СОГЛАСОВАНО

Генеральный директор

ЗАО «Искрауралтел»

Давыдов В.В

«__» _____2012 год

ТЕХНИЧЕСКИЙ ПРОЕКТ

Система обеспечения вызова экстренных оперативных служб по единому номеру «112» в Свердловской области

ПОДСИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПАМР.460018.006.ТП.П2.1

Екатеринбург

2012

Доп. инв. №

Подпись и дата

Инв. № подл.

СОДЕРЖАНИЕ

Введение

В настоящем документе приведены решения по реализации функций подсистемы обеспечения информационной безопасности «Системы обеспечения вызова экстренных оперативных служб через единый номер «112» на базе единых дежурно-диспетчерских служб муниципальных образований». Документ содержит следующие разделы:

1.общие положения;

2.правовая основа обеспечения информационной безопасности «Системы-112»;

3.инвентаризация (учет) и категорирование (классификация);

4.описание объекта защиты;

5.модель угроз и нарушителя;

6.реализация требований к подсистеме обеспечения информационной безопасности.

1 Общие положения

1.1 Наименование и условное обозначение

Полное наименование – «Разработка технического проекта системы обеспечения вызова экстренных оперативных служб через единый номер «112» на базе единых дежурно-диспетчерских служб муниципальных образований Свердловской области»

Условное обозначение – Система-112

Код проекта - ПАМР.460018.006

Основанием для проведения работ по организации проектирования является:

- Договор XXXXXXXXXX

1.2 Заказчик и исполнитель работ

Заказчиком системы является: ООО «НТЦ Протей» г. Санкт-Петербург.

Исполнитель: ЗАО «ИскраУралТел» г. Екатеринбург.

1.3 Сроки выполнения работ

Начало работ по созданию проекта – с момента подписания контракта

Плановый срок завершения работ – 23.12.2012

1.4 Цели, назначения системы

Система-112 предназначена для обеспечения оказания экстренной помощи населению при угрозах для жизни и здоровья, уменьшения социально-экономического ущерба при чрезвычайных происшествиях и чрезвычайных ситуациях, а также для информационного обеспечения единых дежурно-диспетчерских служб муниципальных образований (далее - единые дежурно-диспетчерские службы или ЕДДС).

Система-112 предназначена для решения следующих задач:

- прием по номеру «112» вызовов (сообщений о происшествиях);
- получение от оператора связи сведений о местонахождении лица, обратившегося по номеру «112» и (или) абонентского устройства, с

которого был осуществлен вызов (сообщение о происшествии), а также иных данных, необходимых для обеспечения реагирования по вызову (сообщению о происшествии);

- анализ поступающей информации о происшествиях;
- направление информации о происшествиях, в том числе вызовов (сообщений о происшествиях), в дежурно-диспетчерские службы экстренных оперативных служб в соответствии с их компетенцией для организации экстренного реагирования;
- обеспечение дистанционной психологической поддержки лицу, обратившемуся по номеру «112»;
- автоматическое восстановление соединения с пользовательским (оконечным) оборудованием лица, обратившегося по номеру «112», в случае внезапного прерывания соединения;
- регистрация и документирование всех входящих и исходящих вызовов (сообщений о происшествиях) по номеру «112»;
- ведение базы данных об основных характеристиках происшествий, о начале, завершении и об основных результатах экстренного реагирования на полученные вызовы (сообщения о происшествиях)
- формирование статистических отчетов по поступившим вызовам (сообщениям о происшествиях).

Основными целями создания «Системы-112» в Российской Федерации являются:

- организация удобного обращения к экстренным оперативным службам по принципу «одного окна»;
- уменьшение возможного социально-экономического ущерба вследствие происшествий и чрезвычайных ситуаций;
- организация комплекса мер, обеспечивающих ускорение реагирования и улучшение взаимодействия экстренных оперативных служб при вызовах (сообщениях о происшествиях);

- повышение оперативности и достоверности сбора, регистрации и распространения между экстренными службами информации о происшествиях и чрезвычайных ситуациях на территории субъекта РФ;
- реализация требований гармонизации способа вызова экстренных оперативных служб в РФ с законодательством Европейского союза.

1.5 Основные понятия и определения

Основные понятия и определения приведены в Табл. 1

Табл. 1. Термины и сокращения

Термин	Описание
АРМ	Автоматизированное рабочее место
АИС	Автоматизированная информационная система
АС	Автоматизированная система
ДДС	Дежурная - диспетчерская служба
ЕДДС	Единая дежурная - диспетчерская служба
ИБ	Информационная безопасность
ИС	Информационная система
ИСПДн	Информационная система персональных данных
МСЭ	Межсетевое экранирование
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПТК	Программно-технический комплекс
РД	Руководящий документ
САВЗ	Средство антивирусной защиты

Термин	Описание
СВТ	Средства вычислительной техники
СЗИ	Система защиты информации
ТС	Технические средства
УКЦ	Ключевой центр
ЦОВ	Центр обработки вызовов
ЦУС	Центр управления сетью

2 Правовая основа обеспечения информационной безопасности «Системы-112»

2.1 Общие положения

Учитывая особое значение «Системы-112» обеспечения вызова экстренных оперативных служб через единый номер «112» на базе единых дежурно-диспетчерских служб муниципальных образований Свердловской области, проблема защиты конфиденциальности и целостности критичной информации, а также обеспечение доступности вычислительных и коммуникационных ресурсов «Системы-112» является сложной и важной задачей.

В Доктрине информационной безопасности Российской Федерации задача защиты информационных ресурсов, информационных и телекоммуникационных систем, определена как одна из актуальнейших составляющих национальных интересов Российской Федерации в информационной сфере.

Для принятия адекватных мер защиты, соответствующих современным средствам нападения, и обеспечения приемлемого уровня рисков информационной безопасности создается комплексная система обеспечения информационной безопасности «Системы-112».

Концепция информационной безопасности «Системы-112» призвана консолидировать правовые, технологические, организационные, технические и физические меры и способы защиты информации. Она должна предусматривать возможность прогнозирования и отражения атак в реальном масштабе времени, а

также иметь продуманную долгосрочную политику, обеспечивающую повышение уровня информационной безопасности в соответствии с появлением новых источников и средств реализации угроз.

На систему информационной безопасности возлагаются задачи по организации защиты и предотвращению ущерба, который может быть нанесен за счет хищения, разглашения, утечки, утраты, искажения и уничтожения информации, нарушения работы технических средств, общего и прикладного программного обеспечения «Системы-112».

2.2 Нормативные, нормативно-технические и нормативно-методические документы

Использовались следующие нормативные, нормативно-технические и нормативно-методические документы:

- Конституция Российской Федерации, 12 декабря 1993 г.;
- Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных». Страсбург, 28 января 1981 г.;
- Федеральный закон Российской Федерации от 19 декабря 2005 г. №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон Российской Федерации от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»;
- Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр.-1895;

- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Перечень сведений конфиденциального характера»;
- Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности российской федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Положение о методах и способах защиты информации в информационных системах персональных данных, утверждено приказом ФСТЭК России от 5 февраля 2010г. № 58;
- Положение о лицензировании деятельности по технической защите конфиденциальной информации, утверждено Постановление Правительства Российской Федерации от 15 августа 2006 г. № 504;
- Положение об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утверждено постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781;
- Положение «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,Постановление Правительства Российской Федерации от 15 сентября 2008 г № 687;
- Порядок проведения классификации информационных систем персональных данных, утвержденный совместным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20;
- Руководящий документ Гостехкомиссии России. «Положение об обязательной сертификации продукции по требованиям безопасности информации» 1994 г.;
- Руководящий документ Гостехкомиссии России. «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» 1992 г.;

- Руководящий документ Гостехкомиссии России. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» 1992 г.;
- Руководящий документ Гостехкомиссии России. «Защита от несанкционированного доступа к информации. Термины и определения» 1992 г.;
- Руководящий документ Гостехкомиссии России. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» 1997 г.;
- Руководящий документ Гостехкомиссии России. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», Гостехкомиссия России, Москва, 1999 г.;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.;
- Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Государственной технической комиссией при Президенте Российской Федерации 25 ноября 1994 г.;
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г., № 149/54-144;

- Типовые требования по обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г., № 149/6/6-622;
- ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»;
- ГОСТ Р ИСО/МЭК 27001-2005 «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования»;
- ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения»;
- ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
- ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации»;
- ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем;
- ГОСТ 34.601-90. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;
- РД 50-680-88. Методические указания. Автоматизированные системы. Основные положения;
- РД 50-34.698-90. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на

автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.

3 Инвентаризация (учет) и категорирование (классификация)

В целях формирования дифференцированного подхода к обеспечению безопасности объектов защиты «Системы-112», характеризующихся различными степенями важности сохранения их функционирования или обеспечения конфиденциальности и целостности содержащейся в них информации, для предотвращения возможного ущерба осуществляется:

- категорирование защищаемых помещений – категорирование помещений, в которых проводятся обсуждения или ведутся переговоры по вопросам, содержащим защищаемую информацию, а также осуществляется автоматизированная обработка и хранение защищаемой информации, включающей сведения, составляющие служебную и другие виды тайны, сведения, относимые к категории «Для служебного пользования», и другие конфиденциальные данные;
- категорирование автоматизированных систем, предназначенных для обработки, передачи и хранения защищаемой информации, включающей сведения, составляющие служебную и другие виды тайны, сведения, относимые к категории «Для служебного пользования», и другие конфиденциальные данные;

Для информационных ресурсов «Системы-112» установлены следующие категории информационных ресурсов:

- категория «К» – сведения ограниченного доступа, включающие сведения, составляющие служебную и другие виды тайны, сведения, относимые к категории «Для служебного пользования», и другие конфиденциальные данные. Предъявляются требования к обеспечению конфиденциальности, целостности и/или доступности информационных ресурсов, а также к обеспечению юридической значимости информации (обеспечению неотказуемости) в соответствии с Федеральным законом «Об

информации, информационных технологиях и о защите информации» и руководящим документом Гостехкомиссии России (ФСТЭК России) «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;

- открытые сведения. Требования к обеспечению конфиденциальности, целостности и/или доступности информационных ресурсов, а также к обеспечению юридической значимости информации (обеспечению неотказуемости) не предъявляются.

