ТЕХНИЧЕСКИЙ ПРОЕКТ[1]

системы обеспечения вызова экстренных оперативных служб по единому номеру «112» на базе единых дежурно-диспетчерских служб муниципальных образований субъекта Российской Федерации

Технический проект
подсистемы обеспечения информационной безопасности
системы обеспечения вызова экстренных оперативных служб по единому номеру «112» на базе единых дежурно-диспетчерских служб муниципальных образований субъекта Российской Федерации

Листов 28

2012

Подпись и дата | Инв. № дубл. | Взам. инв. № | Подпись и дата | Инв. № подл.

[1] в настоящем образце не приводятся лист утверждения, лист регистрации изменений и иные элементы оформления согласно стандартам

Оглавление

ПЕРЕЧЕНЬ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ

АРМ	-	автоматизированное рабочее место
АС	-	автоматизированная система
БД	-	база данных
ДДС	-	дежурно-диспетчерская служба, в настоящем документе означает весь перечень экстренных оперативных служб, оперативных служб и организаций, интегрируемых в систему-112
диспетчер	-	сотрудник дежурной службы ДДС
ЕДДС	-	единая дежурно-диспетчерская служба
ИБ	-	информационная безопасность
КТС	-	комплекс технических средств
ЛВС	-	локальная вычислительная сеть
МЧС России	-	Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий
НСД	-	несанкционированный доступ
оператор	-	сотрудник ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС, осуществляющий прием и обработку вызовов по номеру 112
ОС	-	операционная система
ПО	-	программное обеспечение
ПОИБ	-	подсистема обеспечения информационной безопасности
РД	-	руководящий документ
региональный ЦУКС МЧС России	-	центр управления в кризисных ситуациях главного управления Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий по субъекту Российской Федерации
РИВП	-	распределенная информационно-вычислительная платформа
РЦОВ	-	резервный центр обработки вызовов системы-112
САЗ	-	средство анализа защищенности
СЗИ	-	средства защиты информации
система-112	-	система обеспечения вызова оперативных служб по единому номеру «112» на базе единых дежурно-диспетчерских служб муниципальных образований субъекта Российской Федерации
СПО	-	специальное программное обеспечение
ССОП	-	сеть связи общего пользования
СУБД	-	система управления базами данных
Субъект РФ	-	субъект Российской Федерации, в настоящем документе применяется для обозначения субъекта Российской Федерации, на территории которого создается система-112
УОВЭОС	-	узел обслуживания вызовов экстренных оперативных служб
ЦОВ-АЦ	-	центр обработки вызовов системы-112, развертываемый в административном центре субъекта Российской Федерации
ЦОВ-ЕДДС	-	центр обработки вызовов системы-112 на базе единой дежурно-диспетчерской службы муниципального района субъекта Российской Федерации
ЧС	-	чрезвычайная ситуация
ЭРА ГЛОНАСС	-	система экстренного реагирования при авариях, основанная на применении российских средств глобальной спутниковой навигации, ГЛОНАСС и систем спутникового мониторинга транспорта

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование проектируемой системы

Подсистема обеспечения информационной безопасности системы обеспечения вызова экстренных оперативных служб по единому номеру «112» на базе единых дежурно-диспетчерских служб муниципальных образований Субъекта РФ.

Краткое наименование – ПОИБ-112 .

1.2. Назначение, цели создания подсистемы обеспечения информационной безопасности системы-112

Система-112 предназначена для информационного обеспечения единых дежурно-диспетчерских служб муниципальных образований. Она обеспечивает информационное взаимодействие органов повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, в том числе единых дежурно-диспетчерских служб и экстренных оперативных служб. Согласно решению администрации Субъекта РФ интеграции с ситемой-112 подлежат ДДС[2].

Целью реализации ПОИБ-112 является снижение вероятного ущерба от реализации угроз ИБ и выполнение требований законодательства Российской Федерации в части защиты информации системы-112.

ПОИБ-112 предназначена для защиты конфиденциальной информации, включая персональные данные, программного обеспечения и технических средств системы-112.

ПОИБ-112 обеспечивает следующие свойства защищаемой информации, обрабатываемой в системе-112:

доступность информации – возможность для авторизованного пользователя за приемлемое время получить доступ к информационному ресурсу в соответствии с установленными для этого пользователя правами доступа;

целостность – актуальность и непротиворечивость информации, защищенность информационного ресурса от разрушения и несанкционированного изменения в процессах передачи, обработки, хранения или представления;

конфиденциальность информации – защиту информационного ресурса от несанкционированного ознакомления, а также предотвращение утечки конфиденциальной информации по каналам связи.

1.3. Предмет и объект защиты

В системе-112 обрабатывается следующая информация:

данные о вызовах;

данные о лицах, осуществляющих вызовы;

---

[2] перечислить

данные о происшествиях;

данные об экстренных оперативных и дежурных службах, вызов которых осуществляется по номеру «112»;

данные о силах и средствах ДДС, осуществляющих экстренное реагирование;

рекомендации по действиям при типовых происшествиях;

данные о местности и состоянии среды;

данные по особо важным и опасным объектам;

статистическая информация, формируемая пользователями системы для получения различных групп отчетов;

другие данные.

Так же в системе-112 циркулирует информация, влияющая на целостность и устойчивость системы:

управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);

технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);

информационные ресурсы, содержащие информацию об информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в нештатных режимах;

служебные данные (метаданные), появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки информации.

В разработанной на стадии формирования требований к системе-112 частной модели угроз система-112 классифицируется как специальная распределенная информационная многопользовательская система класса К1 с разграничением прав доступа с доступом к сетям связи общего пользования, требования к информационной структуре системы-112 по защите от утечек по каналам побочных электромагнитных излучений и наводок не предъявляются.

Согласно частной модели нарушителя система-112 классифицируется как автоматизированная система класса 1Г и специальная информационная система персональных данных класса К1. Криптографические средства защиты информации, используемые для защиты конфиденциальных и иных охраняемых в соответствии с законодательством Российской Федерации сведений, в том числе персональных данных, обрабатываемых в системе-112, должны обеспечивать криптографическую защиту по уровню не ниже уровня КС2.

В системе-112 не обрабатывается информация, содержащая сведения, составляющие государственную тайну.

