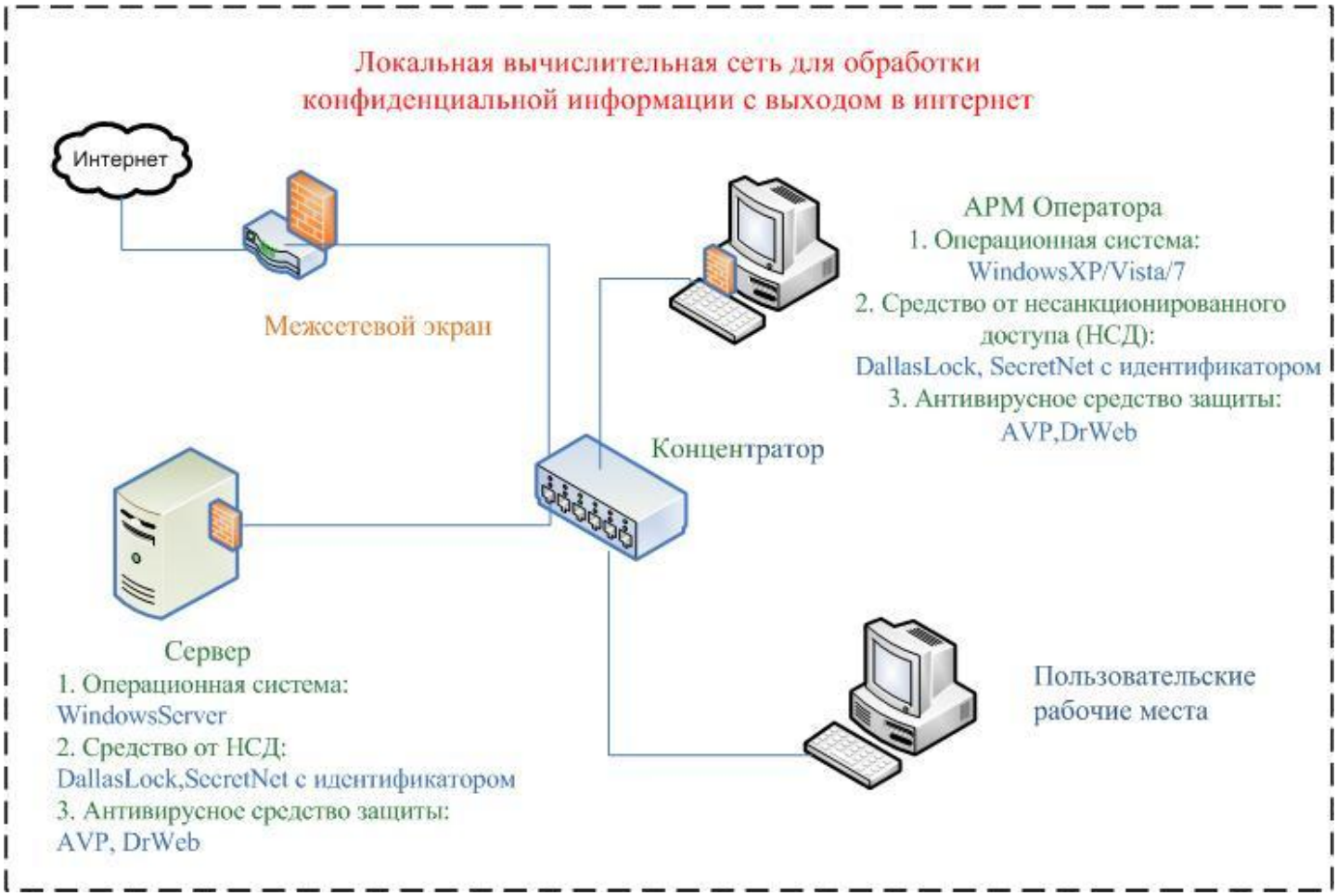
Локальная вычислительная сеть для обработки конфиденциальной информации, имеющая выход во внешнюю сеть или Интернет.

Локальная вычислительная сеть для обработки конфиденциальной информации, сопряженная с Интернет, представляет собой автоматизированную систему, построенную на базе локальной вычислительной сети, имеющей взаимодействие с информационно-телекоммуникационной сетью международного информационного обмена Интернет, в которой может производиться обработка какой-либо информации ограниченного распространения (за исключением государственной тайны) – служебная тайна, коммерческая тайна, банковская тайна и т.д.