Для каждой из категорий информационных ресурсов «Системы-112» устанавливается соответствующий порядок:

- назначения и изменения необходимых полномочий пользователей по доступу к информационным ресурсам соответствующей категории;
- эксплуатация оборудования и программного обеспечения, используемого для работы с информационными ресурсами соответствующей категории;
- обеспечение конфиденциальности, целостности и доступности информационных ресурсов соответствующей категории;
- обеспечение юридической значимости;
- принятие ответных мер в случае выявления действий, направленных на нарушение конфиденциальности, целостности или доступности, а также юридической значимости информационных ресурсов соответствующей категории.

Фрагменты «Системы-112», задействованные в работе с информационными ресурсами категории «К», должны отвечать требованиям ФСТЭК России (Гостехкомиссии России) по классу защищенности не ниже 1Г в соответствии с Руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утверждённого решением

Гостехкомиссии России от 30 марта 1992 года, с использованием сертифицированных средств защиты информации.

Для пользователей информационных ресурсов «Системы-112» устанавливаются формы допуска к информационным ресурсам. Форма допуска пользователя к информационным ресурсам устанавливается в соответствии с наивысшей категорией информационных ресурсов, к которым организован его доступ, и может служить основанием для ограничения использования информационных служб, оборудования и программного обеспечения.

4 Описание объекта защиты

4.1 Структура и состав объекта защиты

Объект защиты – Система-112 в части программно-аппаратного обеспечения ЦОВ-112 (ЦОВ(Д), РЦОВ(Д), ЦОВ ЕДДС МО, МСХД, ЛКП) и ЕДДС/ДДС.

Структура объекта защиты – каналы связи, серверы БД, серверы под управлением ОС Windows, АРМ операторов.

Автоматизированная «Система обеспечения вызова экстренных оперативных служб через единый номер «112» на базе единых дежурно-диспетчерских служб» представляет собой совокупность программно-технических комплексов (ПТК), объединенных каналами связи, имеющей подключения к сетям связи международного информационного обмена.

Система-112 в рамках Свердловской области строится по принципу децентрализованной системы обработки данных, состоящей из 7 центров обработки вызовов (ЦОВ-112), в т.ч. один резервный центр обработки вызовов (РЦОВ), территориально распложенных в центрах муниципальных образований Свердловской области. Каждый ЦОВ-112 является центром обработки информации, поступающей в единую дежурную-диспетчерскую службу (ЕДДС) муниципального образования. В свою очередь, основной ЦОВ, предусмотренный проектом в г. Екатеринбург, и серверное оборудование, расположенное в ЦОВ(Д)/РЦОВ(Д), служит для обеспечения работоспособности «Системы-112» в случае выхода из строя ЦОВ-112 любого из муниципальных образований, а также взаимодействия с геоинформационной системой (ГИС) и репликацию базы данных ЦОВ в часы наименьшей нагрузки. В случае выхода из строя ЦОВ(Д) его функции выполняет РЦОВ(Д).

ЕДДС каждого муниципального образования выполняет координирующую функцию экстренных служб и взаимодействует с каждой дежурной диспетчерской службой (ДДС) муниципального образования. Взаимодействие выполняется посредством электронного документооборота – операторы ЕДДС и ДДС заполняют карточки экстренных ситуаций, регистрирующих в базе данных обращения граждан по номеру «112» и результат работы экстренных служб.

Мониторинг и реагирование на данные, поступающие в Систему-112 осуществляет дежурный персонал. Создание и запись в базу данных карточек экстренных ситуаций осуществляется в автоматическом режиме при помощи специализированного программного обеспечения. Дежурство осуществляется сменным персоналом в круглосуточном режиме.

Создание «Системы-112» предусматривает создание следующих организационных уровней системы:

- Первый уровень – основной ЦОВ(Д) и РЦОВ(Д), расположенные в г.Екатеринбург;
- Второй уровень – ЦОВ ЕДДС МО и ЕДДС каждого муниципального образования Свердловской области;
- Третий уровень – дежурно-диспетчерские службы (ДДС) муниципальных образований Свердловской области.

Корпоративная сеть передачи данных рассматривается как множество узлов всех уровней по Свердловской области, связанных между собой каналами связи, предоставляемых Оператором связи.

В составе «Системы-112» выделяются объекты следующих типов:

- Основной ЦОВ(Д) – основной центр (сервера, коммуникационное оборудование);
- РЦОВ – резервный центр (сервера, коммуникационное оборудование);
- ЦОВ ЕДДС МО (сервера, коммуникационное оборудование);
- ЕДДС – операторские площадки на базе ЕДДС МО (сервера, АРМ оперативного и обслуживающего персонала, коммуникационное оборудование);
- ДДС – существующие ДДС (АРМ операторов, коммуникационное оборудование).

В Системе-112 обрабатывается информация ограниченного распространения, не содержащая сведений, составляющих государственную тайну (защищаемая информация) следующих типов:

- персональные данные граждан;

- информация для служебного пользования.

4.2 **Классификация аварийных ситуаций**

Ситуация, возникающая в результате нежелательного воздействия на Систему-112, не предотвращенного средствами защиты информации (СЗИ), называется аварийной.

Умышленное нападение – аварийная ситуация, которая возникла в результате выполнения заранее обдуманных и спланированных действий.

Под случайной (непреднамеренной) аварийной ситуацией понимается такая аварийная ситуация, которая не была результатом заранее обдуманных действий, и возникновение которой явилось результатом, объективных причин случайного характера, халатности, небрежности или случайного стечения обстоятельств.

По степени серьезности и размерам наносимого ущерба аварийные ситуации разделяются на следующие категории:

- Угрожающая – приводящая к полному выходу «Системы-112» или её компонент из строя, и ее неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации;
- Серьезная – приводящая к выходу из строя отдельных компонентов системы (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа.

Ситуации, возникающие в результате нежелательных воздействий, не наносящих ощутимого ущерба, но, тем не менее, требующие внимания и адекватной реакции к критическим не относятся.

К угрожающим ситуациям относятся:

- нарушение подачи электроэнергии объекта
- выход из строя сервера (с потерей информации);
- выход из строя сервера (без потери информации);

- частичная потеря информации на сервере без потери его работоспособности;
- выход из строя локальной сети (физической среды передачи данных).

К серьезным кризисным ситуациям относятся:

- выход из строя АРМ (с потерей информации);
- выход из строя АРМ (без потери информации);
- частичная потеря информации на АРМ без потери ее работоспособности.

К ситуациям, требующим внимания, относятся несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.

Источники информации о возникновении аварийной ситуации:

- пользователи, обнаружившие несоответствия плану защиты или другие подозрительные изменения в работе или конфигурации системы или средств ее защиты в своей зоне ответственности;
- средства защиты, обнаружившие предусмотренную планом защиты аварийную ситуацию;
- системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения аварийной ситуации.

Наиболее актуальные угрозы, характерные для «Системы-112», определяются исходя из уровня возможности реализации угроз (указанных в разделе «Модели угроз и нарушителя»):

- неверные настройки ПО, изменение режимов работы ТС и ПО (случайное либо преднамеренное);
- доступ в операционную среду (локальную ОС отдельного ТС «Системы-112») с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ;
- доступ в среду функционирования прикладных программ;

- доступ непосредственно к информации пользователя, обусловленный возможностью нарушения ее конфиденциальности, целостности, доступности;
- сканирование сети и анализ сетевого трафика для изучения логики работы «Системы-112», выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены;
- применение специальных программ для выявления пароля;
- реализация угрозы отказа в обслуживании;
- внедрение специализированных вредоносных программ;
- сетевые атаки;
- применение утилит администрирования сети;
- угрозы программно-математических воздействий;
- доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные);
- угрозы неправомерных действий со стороны лиц, имеющих право доступа к информации.

5 Модель угроз и нарушителя

5.1 **Состав информации**

В Система-112 обрабатывается информация ограниченного распространения, не содержащая сведений, составляющих государственную тайну (защищаемая информация) следующих типов:

- персональные данные граждан;
- информация для служебного пользования.

Персональные данные граждан могут быть представлены следующей информацией:

- ФИО;
- Данные о регистрации;
- Дата рождения;
- Номер телефона и место положения;
- Краткое описание обращения (может содержать данные, касающиеся состояния здоровья (диагноз));
- Запись разговора.

Система-112 в дальнейшем может иметь подключения к базам данных (БД), расположенным в других автоматизированных системах, при работе с которыми становится доступным более широкий перечень персональных данных граждан.

Таким образом, персональные данные (ПДн), обрабатывающиеся в системе, в том числе загружаемые из внешних систем, соответствуют наивысшей категории: 1 категории в соответствии с нормативно-методическими документами ФСТЭК России.

В Системе-112 обрабатываются следующие данные:

- прикладные данные – данные, обрабатываемые в системе операторами;
- служебные данные – данные, о конфигурации оборудования, системном и прикладном программном обеспечение, служебной информации, о передаваемых пакетах и т.п.

Средами обработки, хранения, передачи и вывода информации в Системе-112 являются:

- проводные каналы связи;
- стационарные средства хранения информации;
- оптическое отображение информации.

5.2 **Цели защиты информации**

Для информации, циркулирующей в Системе-112, должно быть обеспечено достижение следующих целей защиты информации:

- конфиденциальность;
- целостность;
- доступность.

Таким образом, согласно порядку проведения классификации информационных систем персональных данных, утвержденным Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года №55/86/20, Система-112 представляет собой информационную систему персональных данных (ИСПДн) и относится к категории специальных.

Исходя из системы классификации автоматизированных систем, предназначенных для обработки конфиденциальных данных (информации для служебного пользования) в соответствии с РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», то Система-112 является автоматизированной системой класса 1Г.

5.3 **Состав программно-аппаратных средств «Системы-112»**

В общем случае программное обеспечение «Системы-112», используемое для обработки информации ограниченного доступа, состоит из:

- системного программного обеспечения, представляемого операционными системами MS Windows 7 Pro на рабочих станциях и операционными системами MS Windows 2008 или Linux на серверах;

- прикладного программного обеспечения на серверах и рабочих станциях.

Технические средства «Системы-112», в общем случае состоят из:

- персональных компьютеров;
- серверов;
- коммутационного оборудования.

Типовая схема объекта «Системы-112» представлена на Рис. 1.