1.4. Функции подсистемы обеспечения информационной безопасности системы-112

Основные схемотехнические решения, структура системы информационной безопасности, состав средств защиты информации ПОИБ-112 и технологии защиты определяются:

функциями назначения системы-112;

структурой, составом и процессами функционирования ПТС системы;

моделью нарушителя и моделью угроз;

классом АС и требованиями безопасности в соответствии с РД ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Компоненты ПОИБ-112 комплексно выполняют следующие функции по защите информации, ориентированные на эффективное обеспечение информационной безопасности системы-112:

управления доступом;

регистрации и учета;

обеспечения целостности;

межсетевого экранирования;

криптографической защиты информации;

антивирусной защиты;

обнаружения вторжений;

анализа защищенности;

1.5. Сведения об использовании при проектировании нормативно-технических документов

Работы по созданию ПОИБ-112 проводятся в соответствии с федеральными законами, стандартами и действующими руководящими и нормативными документами уполномоченных органов исполнительной власти, основные из которых следующие:

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

Указ Президента Российской Федерации от 17 марта 2008 года N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

«Требования о защите информации, содержащейся в информационных системах общего пользования», утверждены Приказом ФСБ/ФСТЭК №416/489 от 31.08.2010 г.;

«Положение о методах и способах защиты информации в информационных системах персональных данных», утверждено приказом ФСТЭК №58 от 5.02.2010г.;

ГОСТ 34.601-90. «Автоматизированные системы. Стадии создания»;

ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;

ГОСТ Р 51583-2000. «Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;

ГОСТ 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;

ГОСТ Р 50922-96. «Защита информации. Основные термины и определения»;

ГОСТ Р 34.11-94. «Информационная технология. Криптографическая защита информации. Функция хеширования»;

ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

ГОСТ Р 50739-95. «Средства вычислительной техники. Средства вычислительной техники. Защита от НСД к информации. Общие технические требования»;

ГОСТ 50922-2006. «Защита информации. Основные термины и определения»;

ГОСТ 51583-2000. «Порядок создания АС в защищенном исполнении»;

«Положение о сертификации средств защиты информации по требованиям безопасности информации». Приказ Председателя Гостехкомиссии России от 27.10.1995 г. №199. Зарегистрировано Госстандартом России в Государственном реестре 20.03.1995 г. (Свидетельство №РОСС 1Ш.0001.01БИОС MS Windows SPR);

РД ФСТЭК России (Гостехкомиссии России). «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» от 30 марта 1992 г.;

РД ФСТЭК России (Гостехкомиссии России). «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», 1992 г.;

РД ФСТЭК России (Гостехкомиссии России). «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 года;

РД ФСТЭК России (Гостехкомиссии России). «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» от 30 марта 1992 г.;

РД ФСТЭК России (Гостехкомиссии России). «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» от 25 июля 1997 г.;

РД ФСТЭК России (Гостехкомиссии России). «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» от 4 июня 1999 г. № 114.;

РД ФСТЭК России (Гостехкомиссии России). «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)».

2. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ, ТРЕБОВАНИЯ К СИСТЕМЕ

2.1. Характеристика объекта информатизации

2.1.1 Общие сведения об объекте информатизации

Система-112 предназначена для информационного обеспечения единых дежурно-диспетчерских служб муниципальных образований.

Вызов экстренных оперативных служб обеспечивается каждому пользователю услугами связи посредством набора единого номера «112» либо номера, предназначенного для вызова соответствующей экстренной оперативной службы.

Основными целями создания системы-112 в Российской Федерации являются организация вызова экстренных оперативных служб по принципу «одного окна», организация комплекса мер, обеспечивающих ускорение реагирования и улучшение взаимодействия экстренных оперативных служб при вызовах (сообщениях о происшествиях) и реализация требований гармонизации способа вызова экстренных оперативных служб в Российской Федерации с законодательством Европейского союза.

Система-112 является территориально-распределенной автоматизированной информационно-управляющей системой, охватывает всю территорию Субъекта РФ. Система-112 функционирует в круглосуточном режиме и находится в постоянной готовности к организации экстренного реагирования на вызовы (сообщения о происшествиях).

Система-112 предназначена для выполнения следующих основных функций:

прием и обработка вызовов (сообщений о происшествиях) поступающих на единый телефонный номер «112» от населения и от сигнальных систем мониторинга опасных объектов;

передача в ДДС сообщений о вызовах с возможностью подключения их диспетчеров к разговорам с позвонившим лицом;

координация действий ДДС при реагировании на вызовы (сообщения о происшествиях);

организация оптимального использования сил и средств ДДС при реагировании на вызовы (сообщения о происшествиях);

поддержка единого информационного пространства для всего персонала и пользователей системы.

Система-112 предназначена для решения следующих основных 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 ДДС 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 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);

возможность приема вызовов (сообщений о происшествиях) на иностранных языках.

Коммуникационное оборудование системы-112 обеспечивает информационно-логическое взаимодействие компонентов системы на нескольких уровнях, а также взаимодействие между этими уровнями.

Коммуникационное оборудование включает:

медиашлюз;

кроссовое оборудование для оптических кабелей;

кроссовое оборудование для цифровых потоков;

оптические мультиплексоры;

модемы, использующие технологию xDSL.

маршрутизатор;

коммутатор.

АРМ пользователей включает:

системный блок, обеспечивающий подключение:

двух мониторов;

ручного манипулятора типа «мышь»;

клавиатуры;

двух линий ЛВС через разъем RG-45;

принтера через интерфейс USB 2,0;

гарнитуры;

два монитора;

IP-телефон;

телефонная гарнитура;