Условия эксплуатации АС:

- Режим обработки информации – многопользовательский;
- В АС пользователи имеют различный уровень полномочий на доступ к защищаемым ресурсам АС;
- В АС хранится и обрабатывается информация разного уровня конфиденциальности "служебная или коммерческая тайна".
- АС взаимодействует с информационно-телекоммуникационными сетями международного информационного обмена

В соответствии с (РД АС) руководящим документом "Автоматизированные системы, защита от несанкционированного доступа к информации классификация автоматизированных систем и требования по защите информации" определяется класс защищенности АС.

В качестве средств защиты в автоматизированной системе выступает программное обеспечение общего назначения со встроенными механизмами защиты, сертифицированными по требованиям безопасности ФСТЭК России:

- Сертифицированная серверная операционная система Microsoft Windows Server;
- Сертифицированная операционная система Windows Vista или XP;
- Сертифицированный Антивирус Касперского 6.0 для Windows WorkStations или Антивирус Dr.Web;
- Сертифицированное средство контроля и протоколирования доступа пользователей к устройствам и портам ввода-вывода DallasLock или SecretNet, позволяющий контролировать

весь спектр потенциально опасных устройств: USB-порты, дисководы, CD/DVD-приводы, а также FireWire, инфракрасные, параллельные и последовательные порты, WiFi и Bluetooth-адаптеры, ленточные накопители, КПК, любые внутренние и внешние сменные накопители и жесткие диски;

- Сертифицированный межсетевой экран (МЭ), обеспечивающий межсетевое экранирование с интегрированными сервисами, защищающий информационную среду от угроз, поступающих через Интернет, и одновременно обеспечивающий быстрый и безопасный удаленный доступ к приложениям и данным.

Перечень требований РД АС и их реализация сертифицированным программным обеспечением для АРМ Оператора приведен в таблице 1.

Таблица 1.

Требование РД АС	Средства, обеспечивающие выполнение требований РД
1. ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ	
Идентификация, проверка под-линности и контроль доступа субъектов: в систему, к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройст-вам ЭВМ к программам к томам, каталогам, файлам, записям, полям записей.	Механизмы идентификация и аутентификация: - ОС Windows Vista/XP, - средства контроля и протоколирования доступа пользователей DallasLock или SecretNet;
2. ПОДСИСТЕМА РЕГИСТРАЦИИ И УЧЕТА	
2.1. Регистрация и учет:: входа (выхода) субъектов доступа в (из) систему (узел сети); выдачи печатных (графических) вы-ходных документов запуска (завершения) программ и процессов (заданий, задач) доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, запи-сям, полям записей.	Механизмы аудита безопасности: - ОС Windows Vista/ XP. - средства контроля и протоколирования доступа пользователей DallasLock или SecretNet.
2.2. Учет носителей информации	Реализуется с помощью организационно-распорядительных мероприятий. Как правило ведется «Журнал учета машинных носителей»), в котором регистрируются все машинные носители информации АС.
2.3. Очистка (обнуление, обезличива-ние) освобождаемых областей оперативной памяти ЭВМ и внеш-них накопителей.	Механизм безопасности защита данных пользователя ОС Microsoft Windows Vista/XP. Очистка внешних накопителей обеспечивается пользователями и Администратором безопасности в соответствии с инструкциями и должностными обязанностями.
3. ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ	
3.1. Обеспечение целостности про-граммных средств и обрабатываемой информации:	Отсутствие на ПЭВМ (серверах) средств разработки исполняемых модулей программного обеспечения. Антивирус Касперского или Dr.Web.
3.2. Физическая охрана средств вы-числительной техники и носителей информации.	Реализуется с помощью организационно-распорядительных мероприятий.
3.3. Периодическое тестирование СЗИ НСД.	ОС Microsoft Windows Vista/XP;

Требование РД АС	Средства, обеспечивающие выполнение требований РД
	Антивирус Касперского или Dr.Web. С помощью организационно-распорядительных мероприятий.
3.4. Наличие средств восстановления СЗИ НСД.	Средство резервного копирования и восстановления ОС.

Перечень требований РД АС и их реализация сертифицированным программным обеспечением, применительно к серверу контролеру домена и файлового сервера, приведен в таблице 2.

Таблица 2.