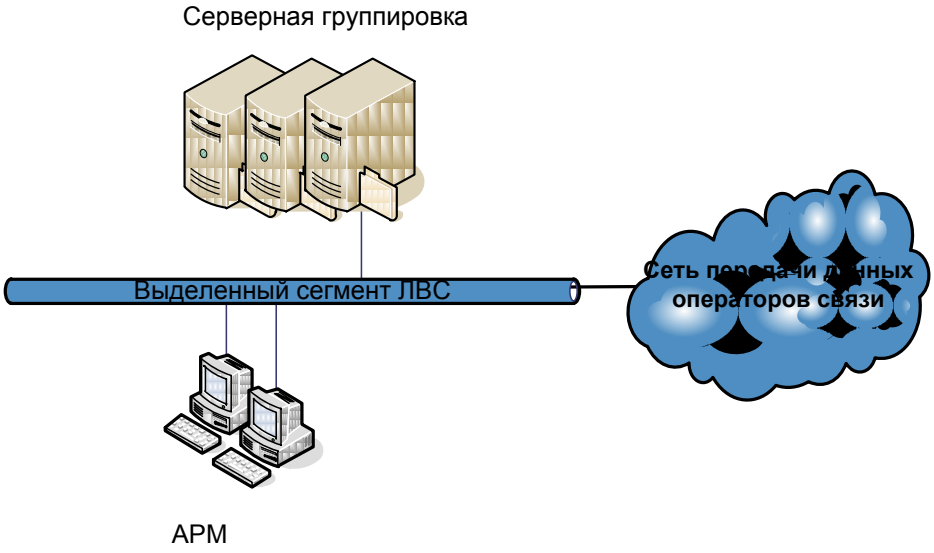

Рис. 1. Типовая схема объекта «Системы-112»

Серверные и сетевые компоненты объектов размещаются в серверных помещениях.

Граница контролируемой зоны (КЗ) проходит по периметру зданий.

Для «Системы-112» рассматривается два рубежа защиты:

- Контролируемая зона по периметру здания, в котором размещается объект.
- Границы помещений, в которых располагается оборудование объекта.

На объектах должен действовать контрольно-пропускной режим.

Прием посетителей осуществляется в соответствии с инструкциями по режиму.

5.4 **Структура объектов «Системы-112»**

Описание информационных процессов, существующих в каждом объекте, представлено в таблице 2

Табл. 2. Описание информационных процессов

Тип объекта	Информационные процессы
Первый уровень	Управление «Системой -112» Сбор и хранение информации Доступ ко всем объектам «Системы-112»
Второй уровень	Сбор и хранение информации Доступ к объектам «Системы-112», расположенным в данном районе Доступ во внешние БД для определения по имеющимся в Системе-112 персональным данным недостающей информации.
Третий уровень	Сбор и хранение информации Доступ к объектам «Системы-112», расположенным в диспетчерской службе Доступ во внешние БД для определения по имеющимся в Системе-112 персональным данным недостающей информации.

5.5 **Описание типовых функций и полномочий сотрудников**

Для описания моделей нарушителя и модели угроз определяются представленные в таблице 3 типовые функции сотрудников и их полномочия по работе на объектах «Системы-112». Данные функции являются типовыми, в зависимости от конкретного объекта возможно объединение для одного сотрудника нескольких функций.

Табл. 3. Функции и полномочия сотрудников

п/п	Функции персонала	Компонент ИСПДн	Полномочия по доступу
1.	Оператор	АРМ, БД ИСПДн	Пользовательские права доступа по обработке ПДн Права ввода информации в БД, ее просмотр или редактирование
2.	Администратор ИСПДн	АРМ, сервера	Информационное взаимодействие с ИСПДн Администраторские права по информационному обслуживанию СВТ, настройке ППО, предоставлению доступа
3.	Системный администратор	Коммуникационное оборудование	Администраторские права по техническому обслуживанию, настройке технических средств информатизации, входящих в состав ИСПДн, их СПО
4.	Обслуживающий персонал, входящий в штат	АРМ, сервера, коммуникационное оборудование, линии передачи данных, электропитания и заземления	Право на уборку помещений, в которых установлены средства информатизации ИСПДн, монтаж электрооборудования и т.п.

п/п	Функции персонала	Компонент ИСПДн	Полномочия по доступу
5.	Представители сторонних организаций, осуществляющие техобслуживание средств информатизации ИСПДн (все типы узлов)	АРМ, сервера, коммуникационное оборудование, линии передачи данных, электропитания и заземления	Монтаж технических средств и систем, осуществление их настройки, технического обслуживания или ремонта

5.6 **Объекты защиты**

В качестве объектов защиты в Системе-112 выступает:

- информация, хранящаяся или обрабатывающаяся на серверах, АРМ, жестких дисках и в оперативной памяти;
- носители информации, установленные в АРМ, серверах (не съёмные жесткие диски);
- конфигурационная и управляющая информация;
- информация в электронных журналах регистрации;
- система защиты информации, в том числе аутентифицирующая пользователей информация;
- общесистемное и прикладное программное обеспечение серверов, АРМ;
- аппаратные средства Система-112: оборудование серверов, АРМ, коммуникационное оборудование;
- побочные сигналы, которые возникают в процессе функционирования технических средств и в которых полностью или частично отражаются персональные данные или другая защищаемая информация;

- структурированные кабельные сети (СКС) внутри помещения, в котором функционирует система;
- оборудование электропитания;
- внешние кабельные коммуникации;
- строительные конструкции и элементы инженерно-технических сооружений помещения, в котором функционирует система.

Нарушение характеристик конфигурационной и управляющей информации может быть использовано потенциальными нарушителями для вывода «Системы-112» из штатного функционирования и реализации угроз безопасности защищаемой информации.

Нарушение целостности записей в электронных журналах регистрации может позволить потенциальным нарушителям скрыть попытки реализации несанкционированного доступа к защищаемой информации.

Остаточная информация на машинных носителях информации может содержать информацию ограниченного доступа.

Перехват побочных электромагнитных сигналов может позволить потенциальным нарушителям раскрыть содержание конфиденциальной информации.

5.7 **Классификация ИСПДн**

Классификация информационных систем персональных данных производится в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года №55/86/20, выделяются следующие категории ПДн:

- категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную

информацию, за исключением персональных данных, относящихся к категории 1;

- категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;
- категория 4 – обезличенные и (или) общедоступные персональные данные.

Результаты анализа состава ПДн, обрабатываемых в ИСПДн представлены в таблице 4.

Табл. 4. Результаты анализа состава ПДн

№ п/п	Анализируемый состав ПДн	Комментарии	Категория ПДн
1	Фамилия, имя, отчество (ФИО)	С одной стороны одни, и те же ФИО могут иметь различные люди, с другой, существуют ФИО редкие, принадлежащие только одному конкретному человеку. Учитывая наличие значительного количества таких данных в БД, существует достаточно большая вероятность наличия в них уникальных ФИО. Таким образом, предлагается изначально предполагать, что такие данные позволяют идентифицировать субъекта ПДн.	3
2	Данные о регистрации	По базе данных, содержащей только данные сведения, невозможно определить их принадлежность к кому-либо.	4 (обезличенные)
3	Дата рождения	По базе данных, содержащей только данные сведения, невозможно определить их принадлежность к кому-либо.	4 (обезличенные)
4	Номер телефона и местоположение	По номеру телефона физического лица, как правило, можно установить владельца данного телефона. Однако, учитывая, что владелец телефона и человек, который его использует для осуществления звонков, могут быть разными людьми, то эти данные	4 (обезличенные)

		обезличены.	
5	Сведения о причине обращения	По данным сведениям возможно получить о человеке дополнительную информацию, также могут содержаться сведения, касающиеся состояния здоровья (диагноз).	1
6	Запись разговора	По самому голосу содержащемуся в базе, невозможно определить их принадлежность к кому-либо, но по контексту возможно получить о человеке дополнительную информацию, также могут содержаться сведения, касающиеся состояния здоровья (диагноз).	1

С использованием результатов приведенного анализа сформированы следующие правила определения категории персональных данных при объединении персональных данных, касающихся одного и того же лица:

- если объединяются данные категории 4 (обезличенные), то полученный в результате массив данных также будет иметь 4 категорию;
- если объединяются данные категории 4 (общедоступные), то полученный в результате массив данных также будет иметь 4 категорию;
- если объединяются данные 3 категории (позволяющие идентифицировать субъекта ПДн) и данные категории 3 или 4 (при этом никакие данные из этих категорий не относятся к перечню данных, входящих в категорию 1), то итоговый массив данных будет относиться к категории 2 (данные позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию);
- если объединяются данные 2 категории и какие-либо данные категории 2-4 (при этом никакие данные из этих категорий не относятся к перечню данных, входящих в категорию 1), то итоговый массив данных также будет иметь 2 категорию;
- если объединяются данные 1 категории с какими-либо данными 2-4 категории, либо данные 2, 3 или 4 категории (общедоступные) с обезличенными данными, которые входят в перечень данных 1 категории

(касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни), то итоговый массив данных будет 1 категории.

Отображение данных правил в табличной форме представлено в таблице 5.

Табл. 5. Итоговые категории объединяемых типов данных

Объединяемые типы ПДн		4 категория (обезличенные)		4 категория (общедоступные)	3 категория	2 категория	1 категория
		Входят в кат. 1	Не входят в кат. 1				
4 категория (обезличенные)	Входят в кат. 1	4	4	1	1	1	1
	Не входят в кат. 1		4	2	2	2	1
4 категория (общедоступные)				4	2	2	1
3 категория					2	2	1
2 категория						2	1
1 категория							1

В соответствии с порядком проведения классификации информационных систем персональных данных определена категория ПДн обрабатываемых в Системе-112. Категория ПДн в Системе-112 - 1.

Помимо категории ПДн класс ИСПДн зависит от параметра, характеризующего объем ПДн и их особенности:

- 1 – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;
- 2 – в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в

отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

- 3 – в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

Планируемый объем обрабатываемых ПДн в Системе-112 – более 100 000.

В соответствии с порядком проведения классификации ИСПДн, установленным Приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г., ИСПДн подразделяются на следующие классы:

- класс 1 (К1) – ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;
- класс 2 (К2) – ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;
- класс 3 (К3) – ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;
- класс 4 (К4) – ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Класс информационных типовых систем определяется в соответствии с таблицей 6.

Табл. 6. Принципы классификации типовых ИСПДн

Категория ПДн	**Объем ПДн**		
	(3)	(2)	(1)

Категория ПДн	Объем ПДн		
	(3)	(2)	(1)
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

Основные характеристики ИСПДн представлены в таблице 7.

