МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт Факультет приборостроения, информационных технологий и электроники	Кафедра «Информационная безопасность систем и технологий»
Специальность 10.05.02 –	Информационная безопасность телекоммуникационных систем
Специализация -	Разработка защищенных телекоммуникационных систем

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ПОДСИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Студент _____ Шилкин Дмитрий Владимирович

Руководитель _____ Мещеряков А.А.

Нормоконтролёр _____ Фатеев А.Г.

Рецензент _____ _____ Паршин Н.М.

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой _____ С.Л. Зефиров

Работа защищена с отметкой _____(протокол заседания ГЭК от _____ № ____)

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2016

ТЗ

РЕФЕРАТ

Отчет о дипломной работе содержит 191 страница, 14 источников, 3 таблицы, 6 рисунков, 6 приложений.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ, РАСПРЕДЕЛЕННАЯ ИСПДН, ПЕРЕЧЕНЬ АКТУАЛЬНЫХ УГРОЗ, МЕРЫ ЗАЩИТЫ, РЫНОК СРЕДСТВ ЗАЩИТЫ.

Объектом исследования в данной дипломной работе является обработка персональных данных в распределенной системе персональных данных.

Целью дипломного проекта является разработка подсистемы защиты информации от несанкционированного доступа (НСД) в распределенной информационной системе персональных данных.

В ходе выполнения дипломной работы на первом этапе была разработана распределенная ИСПДн описаны ее состав и информационные потоки циркулирующие в ней. На втором этапе были определены актуальные угрозы безопасности информационной системы персональных данных и выбраны защитные меры, способные нейтрализовать их. На третьем этапе был рассмотрен рынок средств защиты и были выбраны средства подходящие для разрабатываемой ИСПДн. На четвертом этапе была описана установка и настройка выбранных средств защиты.

В результате была разработана модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных.

В результате выполнения работы все требования задания выполнены в полном объеме и в соответствии с требованиями технического задания.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

FTP − File Transfer Protocol, протокол передачи файлов;

MPLS — механизм в высокопроизводительной телекоммуникационной сети, осуществляющий передачу данных от одного узла сети к другому с помощью меток;

VLAN −Virtual Local Area Network — логическая («виртуальная») локальная компьютерная сеть;

VPN − Virtual Private Network, виртуальная частная сеть;

Wi-Fi − Wireless Fidelity, семейство стандартов передачи цифровых потоков данных по радиоканалам;

АРМ − автоматизированное рабочее место;

ИСПДн − информационная система персональных данных;

КПП − контрольно-пропускной пункт;

ЛВС − локальная вычислительная сеть;

МЭ − межсетевой экран;

НСД − несанкционированный доступ;

ПДн − персональные данные;

ПО − программное обеспечение;

ПТС − программно-технические средства;

ПЭМИН − побочные электромагнитные излучения и наводки;

СВТ − средство вычислительной техники;

СЗИ − средство защиты информации;

СОВ − система обнаружения вторжений;

СУБД − система управления базами данных;

ТТЗ − тактико-техническое задание;

ФСТЭК − Федеральная служба по техническому и экспортному контролю;

ЦОД − центр обработки данных;

ЦТП − центр технической поддержки.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.[1]

Автоматизированное рабочее место - комплекс программно-технических средств, используемый для подготовки и ввода в систему в электронном виде информации, а также для организации регламентированного доступа пользователей к информации, содержащейся в системе.[1]

Аудит - процесс записи информации о происходящих с каким-то объектом (или в рамках какого-то процесса) событиях в журнал (например, в файл). [10]

Доступ к информации - Возможность получения информации и ее использования.[1]

Защита информации от несанкционированного доступа - деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию).[1]

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.[1]

Избирательное управление доступом (англ. discretionary access control, DAC) - управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа. Также называется дискреционным управлением доступом, контролируемым управлением доступом или разграничительным управлением доступом. [1]

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.[1]

Класс защищенности - определенная совокупность требований по защите от несанкционированного доступа к информации.[1]

