанные с системами виртуализации, поскольку такие технологии не применяются в рассматриваемой ИС
3		Из списка рассматриваемых угроз исключаются угрозы, связанные с использованием беспроводных сетей связи, поскольку такие технологии не применяются в рассматриваемой ИС
4		Из списка рассматриваемых угроз исключаются угрозы, связанные с использованием облачных сервисов и/или ресурсов, поскольку такие технологии не применяются в рассматриваемой ИС
5		Из списка угроз исключаются угрозы, связанные с уязвимостями Web-ресурсов, поскольку ИС не содержит веб-серверов, веб-сервисов и веб-ресурсов
6		Из списка рассматриваемых угроз исключаются угрозы, связанные с автоматическими системами управления технологическими процессами (АСУ ТП), поскольку ИС не является системой управления промышленными или иными технологическими мощностями
7		Из списка рассматриваемых угроз исключаются угрозы, связанные с использованием мобильных устройств, поскольку такие устройства не применяются в рассматриваемой ИС
8		Из списка рассматриваемых угроз исключаются оставшиеся угрозы, реализация которых возможна только нарушителем с высоким потенциалом

В следующей таблице приведены описания, условные обозначения, характеристики остальных угроз безопасности согласно банку данных угроз ФСТЭК России. В столбцах «Потенциал внутреннего нарушителя» и «Потенциал внешнего нарушителя» стоит «1», если потенциал высокий; «2»,

если потенциал средний; «3», если потенциал низкий; «-», если потенциал нарушителя не определен в банке данных угроз ФСТЭК России.

В столбце «Нарушаемые свойства безопасности информации» приняты следующие сокращения для свойств безопасности информации:

К – конфиденциальность;

Ц – целостность;

Д – доступность.

В столбце «Применимость» стоит знак «+», если данная угроза существует или может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Применимость» стоит знак «-», если данная угроза не существует и не может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации.

Списки актуальных угроз

Угрозы из банка данных угроз безопасности информации ФСТЭК России являются совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к защищаемой информации.

Из итогового списка исключаются угрозы, для которых в предыдущем разделе обоснована неприменимость.

Меры для нейтрализации угрозы считаются принятыми и достаточными, если они позволяют нейтрализовать все компоненты угрозы. Меры считаются принятыми, но недостаточными, если нейтрализуются не все компоненты угрозы. Меры считаются не принятыми, если они не позволяют нейтрализовать ни один компонент угрозы. Решение о наличии мер для нейтрализации каждой угрозы принимается на основе аудита ИС. В списке актуальных угроз указывается «+», если меры приняты; «+-», если меры приняты, но недостаточны; «-», если меры не приняты.

Существование предпосылок для угроз определяется экспертом с учетом особенностей архитектуры и функционирования ИС.

Вероятность угрозы определяется по таблице:

	Меры не приняты	Меры недостаточны	Меры достаточны
Есть предпосылки	Высокая вероятность (Y_2=10)	Средняя вероятность (Y_2=5)	Низкая вероятность (Y_2=2)

Коэффициент Y_1 – одинаков для всех угроз и определен в разделе «Показатель исходной защищенности.

Далее, для каждой угрозы в зависимости от вероятности и исходного уровня защищенности определяется возможность ее реализации – коэффициент $Y = (Y_1+Y_2)/20$.

В зависимости от значения Y, возможность реализации угроз может быть следующей:

$0 \le Y \le 0,3$ – возможность реализации угрозы низкая;

$0,3 < Y \le 0,6$ – возможность реализации угрозы средняя;

$0,6 < Y \le 0,8$ – возможность реализации угрозы высокая;

$Y > 0,8$ – возможность реализации угрозы очень высокая.

Опасность каждой угрозы зависит от нарушаемых свойств безопасности информации и установлена в разделе «Определение последствий от нарушения свойств безопасности информации (опасность угроз)».

Актуальность угроз определяется по возможности реализации и опасности угрозы исходя из таблицы:

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

№ п/п	Угроза	Меры приняты	Коэффициент вероятности	Коэффициент реализуемости угрозы	Возможность реализации	Опасность	Актуальность
1	УБИ.003	+	5	0,50	Средняя	Средняя	Да

Приложение 2.

ПОЛОЖЕНИЕ
О ЗАЩИТЕ И ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ПАО «Телеком»

ОБЩИЕ ПОЛОЖЕНИЯ

Назначение и область действия документа

Настоящее Положение об обработке персональных данных в ПАО «Телеком» (далее — Положение) определяет порядок сбора, хранения, передачи, использования, уничтожения и любых других видов обработки персональных данных субъектов персональных данных в ПАО «Телеком».

Настоящее Положение разработано в соответствии с федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — Закон), постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Трудовым кодексом РФ.

Цель данного Положения – определение порядка обработки персональных данных субъектов персональных данных в ПАО «Телеком» (далее — Организация).

Юридические и физические лица, в соответствии со своими полномочиями владеющие, получающие и использующие информацию о субъектах персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством Российской Федерации, ответственность за нарушение правил обработки и защиты этой информации.

Настоящее Положение вступает в силу с момента его утверждения {должность руководителя} Организации и действует бессрочно до замены его новым Положением.

Все изменения в Положение вносятся приказом {должность руководителя} Организации.

Все сотрудники Организации, имеющие доступ к персональным данным субъектов персональных данных, в обязательном порядке должны быть ознакомлены с настоящим Положением под роспись для последующего его исполнения.

ОСНОВНЫЕ ПОНЯТИЯ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Термины и определения

Автоматизированная обработка персональных данных - обработка персональных данных с использованием средств вычислительной техники.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Безопасность объекта – состояние защищенности объекта от внешних и внутренних угроз.

Безопасность информации – состояние защищённости информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации.

Блокирование информации – временное прекращение сбора, систематизации, накопления, использования, распространения, информации, в том числе её передачи.

Доступ к информации – возможность получения информации и ее использования.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона - это пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Модель угроз – перечень возможных угроз информации.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации,

помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Уничтожение информации – действия, в результате которого невозможно восстановить содержание информации в информационной системе или в результате которых уничтожаются материальные носители информации.

Уполномоченное оператором лицо – лицо, которому на основании договора оператор поручает обработку персональных данных.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Определение перечня персональных данных, обрабатываемых в ПАО «Телеком».