Табл. 7. Характеристики ИСПДн

№ п/п	Название ИСПДн	Структура ИСПДн	Наличие подключ- чения к ССОП	Режим обработки ПДн	По разгранич-нению прав доступа к ПДн	Местонахож-дение ТС относительно границ РФ	Объем обрабаты-ваемых ПДн	Катего-рия
1	Система-112	Распределенная	Есть	МП	С РПД	В пределах	Более 100 000	1

5.8 **Модель угроз**

Существует единственная методика определения актуальности угроз безопасности персональным данным, зафиксированная руководящим документом ФСТЭК России «Методика определения актуальности угроз безопасности персональным данным, обрабатываемым в информационных системах персональных данных». Предлагается использование данной методики для определения актуальности угроз всех типов информации ограниченного доступа (в том числе и ПДн), обрабатываемой в Системе-112.

В соответствии с методическим документом ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» к характеристикам ИСПДн, обуславливающим возникновение угроз безопасности персональным данным (УБПДн), относятся:

- важность защищаемой информации,

- категория и объем обрабатываемых в ИСПДн ПДн,
- структура ИСПДн,
- наличие подключений ИСПДн к сетям связи общего пользования (ССОП) и/или сетям международного информационного обмена (МИО),
- характеристики подсистемы безопасности ПДн,
- режимы обработки ПДн,
- режимы разграничения прав доступа пользователей ИСПДн,
- местонахождение и условия размещения технических средств ИСПДн.

Характеристики ИСПДн:

- в ИСПДн обрабатываются ПДн (1 категории);
- основными компонентами являются АРМ пользователей и серверы;
- информационная система ПДн является распределенной;
- ИСПДн имеет подключение к узлам, из которых осуществляется выход в сети связи общего пользования и сети международного информационного обмена через АРМ пользователей;
- в подразделениях с компонентами ИСПДн могут присутствовать сотрудники Организации, не являющиеся пользователями ИСПДн;
- в ИСПДн осуществляется многопользовательская обработка информации;
- пользователи ИСПДн обладают одинаковыми правами доступа ко всем обрабатываемым ПДн;
- в составе ИСПДн отсутствуют компоненты, размещенные за пределами Российской Федерации.

Кроме того, исходя из фактических данных, для «Системы-112» верны следующие положения:

- характеристики технологических процессов в рассматриваемой системе одинаковы и позволяют пользователям осуществлять операции чтения, модификации, удаления ПДн;
- к рассматриваемой Системе-112 имеет доступ ограниченный круг сотрудников;
- Организация является владельцем рассматриваемой базы данных, в которой содержится защищаемая информация;
- предоставляемые пользователям ИСПДн данные не являются обезличенными;
- часть ПДн может предоставляться сторонним пользователям, при этом предоставляется часть базы данных, в которой персональные данные подверглись определенной обработке;
- все АРМ и другие компоненты ИСПДн расположены в помещениях, в которых отсутствует неконтролируемый доступ посторонних лиц;
- во всех ИСПДн возможно акустическое озвучивание незначительного объема защищаемой информации, как правило, общедоступной;
- в системе возможно использование съемных носителей информации.

Актуальность угроз для «Системы-112» определена в таблице 8. Угрозы, признанные в данной таблице неактуальными далее не рассматриваются.

Табл. 8. Определение актуальности угрозы безопасности ПДн «Системы-112».

№ п/п	Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
1	Угрозы утечки информации по техническим каналам					
1.1	Угрозы утечки видовой информации:					
1.1.1	визуальный просмотр на экранах дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИСПДн	низкая	низкий	средняя	неактуальна	Визуальный просмотр экранов дисплеев и других средств отображения СВТ, ИВК не представляется

№ п/п	Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
						возможным
1.1.2	визуальный просмотр с помощью оптических (оптикоэлектронных) средств с экранах дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИСПДн	низкая	низкий	средняя	неактуальна	Внедрение, обслуживание подобных средств сложно и не обоснованно для получения ПДн в данном случае.
1.1.3	использование специальных электронных устройств съема видовой информации (видеозакладки)	низкая	низкий	средняя	неактуальна	
1.3	Угрозы утечки информации по каналам ПЭМИН:					
1.3.1	применение специальных средств регистрации ПЭМИН от ТС и линий передачи информации (ПАК, сканерные приемники, цифровые анализаторы спектра, селективные микровольтметры)	маловероятно	низкий	средняя	неактуальна	В местах обработки применяется большое количество разнообразного оборудования, которое излучает ПЭМИ, за счет объема оборудования информационный сигнал будет промоделирован множеством паразитных сигналов, которые сильно затрудняют получение информационного сигнала. С учетом стоимости оборудования съема информации по данному каналу, вероятность угрозы является маловероятной и угроза признана неактуальной
1.3.2	применение токосъемников для регистрации наводок информативных сигналов, обрабатываемых ТС, на цепи электропитания и линии связи, выходящие за пределы служебных помещений	маловероятно	низкий	средняя	неактуальна	
1.3.3	применение специальных средств регистрации радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав ТС ИСПДн или при наличии паразитной генерации в узлах ТС	маловероятно	низкий	средняя	неактуальна	
1.3.4	применение специальных средств регистрации радиоизлучений, формируемых в результате ВЧ-облучения ТС ИСПДн,	маловероятно	низкий	средняя	неактуальна	

№ п/п	Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
	в которых проводится обработка информативных сигналов - параметрических каналов утечки					
2.	Угрозы НСД в ИСПДн					
2.1	Угрозы использования уязвимостей ИСПДн:					
2.1.1	ошибки либо преднамеренное внесение уязвимостей при проектировании и разработке СПО и ТС, недекларированные возможности СПО	низкая	низкий	средняя	неактуальна	На стадии ввода в эксплуатацию проводится тестирование, которое исключает данную угрозу
2.1.2	неверные настройки ПО, изменение режимов работы ТС и ПО (случайное либо преднамеренное)	средняя	средний	высокая	актуальна	Угроза считается актуальной, т.к. существует вероятность неверной настройки ПО пользователем, что может послужить причиной некорректной работы программы и\или ТС и повлечь за собой утечку или искажение информации.
2.1.3	сбои в работе ТС и ПО (сбои в электропитании, выход из строя аппаратных элементов, внешние воздействия электромагнитных полей)	низкая	низкий	средняя	неактуальна	На АРМ и серверах используются ИБП
2.2	Угрозы непосредственного доступа в операционную среду ИСПДн:					
2.2.1	доступ к информации и командам, хранящимся в BIOS с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя	низкая	низкий	средняя	неактуальна	

№ п/п	Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
2.2.2	доступ в операционную среду (локальную ОС отдельного ТС ИСПДн) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ	средняя	средний	высокая	актуальна	
2.2.3	доступ в среду функционирования прикладных программ (локальная СУБД, например)	средняя	средний	высокая	актуальна	
2.2.4	доступ непосредственно к информации пользователя, обусловленный возможностью нарушения ее конфиденциальности, целостности, доступности	низкая	высокий	средняя	актуальна	
2.3	Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:					
2.3.1	сканирование сети и анализ сетевого трафика для изучения логики работы ИСПДн, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены	низкий	средний	средняя	актуальна	
2.3.2	применение специальных программ для выявления пароля (сниффинг, IP-спуффинг, разные виды перебора)	низкий	средний	средняя	актуальна	
2.3.3	подмена доверенного объекта сети с присвоением его прав доступа, внедрение ложного объекта сети	низкий	низкий	средняя	неактуальна	Вероятность реализации данной угрозы считается низкой поскольку технически сложно реализовать подмену доверенного объекта сети.
2.3.4	реализация угрозы отказа в обслуживании	низкая	средний	средняя	актуальна	

№ п/п	Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
2.3.5	внедрение специализированных троянских, вредоносных программ	низкая	средний	средняя	актуальна	
2.3.6	сетевые атаки	низкий	средний	средняя	актуальна	
2.3.7	применение утилит администрирования сети	низкий	средний	средняя	актуальна	
2.4	Угрозы программно-математических воздействий:					
2.4.1	внедрение программных закладок	средняя	средний	высокая	актуальна	
2.4.2	внедрение вредоносных программ (случайное или преднамеренное, по каналам связи)	средняя	средний	высокая	актуальна	
2.4.3	внедрение вредоносных программ (случайное или преднамеренное, непосредственное)	средняя	средний	высокая	актуальна	
2.5	Угрозы несанкционированного физического доступа к ТС и системам обеспечения:					
2.5.1	хищение ПЭВМ	низкий	низкий	средняя	неактуальна	ПЭВМ находятся в контролируемом помещении, где невозможно пребывание нарушителя без контроля сотрудников
2.5.2	хищение сервера	маловероятно	низкий	средняя	неактуальна	Сервера находятся в контролируемом помещении, где невозможно пребывание нарушителя без контроля сотрудников
2.5.3	нарушение функционирования АРМ, НЖМД	низкий	низкий	средняя	неактуальна	Нет опасности для субъекта ПДн
2.5.4	нарушение функционирования сервера, НЖМД	низкий	низкий	средняя	неактуальна	
2.5.5	нарушение функционирования кабельных линий связи, оборудования	средняя	низкий	средняя	неактуальна	

№ п/п	Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
2.5.6	доступ к системам обеспечения, их повреждение	средняя	низкий	средняя	неактуальна	
2.5.7	доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные)	средний	средний	высокая	актуальна	
2.6	Угрозы неправомерных действий со стороны лиц, имеющих право доступа к информации					
2.6.1	несанкционированное изменение информации	средняя	средний	высокая	актуальна	
2.6.2	несанкционированное копирование информации	средняя	средний	высокая	актуальна	
2.6.3	разглашение информации лицам, не имеющим права доступа к ней	средняя	средний	высокая	актуальна	
2.6.4	передача защищаемой информации по открытым каналам связи	средняя	средний	высокая	актуальна	
2.6.5	копирование информации на незарегистрированный носитель информации, в том числе печать	средняя	средний	высокая	актуальна	
2.6.6	передача носителя информации лицу, не имеющему права доступа к имеющейся на нем информации	средняя	средний	высокая	актуальна	

5.9 **Модель нарушителя**

Модель нарушителя, применительно к Системе-112, разрабатывается в соответствии с методическим документом ФСБ России №149/54-144 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденным 21 февраля 2008г.

Модель поведения нарушителя отражает потенциальные и реальные возможности, знания и места действия нарушителя.

Нарушитель – это лицо, предпринявшее попытку реализации угрозы безопасности информации по ошибке, незнанию или осознанно, и использующее для этого различные возможности, методы и средства. Злоумышленником определяем нарушителя, намеренно идущего на нарушение.