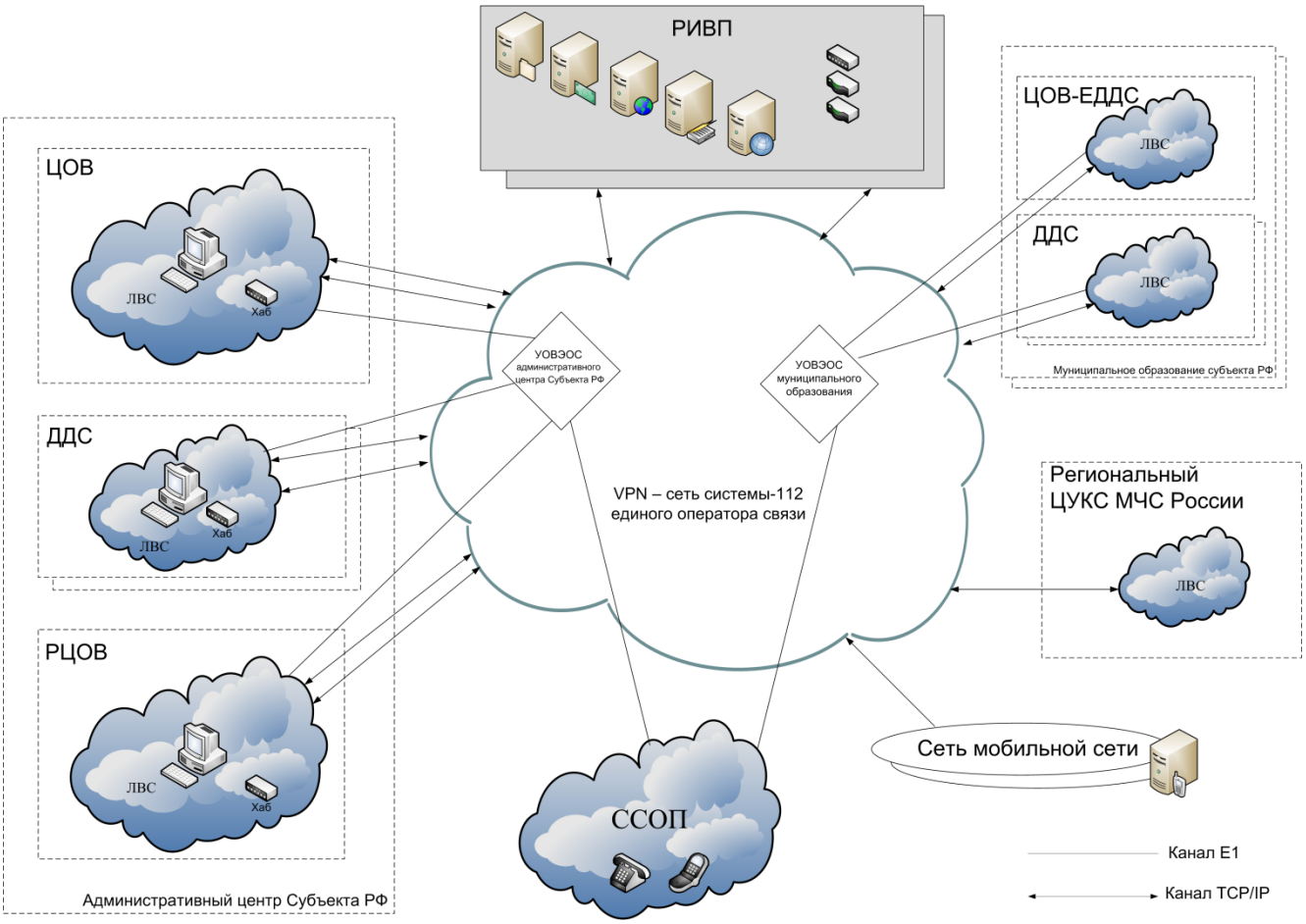
внутренний дополнительный сетевой адаптер с интерфейсом RG-45;

источник бесперебойного питания;

общесистемное, прикладное и специальное программное обеспечение;

принтер лазерный монохромный.

Обобщенная схема системы-112 представлена ниже.



2.1.2 Описание технологии обработки информации

Прием и обработка вызовов (сообщений о происшествиях) в системе-112 производится оператором ЦОВ-АЦ (РЦОВ) либо ЦОВ-ЕДДС (в соответствии с территориальной принадлежностью к зоне ответственности объекта) с применением средств автоматизации и включает:

диалог с заявителем, анализ и передачу характеристик происшествия (при необходимости перенаправление вызовов (сообщений о происшествиях)) в ДДС для непосредственного реагирования;

контроль за реагированием на происшествие, анализ и ввод в базу данных информации, полученной по результатам реагирования, уточнение и корректировку действий привлеченных ДДС, информирование взаимодействующих ДДС об оперативной обстановке, о принятых и реализуемых мерах;

размещение в информационной системе данных о ходе и об окончании мероприятий по экстренному реагированию на принятый вызов (сообщение о происшествии).

Все обращения в систему-112 регистрируются и, при необходимости, направляются дежурным диспетчерам соответствующих ДДС. Взаимодействие операторов ЦОВ-АЦ, РЦОВ и ЦОВ-ЕДДС с диспетчерами ДДС производится согласно регламенту информационного обмена и включает значительный объем информации. Информационную составляющую в целом определяет унифицированная карточка информационного обмена в системе-112. Процесс информационного обмена регламентируется соглашениями о взаимодействии, заключаемыми между ЦОВ-АЦ (РЦОВ), ЦОВ-ЕДДС и ДДС.

Диспетчеры ДДС при получении сообщений о происшествии выполняют меры по реагированию в соответствии с внутренними инструкциями службы и вводят в информационную систему (систему-112) уточненные данные по происшествию и информацию по реагированию на него.

На всех этапах обслуживания вызова происходит отслеживание изменения обстановки и статуса реагирования на происшествие, соответствующая актуализация информации (унифицированной карточки информационного обмена в системе-112). Закрытие унифицированной карточки информационного обмена в системе-112 происходит после завершения реагирования всех привлеченных ДДС.

Унифицированная карточка информационного обмена в системе-112 включает в том числе номер телефона абонента, позвонившего по телефону «112», данные об абоненте, адрес регистрации стационарного телефона.

2.1.3 Информационные связи системы

Для стыковки системы-112 с ССОП используются тракты Е1. Поток Е1 (речевые данные), с помощью медиашлюза преобразуется в вид, пригодный для передачи по IP сетям (SIP). Кроме преобразования речевой и сигнальной информации шлюз отвечает за поддержание некоторых характеристик QoS (качество обслуживания) при установлении соединения.

Объекты системы-112 связаны между собой VPN-сетью, образованной на базе инфраструктуры IP/MPLS-сети.

Информационный обмен между компонентами системы-112 осуществляется посредством:

единой БД системы-112;

специализированного интерфейса программирования приложений;

специализированных информационных сервисов.

Взаимодействие компонентов системы-112 с помощью специфицированных информационных сервисов обеспечивается средствами протокола SOAP, при этом каждый информационный сервис имеет доступную для других компонентов системы WSDL-

спецификацию интерфейса, и обеспечивает синтаксическую интероперабельность средствами XML формата данных и соответствует доступной для компонента XSD-схеме данных.

В системе-112 предусматривается обработка входных документов в электронном виде в XML-формате, выходных – в электронном виде в XML-формате или в бумажном виде по разработанным формам, утверждённым Заказчиком.

Связь системы-112 со смежными и внешними системами осуществляется по цифровым линиям связи в автоматическом режиме по IP-протоколам либо в ручном режиме по имеющимся средствам связи (в случае отсутствия технической возможности автоматического взаимодействия).

Совместимость системы-112 с другими системами и комплексами обеспечивается за счёт использования совместимого оборудования, протоколов, форматов, справочников и классификаторов данных.