В Организации обрабатываются персональные данные следующих категорий субъектов персональных данных:

Персональные данные работников

Цели обработки персональных данных работников:

1) ведение кадрового учета в соответствии с Трудовым кодексом Российской Федерации;

2) начисление заработной платы и премиального вознаграждения;

3) организации системы доступа в помещения {Название организации};

4) подготовка регламентированной отчетности в государственные контрольные органы (ФНС, ПФР, ФСС и другие).

В ПАО «Телеком» как с помощью средств автоматизации, так и без использования таких средств обрабатываются следующие категории персональных данных сотрудников:

фамилия, имя, отчество; дата и место рождения; гражданство; семейное положение; состав семьи; паспортные данные; сведения об образовании; сведения о трудовом стаже; занимаемая должность; сведения о воинской обязанности; адрес регистрации и фактического места жительства; контактные телефоны; сведения о доходах; данные трудового договора; подлинники и копии приказов по личному составу; дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям; анкеты; результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей (без диагноза и других медицинских данных); фотография; индивидуальный номер налогоплательщика; номер страхового свидетельства обязательного пенсионного страхования; сведения об отпусках; сведения о социальных льготах и гарантиях; код карты доступа в помещения; номер карты доступа в помещения; уровень доступа в помещения; время действия карты доступа в помещения; дата выдачи карты доступа в помещения; тип карты доступа в помещения.

Персональные данные соискателей на вакантные должности

Цели обработки персональных данных соискателей:

1) трудоустройство на вакантные должности {Название организации}.

В ПАО «Телеком» как с помощью средств автоматизации, так и без использования таких средств обрабатываются следующие категории персональных данных соискателей:

фамилия, имя, отчество; дата рождения; место рождения; гражданство; пол; сведения о воинском учете; сведения об образовании; сведения о трудовом стаже; другие данные, указанные соискателем самостоятельно в резюме.

Персональные данные контрагентов

Цели обработки персональных данных контрагентов:

1) покупка ПАО «Телеком» техники или запасных частей у контрагента;

2) оказание контрагенту услуг по ремонту техники;

3) оказание контрагенту услуг по продаже техники.

В ПАО «Телеком» как с помощью средств автоматизации, так и без использования таких средств обрабатываются следующие категории персональных данных контрагентов:

фамилия, имя, отчество; ОКОПФ; паспортные данные; адрес регистрации; контактные данные; адрес электронной почты; данные о счетах и договорах; банковские реквизиты счета контрагента.

Принципы обработки персональных данных
Общие принципы обработки

Обработка персональных данных должна осуществляться на основе принципа соответствия объема и характера обрабатываемых персональных данных, а также способов обработки персональных данных заявленным целям обработки персональных данных.

Сбор, накопление, хранение, изменение, использование и распространение, а также другие действия, понимаемые под обработкой персональных данных, могут осуществляться только при условии письменного согласия физического лица, за исключением случаев, предусмотренных Законом.

Обработка персональных данных обрабатывается как с помощью средств автоматизации, так и без использования таких средств.

Правила обработки и защиты персональных данных без использования средств автоматизации установлены в соответствующем внутреннем документе ПАО «Телеком».

Правила обработки персональных данных в информационной системе персональных данных установлены в Инструкции администратора информационной безопасности и в Инструкции пользователя информационной системы персональных данных.

Порядок сбора и хранения персональных данных

При сборе персональных данных Организация обязана предоставить физическому лицу (субъекту персональных данных) по его запросу информацию о целях, способах обработки персональных данных, сведения о лицах, имеющих доступ к персональным данным, перечень обрабатываемых персональных данных и источник их получения, сведения о сроках обработки и хранения персональных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

Информация, представляемая работником при приеме на работу, должна иметь документальное оформление. При заключении трудового договора в

соответствии со статьей 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний -при поступлении на работу, требующую специальных знаний или специальной подготовки;
- дополнительные документы - в случаях предусмотренных федеральными законами, указами Президента РФ или постановлениями Правительства РФ.

В структурных подразделениях по управлению персоналом предприятия создаются, обрабатываются и хранятся следующие документы, содержащие персональные данные работников:

а) Карточка ф. Т-2, в которой отражаются следующие анкетные и биографические данные работника, которые относятся к персональным данным:

общие сведения (ФИО работника, дата рождения, место рождения, пол, гражданство, знание иностранного языка, образование, профессия, общий трудовой стаж, состояние в браке, паспортные данные, адрес места жительства, дата регистрации по месту жительства, номер телефона);

- сведения о воинском учете;
- данные о приеме на работу.

В дальнейшем в карточку ф. Т-2 вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных льготах и гарантиях.

б) Анкета, которая заполняется работником при приеме на работу (содержатся анкетные и биографические данные работника).

в) Трудовой договор (содержит сведения о должности работника, заработной плате, месте работы, рабочем месте, а также иные персональные данные работника).

г) Подлинники и копии приказов по личному составу и основания к ним (содержат информацию о приеме, переводе, увольнении и иных событиях, относящихся к трудовой деятельности работника).

д) Трудовая книжка или ее копия (содержит сведения о трудовом стаже, предыдущих местах работы).

е) Копии свидетельств о заключении брака, рождении детей (необходимы работодателю для предоставления работнику определенных льгот, предусмотренных трудовым и налоговым законодательством).

ж) Справка о доходах с предыдущего места работы (необходима работодателю для предоставления работнику определенных льгот и компенсаций в соответствии с налоговым законодательством).

з) Справка о сумме заработной платы, иных выплат и вознаграждений за 2 последние календарные года для начисления пособия по временной нетрудоспособности.

и) Копии документов об образовании (подтверждают квалификацию работника, обосновывают занятие определенной должности).

к) При необходимости иные документы (материалы служебных расследований, подлинники и копии отчетных, аналитических и справочных материалов), содержащие персональные данные работников.

Персональные данные соискателей на вакантные должности попадают в Организацию через специализированные веб-сайты (электронные биржи труда) или направляются соискателями непосредственно на электронную почту Организации. В случае приглашения соискателя на собеседование, данные в резюме могут подтверждаться документально. Копии подтверждающих документов могут храниться в Организации, но не дольше чем до достижения цели их обработки, то есть до замещения вакантной должности.

Персональные данные контрагентов поступают в Организацию при заключении договора, подтверждаются оригиналами документов и хранятся в течение исполнения договорных обязательств.