Основные мотивы совершения нарушений – безответственность, некомпетентность, халатность, самоутверждение, вандализм, принуждение, месть, корыстный интерес, идейные соображения.

Потенциальные нарушители делятся на:

- внешних нарушителей, не имеющих санкционированных возможностей по доступу в контролируемую зону;
- внутренних нарушителей, имеющих санкционированные возможности по постоянному или разовому доступу в контролируемую зону.

Типы нарушителей по возможностям доступа к различным компонентам объекта представлены в таблице 8.

Табл. 9. Типы нарушителей «Системы-112».

№ п/п	Функциональная характеристика нарушителя	Тип нарушителя
1	Внешний нарушитель	Тип 1
2	Посетитель	Тип 2
3	Обслуживающий персонал	Тип 3
4	Сотрудник, не являющийся пользователем	Тип 4
5	Оператор (пользователь)	Тип 5
6	Администратор	Тип 6
7	Сотрудник, обслуживающий ТС и ПО	Тип 7

К нарушителям 1 типа могут относиться отдельные лица, ведущие злоумышленную деятельность, не имеющие доступа в контролируемую зону (КЗ).

К нарушителям типа 2 могут относиться:

- посетители, имеющий разовый доступ в КЗ;
- определенные категории обсуживающего персонала и представителей ремонтных организаций, не имеющих доступ к компонентам АИСПДн.

Предполагается, что нарушители данного типа постоянно находятся под контролем сотрудников, так как никто не имеет права находиться в пределах КЗ без сопровождения сотрудника.

К нарушителям 3 типа могут относиться представители технических и обслуживающих служб, консультационных и других вспомогательных служб находящихся в пределах КЗ на постоянной основе или периодически. Нарушители этого типа не имеют права доступа к техническим средствам и программному обеспечению АИСПДн.

Предполагается, что нарушители данного типа постоянно находятся под контролем сотрудников.

К нарушителям типа 4 могут относиться сотрудники, не являющиеся операторами или администраторами «Системы-112».

Нарушителю типа 5 не рассматривается в настоящей модели. Предполагается, что операторы являются доверенными лицами и не относятся к категории нарушителей. Их доверенность должна обеспечиваться комплексом организационных мер по подбору персонала.

Нарушитель типа 6 предметно не рассматривается в настоящей модели. Предполагается, что контроль действий системных администраторов особо тщательно осуществляется администратором информационной безопасности, аудиторами информационной безопасности, что приводит к уменьшению риска утечки конфиденциальной информации к минимуму. Доверенность администраторов всех уровней должна обеспечиваться комплексом организационных мер по подбору персонала. При этом должны быть предусмотрены организационно-технические мероприятия по регистрации действий администраторов в Системе-112.

К нарушителям типа 7 могут относиться сотрудники организаций, осуществляющих обслуживание узлов на постоянной основе в соответствии с заключенными договорами (организации-разработчики ПО, ТС, организации, осуществляющие техническую поддержку).

Нарушитель типа 7 предметно не рассматривается в настоящей модели. Защита от нарушителя данного типа обеспечивается комплексом организационно-технических мер, условия обеспечения конфиденциальности должны быть обозначены в договорах с этими Организациями. При этом должны быть предусмотрены организационно-технические мероприятия по выводу защищаемой информации (ограничению доступа к ней) из системы на период проведения работ в системе потенциальных нарушителей данного типа.

Предполагается, что существующая в Организации система подбора кадров, а также действующие организационно-технические мероприятия исключают возможность сговора между нарушителями любых типов.

Предположения об имеющейся у нарушителя информации приведены в таблице 9.

Табл. 10. Предположения об имеющейся у нарушителя информации

№ п/п	Возможные виды потенциально опасной информации	Имеющаяся у нарушителя информация
1	Сведения о парольной и аутентифицирующей информации системы	Не обладает
2	Планы зданий, мест размещения технических средств с привязкой к конкретным помещениям	Обладает частично
3	Данные о составе пользователей	Достоверной информацией не обладает
4	Сведения об информационных ресурсах узлов – порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков	Достоверной информацией не обладает
5	Данные об организации работы, структуре и используемых технических, программных и программно-технических средствах узлов, в том числе тождественные проектной, конструкторской, программной и эксплуатационной документации на все компоненты узлов	Только имеющиеся в свободном доступе (например, сети Интернет)
6	Все возможные данные, передаваемые в открытом виде по каналам связи, не	Достоверной информацией не обладает

№ п/п	Возможные виды потенциально опасной информации	Имеющаяся у нарушителя информация
	защищенным от НСД к информации организационно-техническими мерами (команды синхронизации, незашифрованные адреса, команды управления и т.п.)	
7	Долговременные ключи криптосредств.	Не обладает.
8	Данные об уязвимостях СПО и ППО	Описания, имеющиеся в свободном доступе (например, сети Интернет)
9	Сведения о возможных для данного узла каналах атак	Достоверной информацией не обладает
10	Информация о способах (методах) атак	Описания, имеющиеся в свободном доступе (например, сети Интернет, печатных изданиях)
11	Данные об организациях осуществляющих поставку, ремонт, пуско-наладочные и монтажные работы, обслуживание технических и программных средств	Сведения, имеющиеся в свободном доступе (например, сети Интернет)
12	Данные о местах ремонта и обслуживания технических средств узлов	Сведения, имеющиеся в свободном доступе (например, сети Интернет)
13	Общая информированность нарушителя	Нарушитель 1 типа не обладает достоверной информацией об объекте и порядке обработки информации, информацию получает из источников свободного доступа. Нарушители 2, 3, 4 типов обладают определенной информацией о структуре объектов, однако не имеют достоверной информации об особенностях обработки информации. Нарушитель 5 типа имеет представление об особенностях обработки информации на объектах, однако не имеет достоверной информации и не имеет сведений о сетях связи, работающих на едином ключе.

Предположения о средствах атак, имеющихся у нарушителей, приведены в таблице 10.

Табл. 11. Предположения о средствах атак, имеющихся у нарушителей

№ п/п	Функциональная характеристика нарушителя	Средства атак, которыми могут располагать нарушители
Внешние нарушители		
1	Физические лица, не входящие в состав криминальных структур и иностранных разведок, но пытающиеся получить неправомерный доступ к базам данных и другой конфиденциальной информации, обрабатываемой в АС	Средства, имеющиеся в свободном доступе, в т.ч. в сети Интернет
Внутренние нарушители		
2	Работники и представители сторонних организаций, обеспечивающие охрану и нормальное функционирование служебных помещений (уборщицы, сантехники, электрики)	Средства, имеющиеся в свободном доступе, в т.ч. в сети Интернет
3	Посетители	Средства, имеющиеся в свободном доступе, в т.ч. в сети Интернет
4	Зарегистрированные пользователи АС	Штатные средства АРМ АС (с ограничениями) Средства, имеющиеся в свободном доступе, в т.ч. в сети Интернет

Возможные каналы атак, которые могут использовать нарушители, ограничены следующими предположениями:

- доступ в контролируемую зону подразделения, помещения регламентирован и контролируется соответствующим режимом;

- в пределах контролируемой зоны серверное оборудование, каналы связи и коммуникационное оборудование доступно только для администраторов, доступ пользователей и обслуживающего персонала ограничен;
- обслуживающий персонал при работе в помещениях, где расположены компоненты системы, сотрудники, не являющиеся пользователями, находятся в помещениях с компонентами узлов только в присутствии сотрудников узлов;
- внутренний нарушитель (тип 5) самостоятельно осуществляет создание методов и средств реализации атак, а также самостоятельно реализует атаки. При этом внутренний нарушитель данного типа не имеет прямых возможностей доступа к средствам криптографической защиты информации других компонентов ИС, так как доступ ограничивается межсетевыми экранами, настройками СПО и ППО, вследствие чего его возможности по доступу к СКЗИ соответствуют возможностям нарушителя типа 4.

Основными каналами атак являются:

- внешние каналы связи, не защищенные от НСД к информации организационно-техническими мерами;
- штатные средства;
- каналы непосредственного доступа к объекту атаки (визуальный, физический);
- машинные носители информации;
- носители информации, выведенные из употребления.

Каналы атак, связанные с получением информации по ПЭМИН, через устройства негласного съема информации отсутствуют ввиду имеющихся у нарушителей средств атак и предположений об актуальности угроз. К таким каналам относятся:

- сигнальные цепи;
- цепи электропитания;
- цепи заземления;

- канал утечки за счет электронных устройств негласного получения информации.

Доступ к информационным и управляющим интерфейсам СВТ ограничен ввиду введенных ограничений для нарушителей.

5.10 **Определение типа нарушителя**

На основе введенных предположений, об уровне информации, имеющейся у нарушителя, доступных ему средств и каналах атак можно сделать вывод, что нарушитель:

- не обладает достаточным уровнем возможностей для нарушителя класса Н3, а именно:
  - не известны все сети связи, работающие на едином ключе;
  - отсутствуют возможности по получению аппаратных компонент криптографических средств;
  - не имеют доступа к ключевым центрам;
- возможность использования штатных средств подразумевает уровень возможностей выше уровня нарушителя класса Н1.

Таким образом, нарушитель обладает возможностями класса Н2.

Итоговая классификация «Системы-112», обрабатывающей ПДн, представлена в таблице 12.

Табл. 12. Класс «Системы-112»

Характеристика	**Значение**
Структура системы	Распределенная
Наличие подключения к ТфОП	Есть
Режим обработки ПДн	Многопользовательский
Права доступа пользователей	Разные

Местонахождение ТС относительно границ РФ	В пределах
Объем обрабатываемых ПДн	Более 100 000
Класс ИСПДн	К1

В соответствии с руководящими документами ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» Система-112 класса К1 должна быть аттестована по требованиям безопасности информации.

При этом Система-112 является автоматизированной системой, в которой пользователи имеют одинаковые права доступа ко всей информации системы, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. В соответствии с РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» АС должна быть аттестована по классу 1Г.

В соответствии с руководящим документом ФСБ России «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» для каналов связи имеются следующие типы нарушителей и присваиваются следующие классы СКЗИ:

- нарушитель типа Н2 – нарушитель не владеет необходимой информацией и не обладает возможностями нарушителя типа Н3, однако его возможности выше, чем у нарушителя типа Н1;
- СКЗИ класса КС2.

Поскольку в Системе-112 осуществляется передача и обработка конфиденциальной информации (в том числе ПДн) различных типов и категорий, нарушитель класса Н2 и угроза ознакомления с информацией в канале связи рассматривается исключительно в отношении управляющей информации и информации баз данных. Предполагается, что информация в потоке голосовых данных избыточна и не представляет особой значимости для нарушителя, а способы ее

копирования/модификации не соизмеримы с затратами на проведение подобных работ.