Во всех случаях информационное взаимодействие со смежными и внешними системами осуществляется путем обмена документами и/или сообщениями в соответствии с регламентами, разработанными в процессе проектирования и закрепленными договорами и соглашениями с организациями-владельцами смежных (внешних) систем.

Все данные хранятся в единой БД системы-112, оборудование хранения данных находится на технологических площадках РИВП.

2.1.4 Объекты защиты

В рамках системы-112 к объектам защиты относятся следующие программно-технические средства:

АРМ пользователей системы-112;

коммутационное оборудование;

каналы передачи данных;

оборудование РИВП;

серверы резервирования ЦОВ-ЕДДС.

Обеспечение информационной безопасности РИВП осуществляется непосредственно подсистемой обеспечения информационной безопасности РИВП.

2.2. Требования к системе

Конкретные типы и версии СЗИ должны выбираться с учетом требований по наличию сертификатов соответствия реализованных в них функций безопасности, включая СКЗИ, которые могут использоваться для выполнения требований защищенности в соответствии с моделями угроз и нарушителя. Исходя из соображений обеспечения наилучшей производительности и возможности создания отказоустойчивого решения, ПОИБ-112 должна представлять собой комплекс программно-технических, организационных и правовых мер, обеспечивающих:

защиту от несанкционированного доступа к программно-аппаратным средствам и информации системы-112;

регистрацию и учёт активности пользователей и программного обеспечения;

разграничение доступа к данным и функциям системы зарегистрированных пользователей;

защиту от вредоносного программного обеспечения;

межсетевое экранирование при взаимодействии системы-112 с другими информационными системами и информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры системы;

обнаружение вторжений, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности защищаемой информации, в т. ч. и ПДн;

анализ защищенности, предполагающий применение специализированных средств;

криптографическую защиту при передаче информации по сетям передачи данных.

3. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ ПОДСИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ-112

На основе анализа моделей угроз и нарушителя системы-112, функциональных характеристик сертифицированных средств защиты информации и технического задания на создание системы-112 были разработаны описанные ниже технические решения, реализующие модель защиты и функции назначения. Для защиты информации в системе-112 предусмотрены следующие элементы защиты информации:

межсетевой экран с функцией криптошлюза ViPNet Coordnator HW;

СЗИ от НСД Secret Net 6;

средство обнаружения вторжений Security Studio Endpoint Protection HIPS;

средство анализа защищенности «Сканер-ВС»;

штатные средства управления доступом СУБД и ОС;

организационные меры защиты.

Остальные средства защиты информации входят в состав систем, предоставляющих внешние сервисы информационной безопасности для ПОИБ-112. К этим системам относятся подсистема обеспечения информационной безопасности РИВП, сервисы ИБ смежных и внешних систем.

3.1 Компоненты подсистемы обеспечения информационной безопасности системы-112

ПОИБ-112 предназначена для обеспечения защиты информации от действующих угроз информационной безопасности в соответствии с моделью угроз и моделью нарушителя системы вызова экстренных оперативных служб через единый номер «112».

Основными целями обеспечения информационной безопасности является поддержка и сохранение таких свойств информации, как конфиденциальность, целостность и доступность информации в системе-112. ПОИБ-112 представляет собой комплекс организационно-режимных мероприятий, документированных процедур, технических средств защиты информации, включая средства криптографической защиты информации, а также технологий их применения, и, исходя из модели угроз и вероятного нарушителя информационной безопасности, структурно ПОИБ-112 включает в себя следующие функциональные блоки (компоненты):

управления доступом;

регистрации и учета;

криптографической защиты;

обеспечения целостности;

защиты от вредоносного ПО;

межсетевого экранирования;

обнаружения вторжений;

анализа защищенности.

Управление доступом (разграничение доступа) предназначено для защиты информационных ресурсов системы-112 от несанкционированного доступа к ним. Основными средствами управления доступом являются средства идентификации и аутентификации пользователей. Задачей идентификации и аутентификации является определение и верификация пользователей при доступе к системе по его уникальному идентификатору и/или ключу. При этом необходимо запретить доступ к защищаемым ресурсам пользователей, не прошедших процедуру идентификации и аутентификации.

Назначение функции регистрации и учёта показателей состояния информационной безопасности заключается в обеспечении хранения, обработки данных журналов безопасности и визуализации событий безопасности. Регистрация и учёт показателей состояния информационной безопасности обеспечивается за счет обработки данных журналов безопасности и анализа событий безопасности. Администратору безопасности предоставляется возможность просмотра и анализа событий безопасности системы с его рабочего места. Контроль содержания журналов безопасности должен обеспечить обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение принятых требований в части безопасности информации и привести к возникновению инцидентов безопасности. Результаты регистрации обеспечивают управление информационной безопасностью.

Криптографическая защита информационного обмена предназначена для защиты конфиденциальной информации пользователей при ее передаче по IP/MPLS-сети оператора РИВП.

Обеспечение целостности призвано предотвратить несанкционированное изменение системных файлов операционных систем и прикладного ПО, помешать внедрению и установке посторонних программ или других программных компонентов.

Защита от вредоносного ПО призвана контролировать все потенциальные источники проникновения компьютерных вирусов, выявлять и удалять вирусы, которые могут присутствовать в ресурсах системы.

Одними из основных элементов защиты ресурсов от НСД на сетевом уровне является межсетевое экранирование, основанное на принципах фильтрации сетевых пакетов на основе адресной и другой информации, содержащейся в них. Эта технология предназначена для защиты одной сети от несанкционированного доступа к информации из другой сети.

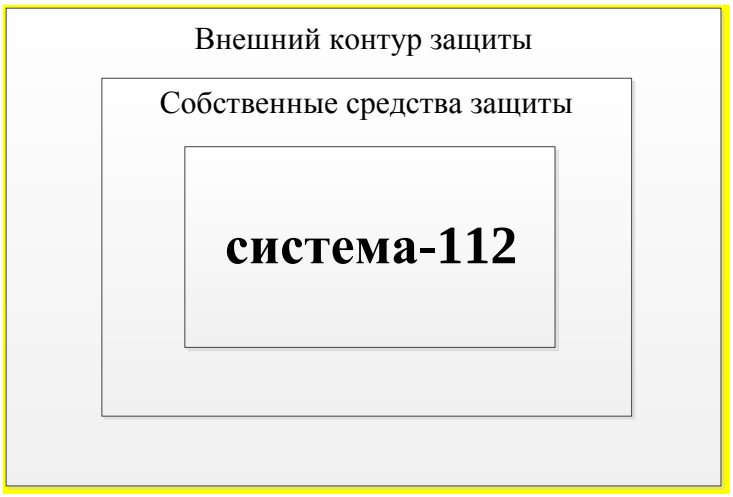
Обнаружение вторжений заключается в контроле всего разрешенного информационного обмена между ресурсами системы-112, выявлении и предотвращении удаленного программного воздействия на ресурсы системы-112.