Процедура получения персональных данных работников

При заключении трудового договора работник обязан предоставить следующие документы, содержащие его персональные данные:

– действующий российский паспорт или иной документ, удостоверяющий личность;

– трудовую книжку;

– страховое свидетельство государственного пенсионного страхования;

– документы воинского учета (военный билет);

– документы об образовании;

– водительское удостоверение (в зависимости от должности);

– идентификационный номер налогоплательщика (при наличии).

Если трудовой договор с работником заключается впервые, трудовая книжка и страховое свидетельство государственного пенсионного страхования оформляются Организацией. В некоторых случаях, в зависимости от характера выполнения работы и конкретных должностных обязанностей, работник должен предоставить дополнительные документы, такие как:

– заграничный паспорт;

– медицинскую справку о стоянии здоровья;

– справку о доходах.

Этот список не ограничивается вышеперечисленными документами и может включать иные документы, содержащие персональные данные работника и необходимые Организации для выполнения ею своих обязательств как по отношению к работнику, так и к третьей стороне. В случае необходимости Организация вправе обратиться к работнику с просьбой о предоставлении документов, содержащих его персональные данные.

Все персональные данные работника следует получать непосредственно от него самого.

Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие на получение его персональных данных у третьей стороны. Организация должна сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

Работник при изменении персональных данных письменно уведомляет работодателя о таких изменениях в срок, не превышающий трех рабочих дней.

В соответствии со статьей 86 главы 14 Трудового кодекса Российской Федерации в целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника должны соблюдать следующие общие требования:

· обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

· при определении объема и содержания обрабатываемых персональных данных работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ и иными федеральными законами;

· защита персональных данных работника от неправомерного их использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном Трудовым кодексом РФ и Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;

· работники и их представители должны быть ознакомлены под роспись с документами предприятия, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

Передача персональных данных третьим лицам

Передача персональных данных третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных федеральным законом, не допускается. Данное ограничение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

Передача персональных данных субъекта в коммерческих целях без его письменного согласия исключается. Обработка персональных данных субъекта в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

Лица, получившие доступ к персональным данным субъекта, должны быть предупреждены о том, что эти данные могут быть использованы лишь в целях, для которых они переданы, и обязаны соблюдать это правило. Лица, получившие персональные данные, обязаны соблюдать режим конфиденциальности.

Передача или получение персональных данных осуществляются в соответствии с утвержденными Правилами рассмотрения запросов субъектов персональных данных или их представителей.

Персональные данные соискателей и контрагентов третьим лицам не передаются.

Персональные данные работников передаются в государственные контролирующие органы в соответствии с федеральными законами (ФНС, ФСС, ПФР и др.), а также в рамках зарплатного проекта в банк «БАНК». Передача персональных данных в финансовую организацию производится с информированного и осознанного согласия работника. В пункте Х.Х соглашения № ХХХХ от ДД.ММ.ГГГГ между ПАО «Телеком» и ЗАО «БАНК» предусмотрена обязанность третьего лица обеспечения конфиденциальности полученной от Организации информации, в том числе и персональных данных.

Трансграничная передача персональных данных

Трансграничная передача персональных данных Организацией не осуществляется.

Все технические средства обработки персональных данных (рабочие станции и сервера) находятся в пределах Российской Федерации (Ленинградская область).

Порядок уничтожения и блокирования персональных данных

Организация обязана прекратить обработку персональных данных и уничтожить их после достижения цели обработки или в случае отзыва субъектом персональных данных согласия на обработку, за исключением случаев, когда уничтожение противоречит федеральному законодательству, а также уведомить о своих действиях субъекта персональных данных и (или) уполномоченный орган. Во всех случаях предусмотрен срок уничтожения персональных данных – три рабочих дня.

В целях оперативной организации уничтожения персональных данных на бумажных носителях приказом {должность руководителя} Организации назначена комиссия по уничтожению персональных данных, а также утверждена форма акта уничтожения персональных данных.

Персональные данные, обрабатываемые в информационной системе персональных данных, удаляются путем стирания записи в базах данных администратором информационной безопасности Организации по запросу субъекта или при достижении целей обработки персональных данных.

Временное прекращение операций по обработке персональных данных (блокирование) должно возникать по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

Защита персональных данных

При обработке персональных данных Организация принимает организационные и технические меры для защиты персональных данных от неправомерных действий в соответствии с требованиями, устанавливаемыми Правительством РФ.

Защита персональных данных при неавтоматизированной их обработке регламентируется внутренним документом «Правила обработки персональных данных без использования средств автоматизации».

Защита персональных данных при их обработке в информационной системе персональных данных (далее - ИСПДн) регламентирована Инструкцией администратора безопасности ИСПДн, Инструкцией пользователя ИСПДн и другими внутренними документами Организации по защите информации.

Приказом {должность руководителя} Организации назначена группа реагирования на инциденты информационной безопасности.

В Организации разработана Модель угроз ИСПДн и Модель нарушителя. Проведена классификация ИСПДн. Для ИСПДн сформировано Техническое задание на систему защиты информации, в котором описаны все

организационные и технические меры, которые необходимо осуществить для нейтрализации актуальных угроз и выполнения требований действующего законодательства по защите персональных данных установленного уровня защищенности.

В Организации проведена внутренняя оценка эффективности принятых мер по защите персональных данных, подтвердившая в целом удовлетворительное состояние системы защиты персональных данных.

Согласие на обработку персональных данных

С соискателей согласия на обработку персональных данных берутся только в случае приглашения соискателя на собеседование в офис Организации.

Размещая свое резюме на электронных биржах труда или присылая резюме на электронную почту Организации, соискатель автоматически дает свое согласие на обработку его персональных данных.

С контрагентов согласия на обработку персональных данных не берутся, поскольку обработка их персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных. В соответствии с пп. 5, п. 1 статьи 6 Федерального закона № 152-ФЗ «О персональных данных» согласие на обработку персональных данных в таких случаях не требуется.

Со всех работников Организации собирается согласие на обработку их персональных данных. Несмотря на то, что обработка персональных данных производится в основном в соответствии с Трудовым Кодексом Российской Федерации, персональные данные работников в рамках зарплатного проекта передаются третьему лицу (ЗАО «БАНК»). В соответствии с п. 3 статьи 6 Федерального закона № 152-ФЗ «О персональных данных» такая передача персональных данных возможна только с согласия субъекта персональных данных.

ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

Организация доступа работников к персональным данным субъектов

Должностные лица Организации должны иметь доступ только к тем персональным данным, которые необходимы им для выполнения своих функциональных обязанностей.