Для нейтрализации и снижения вероятности проявления тех или иных угроз на всех стадиях жизненного цикла узлов необходимо использовать комплекс мер и средств защиты:

- организационных и организационно-технических;
- инженерных и инженерно-технических;
- технических;
- криптографических;
- программных, аппаратных и программно-аппаратных.

6 Реализация требований к подсистеме обеспечения информационной безопасности

6.1 Общая структура подсистемы обеспечения информационной безопасности

Общая структура представлена на Рис. 2.

Рис. 2. Общая структура подсистемы обеспечения информационной безопасности

Подсистема обеспечения информационной безопасности создается в составе следующих подсистем:

- защиты от НСД (реализующей функции: управления доступом, регистрации и учета, обеспечения целостности);
- межсетевого экранирования;

- криптографической защиты;
- антивирусной защиты;
- анализа защищенности;
- обнаружения вторжений.

6.2 **Комплекс технических средств, программное обеспечение подсистемы обеспечения информационной безопасности**

В составе комплекса технических средств подсистемы обеспечения информационной безопасности рассматриваются:

- Серверы IBM x3250, используемые для создания контролеров домена и серверов безопасности;
- Серверы HP DL360, используемые для подсистемы резервирования СЗИ
- АРМ администратора информационной безопасности;
- Шлюз CSP VPN Gate100/1000/3000/7000
- CSP VPN Client
- Stone Gate IPS-1205;
- ПАК «Соболь» (версии 3);
- USB-ключ eToken (Java)/72K/CERT-1883.

Характеристики технических средств приведены в таблице 13.

Табл. 13. Основные характеристики технических средств

Характеристика	Описание
Шлюз CSP VPN Gate100	
Аппаратная платформа	TONK 1400, 2xLAN 10/100
Операционная система	ОС Red Hat Enterprise Linux 5
Число сетевых портов	2x Ethernet 10/100 Mbit
Совместимость с другими программами	Cisco Routers. IOS version 12.4 (13a) и выше; Cisco PIX Security Appliance. Software version

	6.3 и выше; CSP VPN Client; CSP VPN Server; CSP VPN Gate 100B/100/1000/3000/7000; NME-RVPN (MCM).
Шифрование/ Аутентификация	Шифрование по ГОСТ 28147-89 (256 бит), Аутентификация узлов сети. Аутентификация пользователей. Контроль доступа на уровне хостов, индивидуальных пользователей и отдельных приложений.
Производительность шифрования	UDP-, TCP-трафик – до 5 Мбит/сек.
Число одновременно поддерживаемых защищенных соединений	10
Шлюз CSP VPN Gate1000	
Аппаратная платформа	TONK 1800, 4xLAN 10/100
Операционная система	ОС Red Hat Enterprise Linux 5
Число сетевых портов	4x Ethernet 10/100 Mbit
Совместимость с другими программами	Cisco Routers. IOS version 12.4 (13a) и выше; Cisco PIX Security Appliance. Software version 6.3 и выше; CSP VPN Client; CSP VPN Server; CSP VPN Gate 100B/100/1000/3000/7000; NME-RVPN (MCM).
Шифрование/ Аутентификация	Шифрование по ГОСТ 28147-89 (256 бит), Аутентификация узлов сети. Аутентификация пользователей.

	Контроль доступа на уровне хостов, индивидуальных пользователей и отдельных приложений.
Производительность шифрования	UDP-, TCP-трафик – до 10 Мбит/сек.
Число одновременно поддерживаемых защищенных соединений	50
Шлюз CSP VPN Gate3000	
Аппаратная платформа	Cisco UCS C200 M2, Redundant, 4xLAN 1Gb, Rack mount 1U
Операционная система	ОС Red Hat Enterprise Linux 5
Число сетевых портов	4x Ethernet 1000 Mbit
Совместимость с другими программами	Cisco Routers. IOS version 12.4 (13a) и выше; Cisco PIX Security Appliance. Software version 6.3 и выше; CSP VPN Client; CSP VPN Server; CSP VPN Gate 100B/100/1000/3000/7000; NME-RVPN (MCM).
Шифрование/ Аутентификация	Шифрование по ГОСТ 28147-89 (256 бит), Аутентификация узлов сети. Аутентификация пользователей. Контроль доступа на уровне хостов, индивидуальных пользователей и отдельных приложений.
Производительность шифрования	UDP-, TCP-трафик – до 200 Мбит/сек.
Число одновременно поддерживаемых защищенных соединений	1000

Шлюз CSP VPN Gate7000	
Аппаратная платформа	Cisco UCS C200 M2, Redundant, 4xLAN 1Gb, Rack mount 1U
Операционная система	ОС Red Hat Enterprise Linux 5
Число сетевых портов	4x Ethernet 1000 Mbit
Совместимость с другими программами	Cisco Routers. IOS version 12.4 (13a) и выше; Cisco PIX Security Appliance. Software version 6.3 и выше; CSP VPN Client; CSP VPN Server; CSP VPN Gate 100B/100/1000/3000/7000; NME-RVPN (MCM).
Шифрование/ Аутентификация	Шифрование по ГОСТ 28147-89 (256 бит), Аутентификация узлов сети. Аутентификация пользователей. Контроль доступа на уровне хостов, индивидуальных пользователей и отдельных приложений.
Производительность шифрования	UDP-, TCP-трафик – до 500 Мбит/сек.
Число одновременно поддерживаемых защищенных соединений	Не ограничено
Stone Gate IPS-1205	
Производительность МСЭ и отражения атак, Мбит/сек	1 000
Количество одновременно поддерживаемых сессий	1 300 000
Сетевые интерфейсы	6 Gigabit Ethernet + 1 Fast Ethernet (управление)

Форм-фактор	1RU
Сервер защиты сетевого взаимодействия	
Модель	Сервер IBM x3250 M4, Xeon 4C 3.1GHz 1333MHz 18GB, 2x500GB
Процессор	x3250 M4, Xeon 4C 3.10GHz/1333MHz
Оперативная память	18GB DDR3 1333MHz LP RDIMM
Сетевой адаптер	IBM Dual Port 1Gb Ethernet Daughter Card
	Intel PRO/1000 PT Dual Port Server Adapter
Контроллер жестких дисков	IBM ServeRAID BR10il SAS/SATA controller
Жесткий диск	2 IBM 500GB 2.5in SFF Slim-HS 10K 6Gbps SAS HDD
Блок питания	IBM 460W
Удаленное управление	IBM Virtual Media Key
Операционная система	Windows Server Std 2008 R2
Контролер домена/сервер безопасности	
Модель	Сервер IBM x3250 M4, Xeon 4C 3.1GHz 1333MHz 18GB, 2x500GB
Процессор	x3250 M4, Xeon 4C 3.10GHz/1333MHz
Оперативная память	18GB DDR3 1333MHz LP RDIMM
Контроллер жестких дисков	IBM Dual Port 1Gb Ethernet Daughter Card
Жесткий диск	Intel PRO/1000 PT Dual Port Server Adapter
Блок питания	IBM ServeRAID BR10il SAS/SATA controller
Удаленное управление	2 IBM 500GB 2.5in SFF Slim-HS 10K 6Gbps SAS HDD
Операционная система	IBM 460W
АРМ администратора информационной безопасности	
Монитор	LCD 22”
Процессор	Intel Core2 Duo E7300
Оперативная память	4 GB DDR3 PC3-10600
Видеокарта	Intel HD Graphics
Жесткий диск	2 x IBM HotSwap 500GB 7200rpm

Привод	SATA DVD-ROM 16X Max, SATA
Операционная система	Windows 7

6.3 **Размещение средств защиты информации**

Размещение компонент подсистемы обеспечения информационной безопасности приведено в таблице 14.

Табл. 14. Размещение компонент СЗИ

Компонент	Кол-во	Расположение
Программно-аппаратный комплекс "Соболь" (версия 3.0)	199	2 АРМ администратора ИБ 106 серверов приложений ЦОВ-112 (ЦОВ, РЦОВ, МЦОВ, ЕДДС МО) MN - узел управления телекоммуникационным узлом
Сервер безопасности Secret Net 6.5	1	Сервер безопасности 1 (ЦОВ)
Модификатор AD	1	Контролер домена (ЦОВ)
Средство управления Secret Net 6.5 «Монитор»	4	По 2 сервера безопасности (ЦОВ, РЦОВ)
Secret Net 6.5. «Клиент»	969	2 АРМ администратора 5 ПК МЦОВ 962 АРМ оператора
Система учета, управления и аудита средств аутентификации и хранения ключевой информации eToken TMS 2	2	2 контролера домена
Подключение eToken TMS	969	2 АРМ администратора 5 ПК МЦОВ 962 АРМ оператора
USB - ключ eToken PRO (Java)	969	2 АРМ администратора

Компонент	Кол-во	Расположение
		5 ПК МЦОВ 962 АРМ оператора
С-Терра КП	1	Сервер централизованного управления (ЦОВ)
CSP VPN 100	31	29 ЕДДС 2 ДДС
CSP VPN 1000	54	53 ЕДДС 1 ДДС
CSP VPN 3000	6	5 МЦОВ 1 ЕДДС
CSP VPN 7000	4	2 ЦОВ 2 РЦОВ
CSP VPN client	668	ДДС
Kaspersky BusinessSpace Security Russian Edition. 100-149 User 1 year Base License	1073	Все АРМ и серверы
StoneGate IPS-1205	7	1 ЦОВ 1 РЦОВ 5 МЦОВ
XSpider 7.8	1	АРМ администратора ИБ 1
Acronis Backup & Recovery Advanced Server	4	2 Сервера безопасности 2 Контролера домена
Acronis Backup & Recovery Advanced Workstation	2	АРМ администратора ИБ 1 АРМ администратора ИБ 2

6.4 **Режимы функционирования, диагностирования подсистемы обеспечения информационной безопасности**

Определены следующие режимы функционирования:

- штатный режим функционирования;
- нештатный (аварийный) режим функционирования.

Основным режимом функционирования СЗИ является штатный режим. В штатном режиме функционирования системы клиентское программное обеспечение, технические средства пользователей и администраторов системы обеспечивают возможность функционирования в рабочие часы. Серверное программное обеспечение и технические средства серверов обеспечивают возможность круглосуточного функционирования, с перерывами на обслуживание. Степень детализации и периодичность технического обслуживания определяется внутренними документами.