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.[1]

Мандатное управление доступом (англ. Mandatory access control, MAC) - разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности). [1]

Модель нарушителя - совокупность предположений о возможностях нарушителя, которые он может использовать для разработки и проведения а, также об ограничениях на эти возможности.[1]

Несанкционированный доступ - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.[1]

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. [1]

Общедоступные персональные данные - персональные данные доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе. [1]

Персональные данные - Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). [1]

Управление доступом на основе ролей (англ. Role Based Access Control, RBAC) - развитие политики избирательного управления доступом, при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли. [10]

СОДЕРЖАНИЕ

Введение 15
1 Структура распределенной ИСПДн 20
1.1 Оборудование объектов ИСПДн 20
1.2 Характеристики объекта автоматизации 21
2 Состав распределенной ИСПДн 23
3 Информационные потоки, циркулирующие в ИСПДн 30
3.1 Информационные потоки, циркулирующие в сегменте локально вычислительной сети размещаемом в дата центре 30
3.2 Информационные потоки, циркулирующие в помещение ЦТП 31
3.3 Информационные потоки, циркулирующие в сегментах спортивных объектов 33
4 Определение уровня защищенности ПДн и актуальных угроз 36
5 Организационные технические мероприятия и требования для обеспечения требуемого уровня защищенности ИСПДн 74
5.1 Угрозы утечки информации по техническим каналам 74
5.2 Угрозы непосредственного доступа 75
5.2.1 Описание угрозы 75
5.2.2 Вход в систему в обход средств защиты 77
5.2.3 НСД к АРМ пользователя и нелегальное использование нарушителем прав легального пользователя 79
5.2.4 Использование легальным пользователем незарегистрированных носителей информации с целью несанкционированного копирования информации 81
5.2.5 Нелегальное внедрение и использование неучтенных программ 82
5.2.6 Разглашение, передача или утрата атрибутов разграничения доступа 83
5.2.7 Действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, саботаж, и т.п.) 85

5.2.8 Проявление ошибок программно-аппаратных средств..... 87
5.2.9 Действия, приводящие к частичному или полному отказу СВТ или разрушению аппаратных, программных, информационных ресурсов СВТ (порча оборудования, носителей информации, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.)..... 88
5.2.10 Угрозы внедрения вредоносного ПО..... 90
5.3 Угрозы удаленного доступа (в локальной сети)..... 92
5.3.1 Описание..... 92
5.3.2 Анализ сетевого трафика..... 93
5.3.3 Угрозы выявления паролей..... 94
5.3.4Администрирование с нарушением требований нормативной и технической документации, в т.ч. ошибки администрирования 96
5.3.5 Незаконное подключение к линиям связи с целью модификации передаваемых сообщений, подмены законного пользователя, перехвата всего потока данных с целью его дальнейшего анализа и т.п..... 97
5.3.6 Навязывание ложного маршрута сети 99
5.3.7 Повреждение линий связи..... 100
5.3.8 Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др..... 101
5.3.9 Нарушение процедуры аутентификации субъектов виртуализированного информационного взаимодействия..... 101
5.3.10 Атака на гипервизор с виртуальной машины 102
5.3.11 Нарушение работоспособности информационных систем, построенных на основе технологии виртуализации, за счет НСД к средствам виртуализации..... 102
5.3.12 Визуальный съем информации при вводе аутентифицирующих данных 103