В Организации разработана и утверждена разрешительная система допуска к персональным данным (Положение о разграничении прав доступа к персональным данным). Круг лиц, допущенных к обработке персональных данных, определяет руководство Организации на основании данных, представленных руководителями подразделений, в которых ведется обработка персональных данных. Данный Перечень утверждается {должность руководителя} Организации.

Должностные лица Организации допускаются к обработке персональных данных после ознакомления с настоящим Положением, инструкцией

пользователя ИСПДн а также с иной организационно-распорядительной документацией Организации по защите персональных данных.

Должностные лица Организации перед началом обработки персональных данных подписывают соглашение о неразглашении персональных данных.

Доступ должностных лиц к обработке персональных данных осуществляется в соответствии с Перечнем лиц, должностей, служб и процессов, допущенных к работе с персональными данными.

В случае обнаружения нарушений правил обработки персональных данных в Организации руководство Организации и/или администратор безопасности информации и/или ответственный за организацию обработки персональных данных обязаны приостановить предоставление персональных данных пользователям до выявления и устранения причин нарушений.

Работники Организации имеют право на свободный бесплатный доступ к своим персональным данным, а также на получение копий любой записи о своих персональных данных, обрабатываемых в Организации.

Лица, не имеющие доступа к персональным данным в соответствии с Перечнем подразделений и сотрудников, допущенных к работе с персональными данными, могут быть допущены к ним на основании приказа, подписанного {должность руководителя} Организации либо руководителем подразделения данного лица.

Организация доступа субъекту персональных данных к его персональным данным

Организация, обрабатывающая персональные данные, должна обеспечивать бесплатный доступ субъекта к персональным данным, ему соответствующим, за исключением случаев получения персональных данных в результате оперативно-розыскной деятельности, а также других случаев, предусмотренных федеральным законодательством.

Для получения доступа к своим персональным данным субъекту необходимо направить в Организацию запрос, содержащий паспортные данные субъекта персональных данных, в бумажной или электронной форме, подписанные собственноручно или квалифицированной электронной подписью.

Работники Организации должны предоставить персональные данные субъекту в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам.

В случае если персональные данные субъекта являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, Организация обязана удовлетворить требование субъекта по устранению нарушений обработки персональных данных.

С целью организации своевременной обработки запросов и обращений субъектов персональных данных в Организации разработан и утвержден

документ «Правила рассмотрения запросов субъектов персональных данных или их представителей».

Права и обязанности ПАО «Телеком»

Организация имеет право осуществлять обработку персональных данных в законных и обоснованных целях, в том числе предоставлять персональные данные третьим лицам, если на это дано информированное согласие субъекта персональных данных или если это предусмотрено действующим законодательством.

В случае выявления недостоверных персональных данных или неправомерных действий с ними Организации при обращении или по запросу субъекта персональных данных или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, Организация обязана устранить допущенные нарушения или, в случае невозможности устранения, уничтожить персональные данные, а также уведомить о своих действиях субъекта персональных данных или уполномоченный орган.

Должностные лица Организации, в обязанность которых входит обработка запросов и обращений субъектов персональных данных, обязаны обеспечить каждому субъекту возможность ознакомления с документами и материалами, содержащими их персональные данные, если иное не предусмотрено законом, в соответствии с Правилами рассмотрения запросов субъектов персональных данных.

В случае предоставления субъектом неполных, устаревших, недостоверных или незаконно полученных персональных данных Организация обязана внести необходимые изменения, уничтожить или блокировать их, а также уведомить о своих действиях субъекта персональных данных.

Организация обязуется не принимать на основании исключительно автоматизированной обработки решения, порождающие юридические последствия в отношении субъектов персональных данных или иным образом затрагивающие их права и законные интересы.

По запросу уполномоченного органа по защите прав субъектов персональных данных Организация обязана предоставить ему необходимую информацию.

ПРАВА И ОБЯЗАННОСТИ РАБОТНИКОВ ПАО «Телеком»

Общие положения

Работники, допущенные к обработке персональных данных, обязаны ознакомиться с документами Организации, которые устанавливают порядок обработки персональных данных в Организации, и подписать лист ознакомления с ними, а также подписать соглашение о неразглашении персональных данных, полученных в ходе исполнения своих должностных обязанностей.

Права работника

В целях защиты персональных данных, хранящихся в Организации, работник имеет право:

– требовать исключения или исправления неверных или неполных персональных данных;

– на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

– определять своих представителей для защиты своих персональных данных;

– на сохранение и защиту своей личной и семейной тайны;

– на обжалование в суде любых неправомерных действий или бездействия Организации при обработке и защите его персональных данных.

В целях защиты персональных данных, хранящихся в Организации, работник, осуществляющий обработку персональных данных, имеет право:

– получать и вводить информацию в соответствии с его полномочиями;

– требовать оповещения Организацией субъекта персональных данных обо всех произведенных в них исключениях, исправлениях или дополнениях.

Обязанности работника

В части своих персональных данных:

– передавать Организации достоверные документы, содержащие персональные данные, состав которых установлен Трудовым кодексом РФ;

– не предоставлять неверные персональные данные, а в случае изменений в персональных данных или обнаружения ошибок или неточностей в них (фамилия, место жительства и т.д.), незамедлительно сообщить об этом в Организацию.

В части обработки персональных данных субъекта:

– соблюдать режим конфиденциальности;

– не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;

– не сообщать персональные данные субъекта третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законом;

– разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

– не запрашивать дополнительную информацию, содержащую персональные данные, за исключением тех сведений, которые необходимы для достижения целей обработки персональных данных.

Права субъектов персональных данных

Получение сведений об Организации

Субъект персональных данных имеет право на получение сведений об Организации, о месте ее нахождения, о наличии у Организации персональных данных, относящихся к нему, а также на ознакомление с такими персональными данными. Субъект персональных данных вправе требовать от Организации уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Доступ к своим персональным данным

Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю Организацией при обращении либо при получении запроса субъекта персональных данных или его законного представителя.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных Организацией, а также цель такой обработки;

– способы обработки персональных данных, применяемые Организацией;

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Если субъект персональных данных считает, что Организация осуществляет обработку его персональных данных с нарушением требований федерального законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Организации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Ограничение прав субъектов персональных данных

Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

1) обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) предоставление персональных данных нарушает конституционные права и свободы других лиц.

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общие положения

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность за нарушение режима защиты, обработки и порядка использования этой информации.

Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъекта персональных данных, действующего на основании законодательства о персональных данных.