Функциональные блок анализа защищенности призвана контролировать уровень защищенности ресурсов системы, выявлять имеющиеся уязвимости в системном и прикладном ПО системы-112 и своевременно устранять их.

3.2 Общее описание функционирования подсистемы обеспечения информационной безопасности системы-112

3.2.1 Архитектура

Общая архитектура ПОИБ-112 представлена на следующем рисунке.



ПОИБ-112 использует следующие средства защиты:

«наложенные» средства защиты информации (далее - СЗИ), СЗИ, входящие в состав только ПОИБ;

механизмы защиты, встроенные в программное обеспечение функциональных подсистем системы-112;

сервисы информационной безопасности, предоставляемые сторонними, внешними и смежными автоматизированными системами, эксплуатируемыми Заказчиком.

В качестве указанных автоматизированных систем, предоставляющих сервисы ИБ, выступают подсистема обеспечения информационной безопасности РИВП, иные автоматизированные системы[3].

Таким образом, часть функций безопасности предоставляется системе внешними сервисами, остальная реализуется собственными и «наложенными» средствами защиты информации. Использование данных средств защиты в совокупности обеспечивает выполнение всех требований к ПОИБ-112, определенных Техническим заданием на создание системы-112.

Для построения ПОИБ-112 используется комплексный подход к защите информации, который заключается в рациональном сочетании различных организационных и программно-технических мер и средств с учетом требований действующих нормативно-правовых и

[3] указать

нормативно-технических документов, что позволит выработать системное техническое решение по обеспечению безопасности информации в системе-112, учесть технологии и специфику функционирования объекта автоматизации. Это решение, наряду с использованием дополнительных сертифицированных средств защиты информации, применяет штатные защитные механизмы СУБД, операционных систем и телекоммуникационного оборудования. Данный подход позволяет сделать ПОИБ-112 более гибкой и масштабируемой.

Архитектура и технические решения по ПОИБ-112 учитывают необходимость минимизировать накладные расходы, связанные с созданием, настройкой, эксплуатацией и развитием предлагаемых технических решений по защите в рамках требований российского законодательства и нормативных требований федеральных регулирующих органов в области защиты информации. Это достигается за счет:

использования унифицированных и стандартизированных решений по защите информации;

применения апробированных на практике и рекомендованных к применению решений по защите информации;

использования передовых технологий защиты по созданию защищенных АС;

использования встроенных механизмов защиты системного и прикладного программного обеспечения АС;

учета перспектив развития современных информационных технологий;

оптимизации материальных и финансовых затрат.

3.2.2 Структура

Защита системы-112 строится с использованием внешних сервисов информационной безопасности, «наложенных» средств защиты, входящих в ПОИБ-112, а также штатных средствами безопасности системного и прикладного ПО системы.

В качестве внешних сервисов используются подсистема обеспечения информационной безопасности РИВП, сервисы ИБ.

ПОИБ-112 непосредственно реализует функции межсетевого экранирования и криптозащиты при взаимодействии с внешними и смежными системами и РИВП, защиты от вредоносного ПО, защиты и обнаружения вторжений и защиты от несанкционированного доступа, включая как защиту от угроз непосредственного физического доступа к техническим средствам, так и управление доступом пользователей к информации, размещаемой в системе.

При этом функции по защите от несанкционированного доступа и целостности реализуются при помощи организационно-технических мер, так и с использованием сертифицированных ФСТЭК России СЗИ от НСД.

3.2.3 Обобщённая модель защиты

Весь информационный обмен в рамках системы-112 осуществляется с использованием VPN-туннелей, обеспечивающих криптографическую защиту информации с использованием алгоритма ГОСТ 28147-89.

Трафик взаимодействия системы-112 с внешними и смежными системами, а также расшифрованный трафик дополнительно проверяется и контролируется средствами межсетевого экранирования и средствами защиты от сетевых атак, направленных на систему-112.

Идентификация и аутентификация пользователей при доступе к ресурсам системы-112, а также распределение доступа пользователей к информации в системе осуществляется при помощи сертифицированных ФСТЭК России СЗИ от НСД и штатными средствами прикладного ПО системы-112 в соответствии с матрицей доступа. Доступ к ресурсам получают только те пользователи, которые успешно прошли данную процедуру.

Все действия пользователей в системе-112 регистрируются с помощью штатных средств операционных систем, СУБД и сертифицированных ФСТЭК России СЗИ от НСД.

С целью контроля защищенности ресурсов системы-112 и выявления уязвимостей прикладного и системного ПО, ПТС системы осуществляется их регулярное сканирование с использованием сертифицированных ФСТЭК России средств анализа защищенности.

Защита АРМ пользователей системы-112 от вредоносного программного обеспечения обеспечивается применением на них антивирусного ПО.

3.3 Состав подсистемы обеспечения информационной безопасности системы-112

3.3.1 Подсистема управления доступом

Управление и разграничение доступа пользователей к информации в системе, реализуется при помощи СЗИ от НСД Secret Net 6, а также с использованием штатных средств системы-112 в соответствии с матрицей доступа.

Система Secret Net 6 совместно с ОС семейства Windows обеспечивает идентификацию и аутентификацию пользователя с помощью программно-аппаратных средств при его входе в систему.

Функция управления доступом пользователей к конфиденциальной информации, реализованные в СЗИ от НСД Secret Net, позволяют каждому информационному ресурсу назначить один их трёх уровней конфиденциальности: «Не конфиденциально», «Конфиденциально», «Строго конфиденциально», а каждому пользователю – уровень допуска. Доступ осуществляется по результатам сравнения уровня допуска с категорией конфиденциальности информации.

СЗИ от НСД Secret Net обеспечивает разграничение доступа к устройствам с целью предотвращения несанкционированного копирования информации с защищаемого компьютера.

Существует возможность запретить, либо разрешить пользователям работу с любыми портами/устройствами.

Разграничивается доступ к следующим портам/устройствам:

последовательные и параллельные порты;

сменные, логические и оптические диски;

USB-порты.

Поддерживается контроль подключения устройств на шинах USB, PCMCIA, IEEE1394 по типу и серийному номеру, права доступа на эти устройства задаются не только для отдельных пользователей, но и для групп пользователей.

Также существует возможность запретить использование сетевых интерфейсов — Ethernet, 1394 FireWire, Bluetooth, IrDA, Wi-Fi.