5.4 Прочие угрозы 104
5.4.1 Нелегальное подключение неучтенных технических средств 104
5.4.2 Хищение съемных носителей с защищаемой информацией 105
6 Средства защиты информации для обеспечения требуемого уровня защищенности распределенной ИСПДн 106
6.1 Средства защиты от НСД 106
6.1.1 Secret Net 7 106
6.1.2 Dallas Lock 8.0 107
6.2 Антивирусное обеспечение 110
6.2.1 Назначение антивирусного обеспечения 110
6.2.2 Kaspersky Security Center 10 110
6.2.3 Dr.Web 113
6.3 Средства защиты виртуальной среды 115
6.3.1 Описание виртуальной среды 115
6.3.2 Reflex VMC 115
6.3.3 vGate 116
6.4 Межсетевой экран 118
6.4.1 Назначение межсетевого экрана 118
6.4.2 ССПТ-2 119
6.4.3 Cisco ASA 5520 120
6.5 Система обнаружения вторжений 122
6.5.1 Назначение системы обнаружения вторжения 122
6.5.2 ФОРПОСТ 2.0 122
6.5.3 Аргус 124
Заключение 128
Список используемых источников 130
Приложение А Установка и настройка Secret Net 7 132
Приложение Б Установка и настройка Kaspersky Security Center 10 152

Приложение В Установка и настройка vGate 169
Приложение Г Настройка межсетевого экрана ССПТ-2..... 174
Приложение Д Настройка средства обнаружения вторжения Форпост 2.0 179
Приложение Е Протокол проверки ВКР на оригинальность 191

ВВЕДЕНИЕ

В современном мире информация становится стратегическим ресурсом, одним из основных богатств экономически развитого государства. Быстрое совершенствование информатизации в России, проникновение ее во все сферы жизненно важных интересов личности, общества и государства вызвали помимо несомненных преимуществ и появление ряда существенных проблем. Одной из них стала необходимость защиты информации. Учитывая, что в настоящее время экономический потенциал все в большей степени определяется уровнем развития информационной структуры, пропорционально растет потенциальная уязвимость экономики от информационных воздействий.

Каждый сбой работы компьютерной сети это не только "моральный" ущерб для работников предприятия и сетевых администраторов. По мере развития технологий электронных платежей, "безбумажного" документооборота и других, серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем на сегодняшний день.

Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Человека, пытающегося нарушить работу информационной системы или получить несанкционированный доступ к информации, обычно называют "компьютерным пиратом".

В своих противоправных действиях, направленных на овладение чужими секретами, взломщики стремятся найти такие источники конфиденциальной информации, которые бы давали им наиболее достоверную информацию в максимальных объемах с минимальными затратами на ее получение. С

помощью различного вида уловок и множества приемов и средств подбираются пути и подходы к таким источникам. В данном случае под источником информации понимается материальный объект, обладающий определенными сведениями, представляющими конкретный интерес для злоумышленников или конкурентов.

Если ценность информации теряется при ее хранении и/или распространении, то реализуется угроза нарушения конфиденциальности информации. Если информация изменяется или уничтожается с потерей ее ценности, то реализуется угроза целостности информации. Если информация вовремя не поступает легальному пользователю, то ценность ее уменьшается и со временем полностью обесценивается, тем самым реализуется угроза оперативности использования или доступности информации.

Итак, реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. Злоумышленник может ознакомиться с конфиденциальной информацией, модифицировать ее, или даже уничтожить, а также ограничить или блокировать доступ легального пользователя к информации. При этом злоумышленником может быть как сотрудник организации, так и постороннее лицо. Но, кроме этого, ценность информации может уменьшиться ввиду случайных, неумышленных ошибок персонала, а также сюрпризов иногда преподносимых самой природой.

Информационные угрозы безопасности могут быть обусловлены:

а) естественными факторами (стихийные бедствия – пожар, наводнение, ураган, молния и другие причины);

б) человеческими факторами.

Последние, в свою очередь, подразделяются на:

– угрозы, носящие случайный, неумышленный характер. Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи

информации (научно-техническая, коммерческая, валютно-финансовая документация). Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные программы и др.), с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации);

– угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с передачей, искажением и уничтожением научных открытий, изобретений секретов производства, новых технологий по корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); подслушиванием и передачей служебных и других научно-технических и коммерческих разговоров. Эти угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи, хищение носителей информации: дискет, описаний, распечаток и др.).

Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на

аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы, искажение сведений в базах данных либо в системной информации и т.д. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

Умышленные угрозы подразделяются на внутренние, возникающие внутри управляемой организации, и внешние.

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, получил широкое распространение промышленный шпионаж - это наносящие ущерб владельцу коммерческой тайны, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

К основным угрозам безопасности относят:

– раскрытие конфиденциальной информации;

– компрометация информации;

– несанкционированное использование информационных ресурсов;

– ошибочное использование ресурсов; несанкционированный обмен информацией;

– отказ от информации;

– отказ от обслуживания.

Средствами реализации угрозы раскрытия конфиденциальной информации могут быть несанкционированный доступ к базам данных, прослушивание каналов и т.п. В любом случае получение информации,

являющейся достоянием некоторого лица (группы лиц), что приводит к уменьшению и даже потере ценности информации.

1 Структура распределенной ИСПДн

1.1 Оборудование объектов ИСПДн

ИСПДн должна быть реализована как территориально распределенная информационная система, включающая в свой состав оборудование точек доступа, автоматизированные рабочие места, серверное оборудование и средства защиты информации.

Состав изделия, приведен в таблице 1

Таблица 1- Состав изделия

Наименование изделия	Примечание
Станционное оборудование	
Центральный сервер базы данных (ЦСБД)	Основной, резервный
Объектовый сервер базы данных (ОСБД)	
Сервер связи (СС)	Основной, резервный
АРМ объединенного пункта безопасности (АРМ–ОПБ)	
АРМ технического обеспечения (АРМ–ТО)	
АРМ администратора (АРМ-А)	
АРМ бюро пропусков (АРМ–БП)	
Периферийное оборудование	
Блок считывателей управляющий универсальный (БСУУ)	
Блок мониторный (БМ)	
Стойка мониторная (СМ)	
Мобильный терминал (МТ)	
Оборудование дистанционного считывания RFID идентификаторов (ОДС)	

Продолжение таблицы 1

Наименование изделия	Примечание
Подсистема защиты информации	
Система обнаружения вторжения (и/или сетевой датчик)	
Сервер безопасности (СБ)	
АРМ администратора безопасности (АРМ-АБ)	
АРМ управления криптосетью (АРМ-УК)	
Средства защиты информации (СЗИ) от несанкционированного доступа (НСД).	
Сетевое оборудование	

Состав системы должен обеспечивать создание территориально разнесенных объектов информатизации:

- центр обработки данных (ЦОД) ИСПДн;
- центр управления и технической поддержки (ЦУТП);
- спортивные объекты;
- ЦОД внешних систем (шлюз взаимодействия с внешними системами).

1.2 Характеристики объекта автоматизации

Пользователями ИСПДн являются:

- сотрудники объединенного пункта безопасности (ОПБ) спортивного объекта;
- системные администраторы;
- администраторы баз данных;
- администраторы безопасности;

– эксплуатационно-технический персонал.

Функции пользователей должны обеспечиваться соответствующим набором программно-технических средств (ПТС), объединенных локальными сетями на объектах.

Объектом информатизации ИСПДн является совокупность информационных ресурсов, ПТС и локальной сети, используемых в соответствии с заданной информационной технологией; помещений на объектах, в которых они установлены.

Границы ИСПДн и перечень объектов информатизации определяются местами дислокации пользователей, которые расположены на следующих объектах:

– спортивные объекты;
– ЦОД внешних систем;
– ЦОД ИСПДн;
– ЦУТП ИСПДн.

Телекоммуникационное взаимодействие объектов информатизации ИСПДн должно быть реализовано через развертываемую защищенную сеть VPN, функционирующую через мультисервисную сеть связи (МСС) провайдера связи на базе технологии MPLS VPN L3 (топологии «Каждый с каждым»). При этом должно быть осуществлено подключение объектов информатизации ИСПДн к основному и резервному (при наличии) узлам доступа МСС с поддержкой статической и динамической маршрутизации.