Персональная ответственность должностных лиц ПАО «Телеком»

Должностные лица Организации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность, предусмотренную федеральным законодательством.

Руководитель подразделения, разрешивший доступ должностному лицу к персональным данным несет персональную ответственность за данное решение.

Должностные лица Организации, получающие доступ к персональным данным несут персональную ответственность за обеспечение конфиденциальности предоставленной им информации. Кроме того, должностные лица Организации, получающие для работы документы, содержащие персональные данные, несут персональную ответственность за их сохранность.

В случае, когда нарушение конфиденциальности, целостности или доступности персональных данных повлекло за собой какие-либо финансовые потери для Организации, виновные должностные лица обязаны возместить причиненный ущерб.

Приложение 3.

ЖУРНАЛ
учета средств защиты информации в ИС

Начат « » _____ 20__ г.
Окончен « » _____ 20__ г.

Инструкция по ведению журнала

Записи в журнале делаются по мере установки и настройки средств защиты информации.

В графе «Название средства защиты информации» указывается наименование средства защиты информации.

В графе «Тип средства защиты информации» указывается тип средства защиты информации – программные или программно-аппаратный.

В графе «Зав. номер (номер знака соответствия)» указывается заводской номер и номер знака соответствия согласно формуляру на средство защиты (знак соответствия – голограмма ФСТЭК, которая вклеена либо в формуляр, либо наклеена на коробку диска дистрибутива средства защиты). Для средств защиты, сертифицированных ФСБ (например, ViPNet Client) вместо знака соответствия указывается регистрационный номер ФСБ.

В графе «Сертификат» указывается номер сертификата ФСТЭК России и/или ФСБ России и дата до которого он действует.

В графе «Место и дата установки» указывается номер АРМ согласно техпаспорту на систему (если он разработан), либо доменное имя АРМ (или виртуальной машины/сервера), а также дата установки (в ОС Windows можно узнать в меню «Панель задач» - «Программы и компоненты»).

В графе «Примечание» можно делать любые пометки, например об удалении данного экземпляра средства защиты.

№ п/п	Наименование средства защиты информации	Тип средства защиты информации	Зав. номер (номер знака соответствия)	Сертификат	Место и дата установки	Примечание

ЖУРНАЛ
периодического тестирования средств защиты информации в ИС

Начат « » _____ 20__ г.
Окончен « » _____ 20__ г.

Инструкция по ведению журнала

Записи в журнале делаются с периодичностью, установленной в разделе «Тестирование работоспособности средств защиты информации» утвержденного плана мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации.

В графе «Наименование средства защиты информации» указывается название тестируемого средства защиты, например «ViPNet Client»

В графе «Регистрационные номера средства защиты информации» указывается номер голограммы для средств защиты, сертифицированных ФСТЭК и регистрационные номера для средств защиты, сертифицированных ФСБ.

В графе «Дата тестирования» указывается дата проведения тестирования.

В графе «Фамилия и подпись ответственного пользователя, проводившего тестирование» указывается ФИО и подпись администратора безопасности и/или другого лица, проводившего тестирование.

В графе «Наименование теста, используемые средства для проведения теста» вносится краткое описание методики и инструментов тестирования, например, следующее: «Анализ сетевого трафика с помощью Wireshark».

В графе «Результат тестирования» коротко описывается полученные в результате тестов результат, например: «Успешный. Трафик на защищаемые узлы и ресурсы передается в зашифрованном виде».

В графе «Дата очередного тестирования» указывается предполагаемая дата очередного идентичного теста.

№ п/п	Наименование средства защиты информации	Регистрационные номера средства защиты информации	Дата тестирования	Фамилия и подпись ответственного пользователя, проводив	Наименование теста, используемые средства для	Результат тестирования	Дата очередного тестирования

				шего тестирование	проведения теста		

Приложение 4.

ЖУРНАЛ

поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов в ИС

Начат « » _____ 20____ г.
Окончен « » _____ 20____ г.

Инструкция по ведению журнала

Настоящий журнал разработан в соответствии с формой, утвержденной Приказом ФАПСИ от 13.07.2001 №152 (Приложение №2).

Настоящий журнал введен в действие в ПАО «Телеком», поскольку для защиты информации в ИС применяются криптографические средства защиты информации.

В графе «Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов» указывается наименование криптосредства, например «ViPNet Client 4», а также наименование имеющейся эксплуатационной и технической информации, например «Формуляр», «Руководство пользователя». Здесь же указываются названия ключевых документов. Под «ключевым документом» подразумевается физический носитель ключевой информации с записанной на него ключевой информацией, например электронный ключ eToken или RuToken, дискета, компакт-диск. В случае, если ключевая информация хранится на жестком диске, указывается серийный номер тома диска, который можно получить, выполнив команду dir в командной строке Windows.

В графе «Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов» указываются серийные номера СКЗИ, а также номера имеющейся документации при наличии. Серийные номера СКЗИ указаны на самих СКЗИ и/или в формулярах.

В графе «Номера экземпляров (криптографические номера) ключевых документов» указываются номера экземпляров ключевых документов. Как правило, ключевые документы издаются в единственном экземпляре.

В графе «От кого получены или ФИО ОКЗ, изготовившего ключевые документы» указывается название организации-распространителя криптографических средств (лицензиата ФСБ), например: «ООО «Информационный центр». В случае, если ключевые документы изготовлены органом криптографической защиты (ОКЗ) самостоятельно, указывается ФИО сотрудника, изготовившего ключевые документы.

В графе «Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении» указываются дата и номер сопроводительного письма, которое сопровождало передачу криптосредств. В случае, если ключевые документы изготовлены органом криптографической защиты (ОКЗ) самостоятельно, в этой графе сотрудник, изготовивший ключевые документы, ставит свою подпись.

В графе «ФИО пользователя криптосредств» указываются Фамилия Имя и Отчество (инициалы) сотрудника, использующего данный экземпляр криптосредства (ключевого документа).

В графе «Дата и расписка в получении» указывается дата получения криптосредства сотрудником и ставится его подпись.

В графе «ФИО сотрудника ОКЗ, установившего СКЗИ» указывается Фамилия и инициалы сотрудника ОКЗ, производившего установку (инсталляцию) криптографического средства.

В графе «Дата установки и подписи лиц» указывается дата установки (инсталяции) криптосредства и лица, производившие установку ставят свои подписи.