Требование РД АС	Средства, обеспечивающие выполнение требований РД
1. ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ	
Идентификация, проверка под-линности и контроль доступа субъектов: в систему, к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройст-вам ЭВМ к программам к томам, каталогам, файлам, записям, полям записей.	Механизмы идентификация и аутентификация: - серверной ОС Microsoft Windows Server, - средства контроля и протоколирования доступа пользователей DallasLock или SecretNet;
2. ПОДСИСТЕМА РЕГИСТРАЦИИ И УЧЕТА	
2.1. Регистрация и учет:: входа (выхода) субъектов доступа в (из) систему (узел сети); выдачи печатных (графических) вы-ходных документов запуска (завершения) программ и процессов (заданий, задач) доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, запи-сям, полям записей.	Механизмы аудита безопасности: - серверной ОС Microsoft Windows Server. - средства контроля и протоколирования доступа пользователей DallasLock или SecretNet.
2.2. Учет носителей информации	Реализуется с помощью организационно-распорядительных мероприятий. Как правило ведется «Журнал учета машинных носителей»), в котором регистрируются все машинные носители информации АС.
2.3. Очистка (обнуление, обезличива-ние) освобождаемых областей оперативной памяти ЭВМ и внеш-них накопителей.	Механизм безопасности защита данных пользователя ОС серверной ОС Microsoft Windows Server. Очистка внешних накопителей обеспечивается пользователями и Администратором безопасности в соответствии с инструкциями и должностными обязанностями.
3. ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ	
3.1. Обеспечение целостности про-граммных средств и обрабатываемой информации:	Отсутствие на ПЭВМ (серверах) средств разработки исполняемых модулей программного обеспечения. Антивирус Касперского или Dr.Web.
3.2. Физическая охрана средств вы-числительной техники и носителей информации.	Реализуется с помощью организационно-распорядительных мероприятий.

Требование РД АС	Средства, обеспечивающие выполнение требований РД
3.3. Периодическое тестирование СЗИ НСД.	серверной ОС Microsoft Windows Server; Антивирус Касперского или Dr.Web. С помощью организационно-распорядительных мероприятий.
3.4. Наличие средств восстановления СЗИ НСД.	Средство резервного копирования и восстановления серверной ОС Microsoft Windows Server.

В соответствии с руководящим документом "СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ МЕЖСЕТЕВЫЕ ЭКРАНЫ ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ ПОКАЗАТЕЛИ ЗАЩИЩЕННОСТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ" (РД МЭ) для Автоматизированной системы класс защищенности межсетевого экрана должен быть не ниже четвертого. Перечень требований РД МЭ к МЭ четвертого класса, и реализация сервером роли межсетевого экрана, приведен в таблице 3.

Таблица 3.

Требование РД СВТ МЭ для 4 класса защищенности	Средства, обеспечивающие выполнение требований РД
1. ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ (фильтрация данных и трансляция адресов)	
1.1 Управление доступом (фильтра-ция данных и трансляция адресов).	Механизмы управления доступом средствами Межстевого экрана.
1.2. Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств. Фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов. Фильтрация с учетом любых значимых полей сетевых пакетов.	
2. ПОДСИСТЕМА РЕГИСТРАЦИИ	
2.1. Регистрация и учет фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации.	Механизмы аудита средствами Межстевого экрана.
3. ПОДСИСТЕМА АДМИНИСТРИРОВАНИЯ	
3.1. Идентификация и аутентификация администратора МЭ при его локальных запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия.	Механизмы идентификации и аутентификации: - средствами Межстевого экрана.; - ОС Microsoft Windows Server.
3.2. Регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова. Регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ; В параметрах регистрации указываются: дата, время и код регистрируемого события; результат попытки осуществления регистрируемого события – успешная или неуспешная; идентификатор администратора МЭ, предъявленный при попытке осуществления регистрируемого события.	Механизмы аудита: - средствами Межстевого экрана.; - ОС Microsoft Windows Server.

Требование РД СВТ МЭ для 4 класса защищенности	Средства, обеспечивающие выполнение требований РД
4. ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ	
4.1. Наличие средств контроля за целостностью своей программной и информационной части.	Контроль целостности основных конфигурационных файлов средствами программной среды и антивирусными программами.
4.2. Восстановление после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств МЭ.	Механизмы защиты программной среды межсетевого экрана. Средства восстановления реализовываются средствами програмной среды.
4.3. Регламентное тестирование процесса контроля целостности программной и информационной части МЭ.	Механизмы тестирования средствами: - антивируса Касперского; - ОС Microsoft Windows Server.