2 Состав распределенной ИСПДн

Топология информационной сети должна быть радиально-узловой, в которой основными узлами будут являться ЦСБД и резервный ЦСБД, расположенный в ЦУТП, обеспечивающие информационный обмен по каналам связи со всеми ОСБД и внешними системами.

Каждый ОСБД должен подключаться к ЦОД ИСПДн для репликации данных, централизованного управления ИСПДн, принятия внутриведомственных и межведомственных организационных решений, организации мониторинга системы в целом и проведения работ по технической поддержке.

Спортивный (соревновательный) объект должен оснащаться оборудованием, приведенным в таблице 2. Оборудование каждого спортивного объекта должно подразделяться на станционное (размещаемое в серверных помещениях), дополнительное оборудование (АРМ, коммутационное и каналообразующее оборудование) и периферийное (точки доступа).

Таблица 2 – Назначение составных частей объекта

Наименование составной части	Назначение
Объектовый сервер баз данных	Контроллер домена из состава ОСБД: Внутрисетевое взаимодействие рабочих станций и серверов. Разграничение прав доступа пользователей к АРМ, серверам и БД. Администрирование учетных записей пользователей и машин. Выполнение Обеспечение сервисных функций по управлению ролью отказоустойчивого кластера, систем мониторинга, а также участие в обновлении систем и служб на АРМ и серверах.

Продолжение таблицы 2

Наименование составной части	Назначение
	Кластер БД из состава ОСБД: Хранение и обработка информации поступающей от оконечного оборудования, информации, поступающей из центрального сервера баз данных, обработка поступающих запросов от АРМ спортивного объекта, формирование и отправка ответов на запросы; архивирование и хранение архивов ОСБД, выгрузка данных в систему управления соревнованиями.
Сервер безопасности	Хранение файлов конфигурации и архивов событий, вывод на печать информации о событиях связанных с СЗИ
АРМ–ОПБ	Формирование запросов к объектовому и центральному кластеру БД ИСПДн, обработка полученных ответов.
АРМ–ТО	Обновление файлов периферийного оборудования. Хранение архивных копий СПО. Управление Конфигурирование периферийного оборудования. Отображение информации о состоянии периферийного оборудования в режиме реального времени.
АРМ Администратора	Обновление систем. Мониторинг состояния и удаленное управление парком серверов, системы хранения данных (СХД). Администрирование домена, VM, DNS, отказоустойчивых кластеров.

Продолжение таблицы 2

Наименование составной части	Назначение
АРМ–БП	Учет и выпуск пропускных документов, удовлетворяющих требованиям ИСПДн. Контроль пропускных документов, их активация или отмена. Поиск зарегистрированных пропускных документов в базе данных.

Периферийное оборудование предназначено для организации точек доступа следующих типов:

– БСУУ (для считывания RFID-идентификатора и штрих-кода, управления исполнительным устройством (турникетами)), БМ (для отображения информации об абоненте) для организации входа и/или выхода аккредитованных лиц, гостей;

– БСУУ (для считывания RFID-идентификатора и штрих-кода, управления исполнительным устройством (турникетами)), БМ (для отображения информации об абоненте) для организации входа и/или выхода зрителей;

– мобильный беспроводной ручной терминал, реализующий функции сканирования RFID-идентификатора, штрих-кода и отображение фотографии абонента на дисплее. Мобильный терминал должен обеспечивать обслуживание абонентов на транспортном КПП и у калиток на КПП. Передача данных мобильным терминалом должна осуществляться по стандарту Wi-Fi IEEE 802.11 a/b/g;

– ОДС, обеспечивающее автоматическое сканирование RFID-идентификаторов, встроенных в пропускные документы абонентов. ОДС должен использоваться для дистанционного считывания кодов RFID-

идентификаторов пропускных документов при свободном выходе абонентов с объекта. ОДС должен подключается к ЛВС спортивного объекта ИСПДн и обеспечивать передачу сообщений о фактах регистрации кодов RFID-идентификаторов в базу данных ОСБД как события доступа.