В графе «Номера ТС, в которые установлено СКЗИ» указываются серийные или инвентарные номера технических средств (компьютеров, моноблоков, ноутбуков и т. д.), на которые было установлено СКЗИ.

В графе «Дата уничтожения» указывается дата уничтожение ключевых носителей и/или ключевых документов.

В графе «ФИО сотрудника, уничтожившего (изъявшего) СКЗИ» ставится ссылка на акт уничтожения, в котором указаны ФИО председателя и членов комиссии по уничтожению.

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к	Серийные номера СКЗИ, эксплуатационной и технической документации	Номера экземпляров (криптографические номера) ключевых документ	Отметка о получении		Отметка о передаче		Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма или	Ф.И.О. пользователя	Дата расписка в	ФИО сотрудника	Дата установки	Номер ТС, в которо	Дата уничтожен	ФИО сотрудника	Номер акта об	

	ним, ключевых документов	нтации и ним, номера серий ключевых документов	нтов	и ФИО ОКЗ, изготовившего ключевые документы	дата изготовления ключевых документов и расписка в изготовлении	ателя криптосредств	учении	ОКЗ, установившего СКЗИ	ипод-писилиц	рыеустановленоСКЗИ	ия	, уничтожившего (изъявшего) СКЗИ	что-жении	

В графе «Номер акта об уничтожении» указывается номер и дата акта уничтожения СКЗИ.

Приложение 5.

Описание
технологического процесса обработки конфиденциальной
информации в автоматизированных системах

1. Описание объекта информатизации.

1.1. Общие сведения.

Автоматизированная система (АС) организации ПАО "Телеком", предназначенная для обработки, хранения и защиты конфиденциальной информации, включая персональные данные сотрудников, финансовую и техническую документацию.

1.2. Назначение и решаемые задачи.

АС предназначена для:

- Обработки финансовых данных (бухгалтерия, отчетность).
- Хранения и обработки персональных данных сотрудников.
- Управления документами (юридические договоры, технические задания).
- Обеспечения безопасности данных от несанкционированного доступа и утечек.

1.3. Состав программного обеспечения, участвующего в технологическом процессе обработки информации.

Операционные системы: Windows Server 2019, Windows 11 Pro.
СУБД: Microsoft SQL Server, PostgreSQL.
Антивирусное ПО: Kaspersky Endpoint Security.
Резервное копирование: Acronis Cyber Protect, Veeam Backup.
Межсетевые экраны (NGFW): Usergate NGFW.

1.4. Класс защищенности автоматизированной системы.

Класс защищенности “1Д”.

2. Организация работы с конфиденциальной информацией.

2.1. Доступ пользователя к работе на автоматизированной системе.

Доступ пользователей осуществляется через аутентификацию по логину и паролю. Доступ разграничивается на основе ролей (руководство, бухгалтерия, ИТ, сотрудники).

2.2. Настройка средств защиты информации от несанкционированного доступа для конкретных пользователей.

Политики разграничения доступа реализованы через NGFW и средства ОС.
Пользователям назначаются минимально необходимые права доступа.

2.3. Обработка информации, содержащей конфиденциальные сведения.

Обработка конфиденциальной информации производится только на аттестованных рабочих станциях и серверах с использованием СЗИ.

2.4. Хранение документов конфиденциального характера.
Электронные документы хранятся на защищенных серверах с доступом по ролям. Физические документы хранятся в сейфах и архивных помещениях с ограниченным доступом.

2.5. Хранение съемных носителей.
Съемные носители хранятся в защищенных сейфах с обязательной регистрацией в журнале учета.

2.6. Печать, сканирование и копирование с бумажных носителей.
Печать и копирование документов осуществляется на защищенных принтерах, доступ к которым ограничен. Устройства сканирования расположены в контролируемой зоне.

2.7. Удаление электронных документов, содержащих конфиденциальную информацию, со съемных носителей и жестких дисков.
Удаление осуществляется с использованием средств безопасного удаления данных, соответствующих требованиям ФСТЭК и РД.

2.8. Уничтожение съемных носителей.
Физическое уничтожение съемных носителей производится с использованием шредеров или сертифицированных методов утилизации.

3. Описание технологического процесса обеспечения информационной безопасности.

3.1. Защита от несанкционированного доступа.
Разграничение доступа с использованием NGFW и средств ОС.
Аутентификация пользователей по паролям и логинам.

3.2. Антивирусная защита.
Антивирусная защита реализована с помощью Kaspersky Endpoint Security на всех серверах и рабочих станциях.
Регулярное обновление антивирусных баз и выполнение сканирований.

3.3. Обеспечение целостности и доступности информации.
Резервное копирование данных с использованием Acronis и Veeam на сетевое хранилище NAS (NetApp).

Перечень защищаемых в автоматизированной системе ресурсов

N п/п	Наименование защищаемого ресурса	Примечание

1	2	3
1	Финансовая информация	Данные о платежах, счетах, финансовой отчетности, бухгалтерские документы, акты выполненных работ.
2	Персональные данные	ФИО, паспортные данные, контактная информация сотрудников и клиентов, сведения о зарплате.
3	Юридическая документация	Договоры с клиентами и партнёрами, приказы, распоряжения руководства, внутренние регламенты.
4	Техническая информация	Технические задания, спецификации, акты по выполнению работ, отчеты о настройке оборудования.
5	Коммерческая информация	Данные о клиентах, условиях сделок, предложениях, бизнес-планах и стратегиях компании.

Приложение 6.

ПРИКАЗ

«___» _____ 20__ г. №_____

О назначении группы реагирования на инциденты информационной безопасности и о правилах регистрации инцидентов информационной безопасности и реагирования на них в ИС

В целях исполнения требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных Приказом ФСТЭК России № 17 от 11.02.2013 в части регистрации событий безопасности

ПРИКАЗЫВАЮ:

1. Назначить внутреннюю группу по реагированию на инциденты информационной безопасности (далее – ГРИИБ) в составе:
   - ФИО, должность;
   - ФИО, должность;
2. Утвердить прилагаемую, разработанную в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», инструкцию по реагированию на инциденты информационной безопасности.
3. ГРИИБ в своей работе руководствоваться инструкцией по реагированию на инциденты информационной безопасности, руководящими документами ФСТЭК России и ФСБ России, государственными стандартами в области информационной безопасности и общедоступными источниками об угрозах и уязвимостях информационных систем.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель ПАО «Телеком» _____ {И. О. Фамилия}