Для каждого пользователя компьютера СЗИ от НСД Secret Net позволяет сформировать определённый перечень программ, разрешенных для запуска. Он может быть задан как индивидуально для каждого пользователя, так и определен на уровне групп пользователей. Применение этого режима позволяет исключить распространение вирусов, «червей» и шпионского ПО, а также использования АРМ в качестве игровой приставки.

Ограничение доступа к техническим средствам АРМ пользователей системы-112 реализуется при помощи организационно-технических мер, включающими в себя опечатывание АРМ.

3.3.2 Подсистема регистрации и учета

Регистрация и учет действий пользователей к информации в системе, реализуется при помощи СЗИ от НСД Secret Net 6, а также с использованием штатных средств системы-112 в соответствии с матрицей доступа.

Система Secret Net 6 регистрирует все события, происходящие на компьютере: включение/выключение компьютера, вход/выход пользователей, события НСД, запуск приложений, обращения к конфиденциальной информации, контроль вывода конфиденциальной информации на печать и отчуждаемые носители и т.п.

3.3.3 Подсистема обеспечения целостности

Для слежения за неизменностью контролируемых объектов с целью защиты их от модификации используется контроль целостности, который проводится при помощи СЗИ от НСД Secret Net 6 в автоматическом режиме в соответствии с некоторым заданным расписанием.

Объектами контроля могут быть файлы, каталоги, элементы системного реестра и секторы дисков. Каждый тип объектов имеет свой набор контролируемых параметров. Так, файлы могут контролироваться на целостность содержимого, прав доступа, атрибутов, а также на их существование, т.е. на наличие файлов по заданному пути. При обнаружении

несоответствия предусмотрены следующие варианты реакции на возникающие ситуации нарушения целостности:

регистрация события в журнале Secret Net;

блокировка компьютера;

восстановление повреждённой/модифицированной информации;

отклонение или принятие изменений.

Перед входом пользователя в систему производится функциональный самоконтроль подсистем, который предназначен для обеспечения гарантии того, что к моменту завершения загрузки ОС все ключевые компоненты Secret Net 6 загружены и функционируют.

В СЗИ от НСД Secret Net 6 реализована функция контроля вывода конфиденциальной информации на печать. Так, при разрешённом выводе конфиденциальной информации на печать документы автоматически маркируются в соответствии с принятыми в организации стандартами. Факт печати отображается в журнале защиты Secret Net 6.

Уничтожение данных в Secret Net 6 достигается путем записи случайной последовательности на место удаленной информации в освобождаемую область диска. Для большей надежности может быть выполнено до 10 циклов (проходов) затирания.

3.3.4 Подсистема межсетевого экранирования

В качестве средств межсетевого экранирования предполагается использование программно-аппаратного комплекса ViPNet Coordinator HW.

ПАК ViPNet Coordinator HW представляет собой интегрированное решение на базе нескольких аппаратных платформ и программного обеспечения производства ОАО "Инфотекс", предназначенное для организации сетевой защиты в VPN-сетях. В качестве аппаратной платформы используется компактный компьютер или полноценный сервер, устанавливаемый в стандартные коммутационные шкафы:

в РИВП - ПАК ViPNet Coordinator HW2000 на базе серверов AquaServer T50 D55 в отказоустойчивом кластере;

в ЦОВ-АЦ (РЦОВ) - ПАК ViPNet Coordinator HW1000 на базе серверов AquaServer T40 S42 в отказоустойчивом кластере;

в ЦОВ-ЕДДС и ДДС - ПАК ViPNet Coordinator HW100 на базе мини-компьютера серии eBox-4.

В состав всех разновидностей ПАК ViPNet Coordinator HW входит программное обеспечение ViPNet Coordinator Linux, которое является одним из программных продуктов семейства ViPNet CUSTOM Linux и обеспечивает следующую основную функциональность комплекса:

криптошлюза для организации защищенных туннелей в рамках виртуальной частной сети ViPNet;

межсетевого экрана;

сервера IP-адресов виртуальной частной сети ViPNet (поддержка работы удаленных мобильных пользователей и любых других узлов сети с динамическими IP-адресами);

сервера-маршрутизатора почтовых конвертов.

Для создания отказоустойчивого кластера на базе ПАК ViPNet Coordinator HW1000/2000 в ПО ViPNet Coordinator Linux реализована технология горячего резервирования комплексов, объединенных в кластер. В случае выхода из строя одного из комплексов, входящих в кластер, переключение на второй (резервный) комплекс происходит автоматически без вмешательства администратора. ПО ViPNet Coordinator Linux в составе комплекса функционирует под управлением адаптированной ОС Linux.

3.3.5 Подсистема обнаружения вторжений

Средства обнаружения вторжений призваны контролировать трафик информационного обмена системы-112 на предмет наличия в нем запрещенного контента, используемого для осуществления атак на web приложения.

В качестве системы обнаружения вторжений для системы-112 было выбрано Security Studio Endpoint Protection. Данное СЗИ обеспечивает защиту компьютера с применением межсетевого экрана, антивируса и средства обнаружения вторжений. Обеспечивает безопасную и комфортную работу с сетью Интернет, предотвращая любые попытки проникновения на компьютер вредоносного ПО и блокируя нежелательный трафик.

Некоторые вредоносные приложения могут внедряться в легальные программы и осуществлять свои действия от имени доверенных приложений. Это в свою очередь может привести к утечке информации или к тому, что злоумышленнику удастся получить полный контроль над вашей системой.

Компоненты "Детектор атак" и "Локальная безопасность", входящий в состав Security Studio Endpoint Protection, не допускают действия таких программ и таким образом полностью защищает вас от троянов, шпионского ПО и неизвестных на данный момент угроз.

Детектор атак защитит от таких действий, как DDoS-атаки, IP-spoofing, ARP-флуд – попытка подвесить систему; предотвращает подмену IP- и MAC-адреса. Защитит от ложных сообщений "IP-адрес уже занят". Можно задать поведение системы при обнаружении атак, установив требуемый уровень тревоги. Также можно настроить механизм визуальных и звуковых оповещений об обнаруженных атаках.

Модуль "Локальная безопасность" реализует защиту от атак — контролирует взаимодействие программ, предотвращая неизвестные или подозрительные операции, и таким образом защищает компьютер от нераспознаваемых угроз. Такие угрозы возникают, когда вредоносные приложения внедряются в легальные программы и действуют от имени доверенных приложений. Например, некоторые вирусы могут внедриться в компьютерную

систему под видом модуля легальной программы (например, стандартного браузера) и таким образом получить привилегии для соединения с компьютером хакера. Другие программы могут запустить процесс в скрытом режиме или захватить память доверенного процесса.