Основными признаками нормального функционирования являются исправно работающее оборудование системы. Исправно функционирует системное и прикладное программное обеспечение системы. Для обеспечения нормального режима функционирования системы необходимо выдерживать условия эксплуатации программного обеспечения и программно-аппаратных комплексов системы, указанные в соответствующих технических документах (техническая документация, инструкции по эксплуатации).

Аварийный режим функционирования системы характеризуется отказом одного или нескольких компонентов программного и (или) технического обеспечения. В случае перехода системы в аварийный режим требуется при необходимости завершить работу всех приложений с сохранением данных. Выключить при необходимости рабочие станции работников. Выключить при необходимости все периферийные устройства. Выполнить внеплановое резервное копирование выделенных информационных ресурсов. После этого необходимо выполнить комплекс мероприятий по устранению причины перехода системы в аварийный режим.

Табл. 15. Режимы функционирования компонент подсистемы обеспечения информационной безопасности

Компонент	Режим функционирования
Kaspersky BusinessSpace Security Russian Edition. 100-149 User 1 year Base License	Круглосуточно и ежедневно (для серверов); В рабочие часы пользователей;

Компонент	Режим функционирования
	В рабочие часы администраторов
Secret Net 6.5 (Сервер безопасности)	Круглосуточно и ежедневно
Secret Net 6.5 (Клиент)	Круглосуточно и ежедневно (для серверов); В рабочие часы пользователей; В рабочие часы администраторов
eToken TMS	Круглосуточно и ежедневно
USB-ключ eToken PRO (Java)	В рабочие часы пользователей; В рабочие часы администраторов
С-Терра КП	Круглосуточно и ежедневно
CSP VPN 100	Круглосуточно и ежедневно
CSP VPN 1000	Круглосуточно и ежедневно
CSP VPN 3000	Круглосуточно и ежедневно
CSP VPN 7000	Круглосуточно и ежедневно
CSP VPN client	В рабочие часы пользователей
Stone Gate IPS-1205	Круглосуточно и ежедневно
Catalyst 2960S 24 GigE	Круглосуточно и ежедневно
Контролер домена	Круглосуточно и ежедневно
Сервер безопасности	Круглосуточно и ежедневно
XSpider 7.8	В рабочие часы администратора

Диагностика работы систем, анализ защищенности, проверка корректности работы и настройки механизмов защиты производится посредством сканера безопасности «XSpider 7.8» и стандартных механизмов, предоставляемых программным обеспечением и аппаратными средствами средств защиты.

Диагностике должны быть подвергнуты АРМ и серверное оборудование.

6.5 **Подсистема защиты от НСД**

Подсистемой должны быть реализованы функции по защите информации от несанкционированного доступа, включающие в себя: управление доступом, регистрацию и учет действий пользователей и процессов, обеспечение целостности.

Защита информации от НСД реализуется встроенными механизмами на оборудовании телекоммуникационного узла и сертифицированными средствами «SecretNet 6.5 (Вариант К)» и «eToken» на серверах и АРМ.

Механизмы безопасности «SecretNet 6.5 (Вариант К)»

Механизмы Secret Net 6.5, вариант-К (Сетевой) по разграничению доступа:

- разрешение/запрет работы субъекта доступа на рабочей станции или сервере (в том числе по времени);
- требования к сложности пароля пользователя и регулярности его смены;
- параметры блокировки учетной записи пользователя при неудачных попытках входа;
- привилегии входа пользователя в систему;
- привилегии пользователя по завершении работы системы;
- привилегии пользователя по работе в сети;
- привилегии пользователя по использованию штатных средств Windows;
- привилегии пользователей на доступ к защищаемым файлам и каталогам ИСПДн (механизм полномочного разграничения доступа);
- блокировка сессии доступа к рабочей станции или серверу ИСПДн;
- права доступа пользователя к аппаратным средствам компьютера.

Средствами «Secret Net 6.5, вариант-К (Сетевой)» реализуется регистрация следующих событий безопасности:

- регистрация входа (выхода) пользователя в ОС;
- регистрация запуска (останова) службы регистрации;

- аудит изменения настроек регистрации;
- регистрация событий переполнения журнала регистрации;
- регистрация очистки журнала регистрации;
- регистрация обработки задания на контроль целостности.

Средствами «Secret Net 6.5, вариант-К (Сетевой)» реализуются следующие функции по контролю целостности:

- контроль целостности системных файлов и конфиденциальной информации, обрабатываемой на рабочих станциях пользователей и файловых серверах;
- оповещение администраторов о фактах нарушения политик контроля целостности;
- регистрация события в журнале SecretNet;
- блокировка компьютера;
- контроль контрольных сумм объектов.

Средствами управления «Secret Net 6.5, вариант-К (Сетевой)» реализуются следующие функции:

- настройка системы и управление работой защитных механизмов;
- мониторинг и оперативное управление;
- аудит системы.

Средствами оперативного управления «Secret Net 6.5, вариант-К (Сетевой)» реализуются следующие функции:

- контроль состояния автоматизированной системы;
- оповещение о событиях НСД;
- выдача оперативных команд управления;
- централизованный сбор, хранение и архивирование журналов;
- загрузка записей журналов для просмотра и анализа зарегистрированных событий.

Secret Net 6.5, вариант-К (Сетевой) состоит из следующих компонентов:

- Secret Net 6.5, вариант-К - Сервер Безопасности;
- Secret Net 6.5, вариант-К - Клиент;
- Secret Net 6.5, вариант-К – Модификатор схемы AD;
- Secret Net 6.5, вариант-К – Средства управления.

Сервер Безопасности обеспечивает взаимодействие всех компонентов средства, сбор, обработку и передачу данных, передачу команд оперативного управления. Сервер безопасности управляет поведением агентов оперативного управления, устанавливаемых на клиентские рабочие станции, или подчиненных серверов безопасности, принимает от них уведомления о событиях, производит сборку журналов и накапливает полученную информацию в базе данных оперативного управления.

Клиент обеспечивает реализацию защитных механизмов рабочих станций, следит за соблюдением настроенной политики безопасности на рабочих станциях и серверах, обеспечивает регистрацию событий безопасности и передачу журналов на Сервер Безопасности, а также приём от него оперативных команд и их выполнение.

Модификатор схемы Active Directory (AD) представляет собой программное средство автоматического добавления в схему AD классов и атрибутов, необходимых для функционирования системы Secret Net 6.5, вариант-К. Компонент применяется однократно перед развертыванием системы в домене. Схема Active Directory содержит правила создания объектов в домене (лесе доменов). Эти правила определяют информацию, которая может быть сохранена с каждым объектом, и тип данных, соответствующий этой информации. Таким образом, в домене нельзя создать объект, если он не описан в схеме AD. Процесс расширения схемы называется модификацией схемы AD и является стандартным. Модификация схемы AD для установки системы Secret Net 6.5, вариант-К — это процедура описания в схеме AD объектов Secret Net 6.5, вариант-К, выполняемая Модификатором AD.

Тесная интеграция системы управления с Active Directory позволяет использовать Secret Net 6.5, вариант-К для организации защиты сети, использующей многодоменную структуру.

Secret Net 6.5, вариант-К – Средства управления состоит из компонент, которые делятся на две группы:

- средства централизованной настройки и управления — обеспечивают централизованное управление параметрами защитных подсистем клиентов;
- средства оперативного управления — предоставляют возможности мониторинга защищаемых компьютеров и оперативного управления ими с рабочего места администратора, а также осуществляют централизованный сбор, хранение и архивирование системных журналов.

Централизованная настройка защитных механизмов и изменение параметров пользователей осуществляются следующими средствами:

- редактор свойств пользователей и редактор объектов групповой политики — представляют собой расширения стандартных средств централизованного управления ОС Windows;
- программа «Контроль программ и данных» в централизованном режиме работы — устанавливается на защищаемых компьютерах при установке клиентского ПО в сетевом режиме функционирования. В этой программе можно централизованно выполнять настройку механизмов контроля целостности и замкнутой программной среды.

В качестве хранилища централизованно заданных параметров используется Active Directory.

Программа мониторинга устанавливается на рабочем месте администратора - сотрудника, уполномоченного контролировать и оперативно корректировать состояние защищаемых компьютеров в режиме реального времени.

Программа мониторинга обеспечивает:

- получение от Сервера Безопасности информации об изменении состояния компьютера и отображение сведений о текущем состоянии;
- информирование оператора о получении уведомления о НСД;

- передача команд оператора на утверждение изменений аппаратной конфигурации, на перезагрузку компьютера или принудительный выход пользователя и пр.

В процессе работы программа мониторинга взаимодействует с сервером безопасности, по отношению к которому она является клиентом.

При изменении состояния какого-либо компьютера установленный на нем агент передает эти сведения серверу безопасности, а сервер в свою очередь — программе мониторинга. Аналогичным образом в программу мониторинга поступают сведения о НСД.

Программа просмотра централизованных журналов устанавливается на рабочем месте сотрудника, уполномоченного проводить аудит системы защиты.

По запросу сервера безопасности агенты передают ему локальные журналы защищаемых компьютеров, и сервер загружает их в свою базу данных оперативного управления. После передачи локальные журналы очищаются. Сбор журналов осуществляется сервером по команде или по расписанию, составленному администратором.

Функции безопасности eToken

Средством защиты от НСД eToken реализуются следующие функции:

- двухфакторная аутентификация пользователей и администраторов;
- автоматическая генерация сложных паролей;
- автоматическая блокировка консоли рабочей станции при отсоединении eToken.

Функции безопасности ОС Линукс

Операционная система Линукс предназначена для обеспечения выполнения программ в защищённой среде.

Комплекс встроенных средств защиты информации (КСЗ), является принадлежностью операционной среды и неотъемлемой частью ядра ОС и системных библиотек, предназначенный для защиты от несанкционированного доступа к обрабатываемой (хранящейся) информации на сервере.

Функции ОС Линукс, обеспечивающие защиту данных:

- реализация механизма идентификации и аутентификации (МИА) пользователей (парольный вход пользователей в систему);
- объединение пользователей в группы с общими файлами и каталогами;
- реализация дискреционного метода защиты файлов (чтение, запись, удаление, переименование, изменение системного атрибута, создание с тем же именем);
- изменения правил разграничения доступа (установка/изменение атрибутов защиты);
- регистрация событий в системных журналах (события МИА, запросы на доступ к защищаемым ресурсам, создание и уничтожение объектов, изменения правил разграничения доступа);
- автоматическая установка атрибутов защиты и владения на новые создаваемые пользователем файлы и каталоги;
- скрытие служебной информации: персональной, регистрационной и конфигурационной;
- очистка памяти для новых процессов.
- безопасное удаление файлов.