Приложение 7.
Инструкция по реагированию на инциденты информационной безопасности в ИС ПАО «Телеком»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политики информационной безопасности и меры по защите информации в ГИС не могут полностью гарантировать защиту информации, информационных систем, сервисов или сетей. Всегда существует вероятность, что после внедрения системы защиты информации останутся слабые места, которые могут сделать обеспечение информационной безопасности неэффективным, и, следовательно, инциденты информационной безопасности – возможными. Инциденты информационной безопасности могут оказывать прямое или косвенное негативное воздействие на деятельность ПАО «Телеком». Также неизбежно выявление новых, ранее не идентифицированных угроз безопасности информации. Исходя из вышесказанного, важно применять структурный подход к:

- обнаружению, оповещению об инцидентах безопасности и их оценке;
- реагированию на инциденты информационной безопасности, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и (или) восстановления после наступления негативных последствий вследствие инцидента безопасности информации;
- извлечению уроков из инцидентов информационной безопасности, совершенствованию системы защиты информации, введению превентивных защитных мер и улучшению общего подхода к менеджменту инцидентов информационной безопасности.

1.2. Регистрация событий безопасности, выявление инцидентов безопасности информации и реагирование на них производится, в том числе, с целью выполнения требований Приказа ФСТЭК № 17 от 11.02.2013 с индексами: РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.5, РСБ.6, РСБ.7.

1.3. Для реагирования на инциденты информационной безопасности создается группа реагирования на инциденты информационной безопасности (далее – ГРИИБ).

1.4. Важным членом ГРИИБ является Администратор безопасности информации (далее – Администратор), назначаемый приказом руководителя ПАО «Телеком». Он осуществляет централизованный мониторинг событий безопасности в соответствии с Инструкцией администратору безопасности.

1.5. Инцидентом информационной безопасности (далее - инцидент ИБ) является событие, нарушающее одно из свойств защищаемой информации (целостность, доступность или конфиденциальность) или несколько таких свойств одновременно.

2. РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ В ИС

2.1. Событиями безопасности, подлежащими регистрации, являются записи в журналах операционных систем, прикладного программного обеспечения и средств защиты информации (электронные журналы сообщений).

2.2. Информация о событиях безопасности информации является защищаемой информацией и к ней применяются те же, утвержденные правила и политики по защите информации, что и к другой защищаемой конфиденциальной информации в ПАО «Телеком».

2.3. Далеко не все события безопасности информации являются инцидентами безопасности информации. Инцидентами безопасности являются только запрещенные в ГИС действия, с которыми может быть связано создание угрозы информационной безопасности.

2.4. Информация о событиях безопасности также может поступать Администратору безопасности от сотрудников ПАО «Телеком», заметивших аномальную активность в информационной системе. Информацией о событиях безопасности также являются сведения о потере, краже или компрометации машинных и других носителей информации.

2.5. Администратор анализирует электронные журналы сообщений и принимает решение, является ли событие безопасности инцидентом информационной безопасности.

2.6. По степени возможного ущерба информационной системе инциденты информационной безопасности можно условно разделить на незначительные и значительные.

2.7. Незначительными признаются инциденты информационной безопасности, соответствующие одному или нескольким критериям:

· инцидент был быстро обнаружен и локализован, значительных последствий в результате инцидента не произошло;

· инцидент затронул небольшое количество сотрудников;

· инцидент не требует существенных усилий и затрат на восстановление работоспособности информационной системы или ее частей;

· в результате инцидента не была нарушена конфиденциальность, целостность и доступность больших массивов защищаемой информации (например, всей базы данных), нарушена безопасность только небольшого фрагмента информации (одной или нескольких записей базы данных);

· инцидент не требует концептуального пересмотра политик информационной безопасности;

· в результате инцидента организации нанесен минимальный ущерб или не нанесено никакого ущерба;

· инцидент не вызвал долгосрочного простоя информационной системы и не нарушил бизнес-процессы и технологические процессы обработки информации.

2.8. Значительными признаются все инциденты информационной безопасности, которые не могут быть признаны незначительным в соответствии с пунктом 2.7 данной Инструкции.

3. РЕАГИРОВАНИЕ НА ИНЦИДЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УСТРАНЕНИЕ ПОСЛЕДСТВИЙ И ПРИЧИН ИНЦИДЕНТА

3.1. В случае обнаружения незначительных инцидентов, Администратор самостоятельно принимает меры по устранению последствий инцидента информационной безопасности.

3.2. В случае обнаружения значительных инцидентов, Администратор созывает ГРИИБ, которая оценивает инцидент и реагирует на него наиболее целесообразным и результативным способом.

3.3. После устранения последствий инцидента, ГРИИБ делаются соответствующие выводы (оформляемые в виде акта) и вносятся предложения по совершенствованию технических и организационных аспектов защиты информации в ИС с целью предотвращения подобных инцидентов в будущем.

3.4. Процесс реагирования на инцидент информационной безопасности и восстановление ущерба, нанесенного ИС, может состоять из следующих этапов:

- обнаружение и оповещение о возникновении событий ИБ (человеком или автоматическими средствами);
- сбор информации, связанной с событиями информационной безопасности и оценка этой информации с целью определения, какие события можно отнести к категории инцидентов ИБ;
- незамедлительное реагирование на инцидент ИБ;
- локализация АРМ или сегмента сети, на который распространились негативные последствия инцидента;
- при необходимости - привлечение специалистов сторонних организаций для получения качественных консультаций;
- выполнение мер по нейтрализации факторов, вызвавших инцидент ИБ;
- восстановление ущерба, вызванного инцидентом ИБ;
- регистрация всех действий и решений для последующего анализа;
- правовая оценка инцидента ИБ;
- при необходимости и при наличии правовых оснований, обращение в правоохранительные органы;
- принятия мер для предотвращения подобных инцидентов в будущем.

4. РАССЛЕДОВАНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Расследование инцидента информационной безопасности проводится с целью выявления и наказания лиц, виновных в инциденте, а также с целью выявления недоработок в политиках информационной безопасности и их оперативного устранения.

4.2. Расследование инцидента проводится Администратором безопасности самостоятельно (в случае незначительного инцидента) либо

ГРИИБ (в случае значительного инцидента). В случаях, когда виновником инцидента является внешний нарушитель, к расследованию инцидента могут привлекаться сотрудники правоохранительных органов в установленном порядке.