Применяя технологии контроля компонентов, контроля утечек (Anti-Leak) и контроля критических системных объектов, механизм локальной безопасности обеспечивает первую линию обороны от вредоносного ПО, проактивно контролируя поведение и взаимодействие приложений на компьютере.

Сертификат № 2170 ФСТЭК России удостоверяет, что средство защиты информации Security Studio Endpoint Protection Firewall является программным средством защиты от несанкционированного доступа к информации, соответствует требованиям руководящего документа "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" (Гостехкомиссия России, 1999) – по 4 уровню контроля, «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации», (Гостехкомиссия России, 1997) – по 4 классу защищенности и уровню контроля, а также может использоваться для создания автоматизированных систем до класса защищенности 1Г включительно и для защиты информации в информационных системах персональных данных до 1 класса включительно;

Сертификат № 2171 ФСТЭК России удостоверяет, что средство защиты информации Security Studio Endpoint Protection HIPS является программным средством, предназначенным для обнаружения вторжений из внешних вычислительных сетей, соответствует требованиям руководящего документа "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" (Гостехкомиссия России, 1999) – по 4 уровню контроля, «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации», (Гостехкомиссия России, 1997) – по 4 классу защищенности и уровню контроля, а также может использоваться для создания автоматизированных систем до класса защищенности 1Г включительно и для защиты информации в информационных системах персональных данных до 1 класса включительно.

3.3.6 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.

В качестве средства анализа защищенности для системы-112 был выбран Сканер-ВС.

Система комплексного анализа защищенности «Сканер-ВС» - это загрузочный DVD с операционной системой и предустановленным программным обеспечением для комплексного тестирования защищенности информационных систем.

САЗ «Сканер-ВС» позволяет:

производить определение топологии сети, инвентаризацию ресурсов сети, котролировать появление сетевых сервисов;

производить сканирование сетевых сервисов на известные уязвимости;

производить локальный и сетевой аудит стойкости паролей. Сканер-ВС содержит мощные средства локального аудита паролей для операционных систем семейства Windows (NT, 2000, 2003, 2008, XP, Vista, 7) и Linux (МСВС, Linux XP, Astra Linux и др.). Сканер-ВС поддерживает возможность подбора паролей по более чем 20-ти сетевым протоколам (HTTP, SMTP, POP, FTP, SSH и др);

производить поиск остаточной информации на жестком диске. В Сканер-ВС включено средство для поиска остаточной информации на жестких дисках и других носителях вне зависимости от файловой структуры;

перехватить всю передаваемую информацию между любыми узлами коммутируемой сети (с помощью технологии ARP-спуфинга) и выполнить ее анализ, в том числе извлечь переданные пароли. Возможен перехват шифрованного трафика (HTTPS) с помощью подмены сертификата;

получить информацию об аппаратной конфигурации системы и установленном программном обеспечении, а также перечень USB-устройств, подключавшихся к компьютеру;

рассчитывать контрольные суммы по алгоритмам CRC32, ГОСТ Р 34.11-94, MD5;

проводить аудит парольной защиты WI-FI сетей с помощью модуля анализа защищенности беспроводных (WI-FI) сетей;

с помощью модуля гарантированной очистки информации на носителях производит многократное затирание файлов по определенному алгоритму, что приводит к невозможности восстановления информации.

Использование системы позволяет выполнить требования многочисленных нормативных документов, определяющих необходимость проведения контроля эффективности средств защиты информации (Постановление Правительства Российской Федерации 2012 г. №1119, приказ ФСТЭК России 2013 г., Руководящий документ Гостехкомиссии России “Концепция защиты СВТ и АС от НСД к информации”).

Система комплексного анализа защищенности «Сканер-ВС» имеет следующие сертификаты:

Минобороны России № 631 на соответствие Приказу МО РФ, в том числе: требованиям руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к

информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999 г. - по второму уровню контроля; требованиям по соответствию реальных и декларируемых в документации функциональных возможностей;

ФСТЭК России №2204 от 13 ноября 2010 г. на соответствие требованиям: руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Классификация по уровню контроля отсутствия недекларированных возможностей» – по четвертому уровню контроля; технических условий НПЭШ.00606-01 ТУ.

3.3.7 Подсистема обеспечения антивирусной защиты

Подсистема обеспечения антивирусной защиты призвана контролировать все потенциальные источники проникновения компьютерных вирусов, выявлять и удалять вирусы, которые могут присутствовать в ресурсах системы.

В качестве средства антивирусной защиты для системы-112 было выбрано Security Studio Endpoint Protection.

Антивирусные и антишпионские возможности данного продукта совмещены в одном компоненте для защиты компьютера от любых вредоносных программ, представляющих угрозу системе во время навигации в сети. Быстрый и эффективный сканер, сочетающий антивирус (аттестованный Virus Bulletin) и антишпион, автоматически обнаруживает и обезвреживает или удаляет вредоносное ПО. Монитор доступа защищает компьютер от попыток проникновения и активации вредоносных программ.

В режиме постоянной защиты компонент "Антивирус+Антишпион" обеспечивает защиту от шпионских программ и вирусов в реальном времени. Можно настроить вывод визуальных и звуковых оповещений при обнаружении угроз. Запуск процесса сканирования может быть задан по расписанию.

В компонент "Антивирус+Антишпион" входит также почтовый сканер, проверяющий файлы, прикрепленные к электронным письмам.

Сертификат № 2166 ФСТЭК России удостоверяет, что средство защиты информации Security Studio Endpoint Protection Antivirus является программным средством антивирусной защиты, соответствует требованиям руководящего документа "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" (Гостехкомиссия России, 1999) – по 4 уровню контроля и требованиям технических условий, а также может использоваться для создания автоматизированных систем

до класса защищенности 1Г включительно и для защиты информации в информационных системах персональных данных до 1 класса включительно.

3.3.8 Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для осуществления защиты информационного обмена - для защиты конфиденциальной информации пользователей при ее передаче по IP/MPLS-сети оператора РИВП.

В качестве криптошлюза предусматривается использование программно-аппаратного комплекса ViPNet Coordinator HW.

В состав всех разновидностей комплекса входит программное обеспечение (ПО) ViPNet Coordinator Linux, которое является одним из программных продуктов семейства ViPNet CUSTOM Linux и обеспечивает возможность создания криптошлюза для организации защищенных туннелей в рамках виртуальной частной сети ViPNet.