6.6 Подсистема криптографической защиты, межсетевого экранирования

Для выполнения требований применяются средства межсетевого экранирования, криптографической защиты:

- С-Терра КП;
- CSP VPN 100;
- CSP VPN 1000
- CSP VPN 3000
- CSP VPN 7000

- CSP VPN Client

С-Терра КП – это комплекс программного обеспечения, включающий в себя:

- центр управления сетью (ЦУС);
- удостоверяющий и ключевой центр (УКЦ).

Центр управления сетью является регистрационным центром и предназначен для конфигурации и управления виртуальной сетью, решает следующие основные задачи:

- задает узлы сети, группы пользователей и пользователей в них;
- задает допустимые связи между группами пользователей и, соответственно, между узлами. Эти связи, определяющие возможности доступа к конкретным техническим и информационным ресурсам корпоративной сети, адресные книги и ключевая информация не доступны для модификации со стороны пользователей и их может изменить только ЦУС;
- определяет типовые политики безопасности и распределение допустимых полномочий пользователей и локальных администраторов на конкретных узлах по изменению политик безопасности для этих узлов;
- обеспечивает автоматическую защищенную доставку и контроль доставки на узлы измененных справочников доступа, ключевой информации из УКЦ (симметричные ключи, сертификаты пользователей, списки сертификатов, выведенных из действия, сертификаты ключевых центров других сетей.);
- обеспечивает обмен с ЦУСами других виртуальных сетей списками объектов своих сетей, которые должны взаимодействовать между собой. Производит взаимное согласование с этими ЦУСами допустимых межсетевых связей между объектами сетей. Обеспечивает обмен корневыми сертификатами этих сетей, списками сертификатов, выведенных из действия;
- выполняет оперативные действия в случаях компрометации ключевой информации на объектах сети;

- осуществляет автоматическое обновление программного обеспечения на объектах сети в удаленном режиме;
- обеспечивает удаленный просмотр и анализ журналов событий для компонент CSP VPN 100/1000/3000/7000/Client, контроль успешности высланных ЦУСом обновлений ключей, справочников и программного обеспечения.

Удостоверяющий и ключевой центр предназначен для обеспечения ключевой информацией всех участников VPN-сети и выполнения функций удостоверяющего центра. Последующее обновление ключевой информации осуществляется автоматически по защищенным VPN-каналам.

Удостоверяющий и ключевой центр решает следующие основные задачи:

- формирование и автоматическое обновление через ЦУС симметричной ключевой информации и первичной парольной информации для объектов и пользователей сети;
- выполнение функций удостоверяющего центра сертификатов цифровых подписей.

CSP VPN 100/1000/3000/7000 – программно-аппаратный комплекс, выполняющий функции универсального сервера защищенной сети и выполняет следующие функции:

- сервер IP-адресов – обеспечивает регистрацию и доступ в реальном времени к информации о состоянии объектов защищенной сети и текущем значении их сетевых настроек (IP- адресов и т.п.);
- прокси-сервер защищенных соединений – обеспечивает подключение локальной ViPNet сети к другим аналогичным сетям через публичные сети (Интернет);
- туннельный сервер (криптошлюз) – обеспечивает туннелирование (шифрование) трафика от незащищенных компьютеров и серверов локальной сети для его передачи к другим объектам защищенной сети (в том числе мобильным и удаленным) в зашифрованном виде по открытым каналам публичных сетей;

- межсетевой экран – обеспечивает в соответствии с заданной политикой безопасности фильтрацию трафика по множеству параметров (порты, протоколы, диапазоны адресов и др.) между сегментами защищенной и открытой сетей;
- сервер защищенной почты – обеспечивает маршрутизацию почтовых сообщений и служебных рассылок в рамках защищенной сети.

CSP VPN Client – программное обеспечение, реализующее на рабочем месте пользователя или сервере с прикладным ПО функции VPN-клиента, персонального экрана, средства идентификации и аутентификации.

6.7 **Подсистема обнаружения вторжений**

Для выполнения требований применяется средство межсетевого экранирования и обнаружения вторжений - программно-аппаратный комплекс Stone Gate IPS, позволяющий обеспечить проактивную защиту от вторжений.

В основе StoneGate IPS лежат различные методы обнаружения вторжений, такие как:

- сигнатурный анализ;
- технология декодирования протоколов, не имеющих сигнатур;
- анализ аномалий протоколов;
- анализ поведения конкретных узлов;
- выявление статистических отклонений в потоке данных;
- корреляционный анализ происходящих событий.

Ключевые особенности решения:

- обнаружение и предотвращение попыток НСД в режиме реального времени в прозрачном для пользователей режиме;
- кластеризация и возможность плавного наращивания производительности;
- обширный список сигнатур атак (по содержанию, контексту сетевых пакетов и другим параметрам);

- возможность обработки фрагментированного сетевого трафика;
- возможность выявления попыток туннелирования трафика, поддержка IPv6;
- инспекция внутри SSL/TLS;
- возможность борьбы с (D)DoS-атаками;
- декодирование протоколов для точного определения специфических атак для более чем 20 протоколов уровня приложений с возможностью задания специфических параметров для них;
- возможность фильтрации трафика по принципу «прозрачных» межсетевых экранов вплоть до 2-го уровня модели OSI (оперирование фреймами);
- возможность контроля нескольких сегментов на одном устройстве с разными скоростями – виртуализация сенсора;
- наличие встроенного аппаратного bypass-модуля для отказоустойчивости канала связи;
- возможность автоматического обновления базы данных правил инспекции потоков и системного ПО;
- блокировка или завершение нежелательных сетевых соединений (в том числе установки динамических фильтров на межсетевых экранах для блокирования атакующих), выдача HTML ответа пользователю с детализацией ошибки по факту блокирования;
- возможность профилирования сетей и сервисов (profile) для выявления новых сервисов и узлов, установленных без ведома администратора;
- анализ «историй» событий безопасности и расследования инцидентов;
- ведение аудита и выявление истории изменений, в том числе графического сравнения разных конфигураций сенсоров;
- редактирование и произвольное составление отчетов с помощью более 100 доступных счетчиков;

- встроенный анализатор событий, позволяющий эффективно снижать поток ложных срабатываний (доступна не только групповая, но и корреляция по последовательностям событий);
- создание собственных сигнатур атак, шаблонов анализа атак, аномалий и др.;
- распределенная многоуровневая система управления и мониторинга с возможностью создания отказоустойчивых конфигураций;
- мониторинг и управление (контекстное, tool profile) сторонними устройствами;
- сбор, хранение и консолидированная обработка событий от сторонних устройств;
- централизованное дистанционное обновление программного обеспечения вместе с операционной системой;
- интуитивно понятный интерфейс, интегрированный с межсетевым экраном StoneGate и системой построения VPN;
- ролевое разграничение полномочий администраторов и развитая система оповещения о событиях;
- поддержка иерархической доменной архитектуры в системе управления, позволяющей легко создавать новые сервисы для MSSP и подключать новых Клиентов;
- интеграция с технологией NAC и поддержка другими мировыми вендорами решений по обеспечению безопасности.

StoneGate IPS имеет возможности комбинирования режимов IDS и IPS для разных сегментов сети, что позволяет осуществлять контроль подсетей с применением различных политик безопасности. Для осуществление контроля на уровне VLAN имеется возможность логического деления физического интерфейса на подуровни.

В состав StoneGate IPS входит анализатор событий, позволяющий обрабатывать информацию с нескольких сенсоров и осуществлять корреляцию событий между ними. Система обнаружения и предотвращения вторжений StoneGate IPS оптимизирована для обнаружения атак, распределенных во времени,

специфических атак, использующих слабые места почтовых систем, систем ERP, предотвращения распространения и использования вредоносного и шпионского ПО, утечки информации с использованием пиринговых сетей, ICQ и др. Имеются уникальные механизмы по анализу действий пользователей в сети и анализу аномальной активности.

6.8 **Подсистема анализа защищенности**

Анализ защищенности проводится для распределенных информационных систем и информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) анализа защищенности. Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

Для выполнения требования применяется средство анализа защищенности - сканер безопасности «XSpider 7.8».

Механизмы сканера безопасности «XSpider 7.8»:

- полная идентификация сервисов на случайных портах;
- проверка на уязвимость серверов со сложной нестандартной конфигурацией, когда сервисы имеют произвольно выбранные порты;
- эвристический метод определения типов и имен серверов;
- определение RPC-сервисов и поиска уязвимостей в них;
- проверка стойкости парольной защиты;
- подбор паролей в сервисах, требующих аутентификации, для выявления нестойких паролей/не соответствующих разработанным политикам;
- поиск и анализ директорий доступных для просмотра и записи;
- проведение проверок на нестандартные DoS-атаки;

- осуществление проверок «на отказ в обслуживании»;
- механизмы, уменьшающие вероятность ложных срабатываний при осуществлении сканирования.

6.9 **Подсистема антивирусной защиты**

В автоматизированных информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

Для выполнения данного требования применяется антивирусное средство Dr.Web. Механизмы, выполняемые антивирусными средствами Dr.Web:

- антивирусная защита ключевых узлов сети - рабочих станций, серверов;
- поддержка всех основных операционных систем для рабочих станций;
- расширенная проактивная защита рабочих станций и файловых серверов от новых вредоносных программ;
- проверка электронной почты и интернет-трафика в режиме реального времени;
- защита серверов под управлением Windows Server 2008 R2, Linux.

7 Взаимосвязь с внешними системами

К внешним системам относятся:

- внешние сети передачи данных;
- телекоммуникационное оборудование;
- система электропитания и заземления.

Защита ИСПДн при подключении к открытой сети, внешним сетям передачи данных осуществляется только при установке средств межсетевого экранирования.

Электропитание оборудования должно осуществляться от однофазной (трехфазной) сети переменного тока 220 В, 50 Гц.

Для бесперебойного питания оборудования должны использоваться источники бесперебойного питания.

Лист согласования

Наименование организации	Должность	ФИО	Подпись	Дата

Лист регистрации изменений

Изм	Номера листов (страниц)				Всего листов (страниц) в док.	№ разреш. документа	Подпись	Дата	Примечание
	Измененных	Замененных	Новых	Аннулированных					