4.3. Расследование инцидента проводится в следующем порядке:

· проводится сбор информации об инциденте из всех возможных источников, проводится анализ собранной информации, формируется доказательная база;

· анализируются каналы атаки, уязвимости и другие факторы, которые сделали возможным появление инцидента информационной безопасности;

· анализируются сценарии действий нарушителя, в случае антропогенной природы инцидента;

· составляется список подозреваемых в инциденте лиц, в случае антропогенной природы инцидента;

· выявляются лица, виновные в инциденте информационной безопасности, в случае антропогенной природы инцидента;

· определяется степень ущерба, нанесенная информационной системе, организации, субъектам персональных данных в результате инцидента информационной безопасности;

· составляется отчет о расследовании.

4.4. В случаях, если инцидент произошел по вине сотрудников, руководство принимает решение о мерах, которые будут применены к виновному лицу.

4.5. В случаях, если инцидент произошел по вине контрагента или сотрудника сторонней организации, осуществляющей какие-либо работы, виновный в инциденте несет ответственность в соответствии с положениями договора между ПАО «Телеком» и контрагентом/сторонней организацией.

4.6. В случаях, если инцидент произошел по вине внешнего нарушителя, виновный несет ответственность в соответствии с уголовным и административным кодексами Российской Федерации.

4.7. После выявления и наказания виновных в инциденте, Администратором безопасности после согласования с руководством ПАО «Телеком» могут быть проведены занятия с сотрудниками по разбору произошедшего инцидента с целью предотвращения повторения инцидента в будущем.

4.8. Из каждого инцидента информационной безопасности извлекаются уроки, делаются выводы о необходимости изменения и улучшения организационных и технических частей системы защиты информации в ПАО «Телеком». Изменения в системе защиты информации, призванные предотвратить появление выявленного и расследованного инцидента информационной безопасности, должны быть осуществлены в кратчайшие сроки.

5. КЛАССИФИКАЦИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Инциденты ИБ по происхождению делятся на преднамеренные и случайные. Случайные инциденты могут быть вызваны антропогенными факторами (ошибка сотрудника, техническая неграмотность), социальными явлениями, природными явлениями, техногенными факторами (аварии, катастрофы).

5.2. Инциденты ИБ также можно разделить на инциденты, вызванные техническими средствами, и инциденты, вызванные нетехническими средствами.

5.3. В целом все инциденты безопасности можно разделить на следующие категории:

· {перечислить}

5.4. Одним из широко распространенных видов инцидентов ИБ является инцидент типа «Отказ в обслуживании». Результатом такого инцидента является неспособность систем, сервисов или сетей продолжать функционирование с прежней производительностью. Часто это сопровождается полным отказом в доступе авторизованным пользователям. Инциденты типа «отказ в обслуживании» могут быть вызваны как техническими, так и нетехническими средствами. Инциденты типа «отказ в обслуживании», вызываемые техническими средствами можно категорировать на инциденты, направленные на уничтожение ресурсов, и на инциденты, направленные на истощение ресурсов. Типовыми примерами таких преднамеренных технических инцидентов ИБ являются:

· зондирование сетевых широковещательных адресов с целью полного заполнения полосы пропускания сети трафиком ответных сообщений;

· передача данных в непредусмотренном формате в систему, сервис или сеть в попытке разрушить или нарушить их нормальную работу;

· одновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью в попытке исчерпать их ресурсы.

Инциденты ИБ типа «Отказ в обслуживании», создаваемые нетехническими средствами и приводящие к утрате информации, сервиса и (или) устройств обработки информации, могут вызываться, например, следующими факторами:

· нарушения систем физической защиты, приводящие к хищениям, преднамеренному нанесению ущерба или разрушению оборудования;

· случайное нанесение ущерба техническим средствам ГИС и или месту их расположения от огня или воды;

· экстремальные условия окружающей среды, например высокая температура воздуха, вызванная выходом из строя системы кондиционирования воздуха;

· неправильной функционирование или перегрузка системы;

· неконтролируемые изменения в системе;

· неправильное функционирование программного и аппаратного обеспечения.

5.5. Инциденты ИБ типа «Сбор информации» подразумевают действия, связанные с определением потенциальных целей атаки и получением представления о сервисах, работающих на идентифицированных целях атаки. Подобные инциденты ИБ предполагают проведение разведки с целью определения:

· наличия цели, получения представления об окружающей ее сетевой топологии;

· потенциальных уязвимостей цели или непосредственно окружающей ее сетевой среды, которые можно использовать для атаки.

Типичными примерами атак, направленных на сбор информации техническими средствами, являются:

· сбрасывание записей DNS;

· отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы;

· зондирование системы с целью идентификации операционной системы хоста;

· сканирование доступных сетевых портов на протокол передачи файлов системе с целью идентификации соответствующих сервисов и версий программного обеспечения этих сервисов;

· сканирование одного или нескольких сервисов с известными уязвимостями по диапазону сетевых адресов.

Инциденты, направленные на сбор информации, создаваемые нетехническими средствами, приводят к:

· прямому или косвенному раскрытию или модификации информации;

· хищению интеллектуальной собственности;

· нарушению учетности, например, при регистрации учетных записей;

· неправильному использованию информационных систем (например, с нарушением закона или политики организации);

Инциденты могут вызываться, например, следующими факторами:

· нарушениями физической защиты, приводящими к несанкционированному доступу к информации и хищению устройств хранения данных, содержащих значимые данные, например ключи шифрования;

· неудачно и (или) неправильно сконфигурированными операционными системами по причине неконтролируемых изменений в системе или неправильным функционированием программного или аппаратного обеспечения, приводящим к тому, что персонал организации или посторонний персонал получает доступ к информации, не имея на это разрешения.

5.6. Несанкционированный доступ как тип инцидента включает в себя инциденты, не вошедшие в первые два типа. Главным образом этот тип инцидентов состоит из несанкционированных попыток доступа в систему или неправильного использования системы, сервиса или сети. Некоторые примеры

несанкционированного доступа с помощью технических средств включают в себя:

- попытки извлечь файлы с паролями;
- атаки переполнения буфера с целью получения привилегированного доступа к сети;
- использование уязвимостей протокола для перехвата соединения или ложного направления легитимных сетевых соединений;
- попытки расширить привилегии доступа к ресурсам или информации по сравнению с легитимно имеющимися у пользователя.

5.7. Более подробное описание угроз безопасности ГИС, а, следовательно, и возможности для возникновения инцидентов ИБ приведено в документе «Модель угроз безопасности информации в ГИС».