3.4 Состав СЗИ на объекте защиты

Комплекс СЗИ в ПОИБ-112 включает:

ПАК ViPNet Coordinator HW1000 – по 2 единицы в ЦОВ-АЦ и РЦОВ;

ПАК ViPNet Coordinator HW100 – по 1 единице в каждом в ЦОВ-ЕДДС и ДДС;

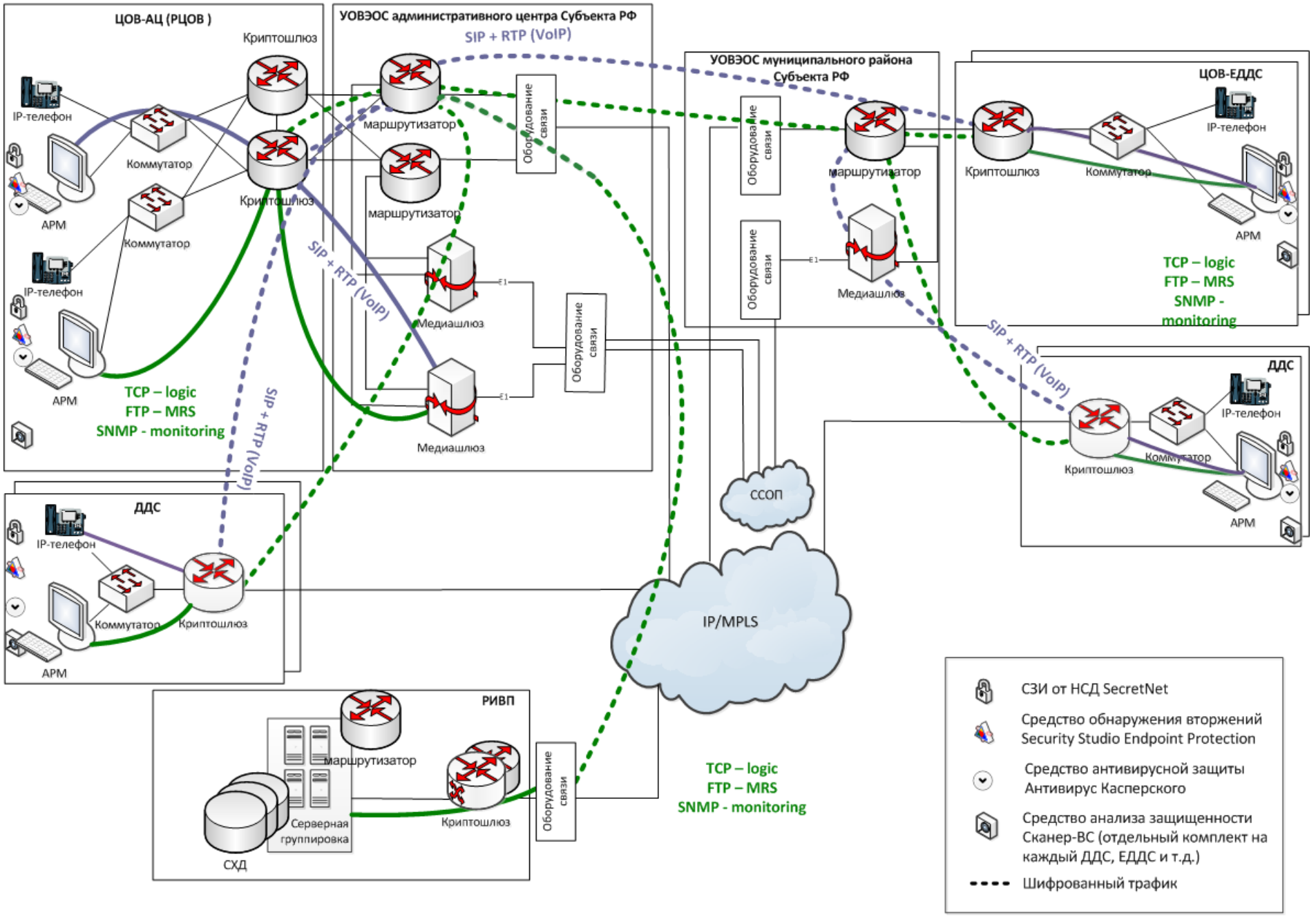
ПО Security Studio Endpoint Protection – по 1 единице на каждом АРМ ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС и ДДС, включенных в VPN-сеть системы-112;

СЗИ от НСД Secret Net 6 – по 1 единице на каждом АРМ ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС и ДДС, включенных в VPN-сеть системы-112;

средство анализа защищенности «Сканер-ВС» – по 1 единице в ЦОВ-АЦ, РЦОВ, каждом в ЦОВ-ЕДДС и ДДС.

Схема подключения СЗИ на объектах системы-112 приведена ниже.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата



Изм	Лист	№ документа	Подпись	Дата

4. МЕРОПРИЯТИЯ ПО ПОДГОТОВКЕ ОБЪЕКТОВ АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ-112 В ДЕЙСТВИЕ

Перечень конкретных мероприятий по вводу подсистемы обеспечения информационной безопасности объекта системы-112 определяется с учетом конфигурации и состава технических средств объекта и уровнем подготовки имеющегося персонала.

4.1 Мероприятия по созданию необходимых подразделений и рабочих мест

На ЦОВ-АЦ на технического специалиста, входящего в состав дежурной смены, возлагается выполнение обязанностей администратора информационной безопасности.

Администратор информационной безопасности должен иметь квалификацию, необходимую для настройки ПАК ViPNet Coordnator HW, ПО Security Studio Endpoint Protection, СЗИ от НСД Secret Net 6, средства анализа защищенности «Сканер-ВС». Администратор информационной безопасности должен знать и выполнять требования действующего законодательства в области защиты информации.

Пользователи должны быть проинструктированы о работе с ПО Security Studio Endpoint Protection, СЗИ от НСД Secret Net 6.

4.2 Мероприятия по изменению объекта автоматизации

При подготовке каждого объекта автоматизации необходимо провести комплекс организационно-технических мероприятий.

В результате данных мероприятий:

должна быть исключена возможность бесконтрольного проникновения в помещения, в которых установлены технические средства системы-112, посторонних лиц и обеспечена физическая сохранность находящихся в помещении защищаемых ресурсов (технических средств, документов и т.п.);

размещение и установка технических средств должна производиться с учетом необходимости исключения возможности визуального просмотра вводимой (выводимой) информации лицами, не имеющими к ней отношения;

должны быть приняты меры, не позволяющие применять средства удаленного наблюдения;

АРМ пользователей системы-112 должны иметь возможность опечатывания;

на всех АРМ системы должна быть проведена настройка ОС на блокировку рабочего стола по истечении не более 10 минут бездействия пользователя.