В состав объекта информатизации ЦОД должны входить:

– ЦСБД;

– сервер связи;

– сервер безопасности;

– средства обнаружения компьютерных атак/вторжений и/или сетевой датчик (при необходимости);

– сетевое оборудование для организации ЛВС;

– средства бесперебойного питания;

– средства комплексирования (стойка, патч-панели, кабели, переходники, преобразователи и т.п.);

– линии связи между маршрутизатором (коммутатором) и узлами доступа (основным и, при наличии, резервным) МСС провайдера связи на объектах.

В состав объекта информатизации ЦУТП должны входить:

– ЦСБД (резервирование);

– сервер безопасности;

– АРМ администратора;

– АРМ администратора безопасности;

– АРМ управления криптосетью;

– АРМы технического обеспечения;

– АРМы ОПБ;

– межсетевые экраны;

– средства обнаружения компьютерных атак/вторжений и/или сетевые датчики (при необходимости);

– сетевое оборудование для организации ЛВС;

– средства бесперебойного питания;

– средства комплексирования (стойка, патч-панели, кабели, переходники, преобразователи и т.п.);

– линии связи между маршрутизатором (коммутатором) и узлами доступа (основным и, при наличии, резервным) МСС провайдера связи на объектах.

В состав типового объекта информатизации – спортивного объекта должны входить:

– ОСБД;

– сервер безопасности;

– АРМ администратора системы;

– АРМ администратора безопасности;

– АРМы технического обеспечения;

– АРМы ОПБ;

– сетевое оборудование для организации ЛВС;

– СЗИ;

– средства бесперебойного питания;

– средства комплексирования (стойка, патч-панели, кабели, переходники, преобразователи и т.п.);

– мобильные терминалы;

– БСУУ;

– блоки мониторные;

– ОДС;

– оборудование для организации беспроводного доступа к ЛВС;

– линии связи между маршрутизатором (коммутатором) и узлами доступа (основным и, при наличии, резервным) МСС провайдера связи на объектах.

В состав типового объекта информатизации – шлюза взаимодействия с внешними системами должны входить:

– сетевое оборудование для организации ЛВС;

– средства бесперебойного питания;

– средства комплексирования (стойка, патч-панели, кабели, переходники, преобразователи и т.п.);

– линии связи между маршрутизатором (коммутатором) и узлами доступа (основным и, при наличии, резервным) МСС провайдера связи на объектах.

На данном этапе работы была разработана структурная схема ИСПДн, представленная на рисунке 1.

Структура объектового сегмента распределенной ИСПДн размещения на спортивном объекте представлена на рисунке 2.

Архитектура центра управления технической поддержки распределенной ИСПДн представлена на рисунке 3.

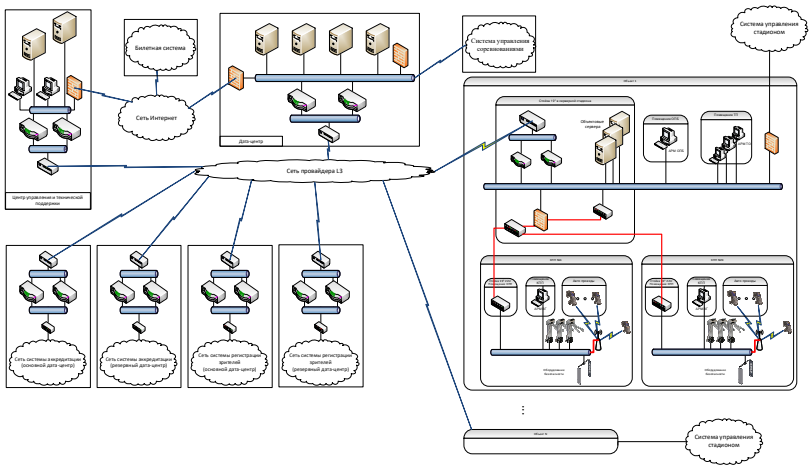

Рисунок 1 - Структурная схема распределенной ИСПДн

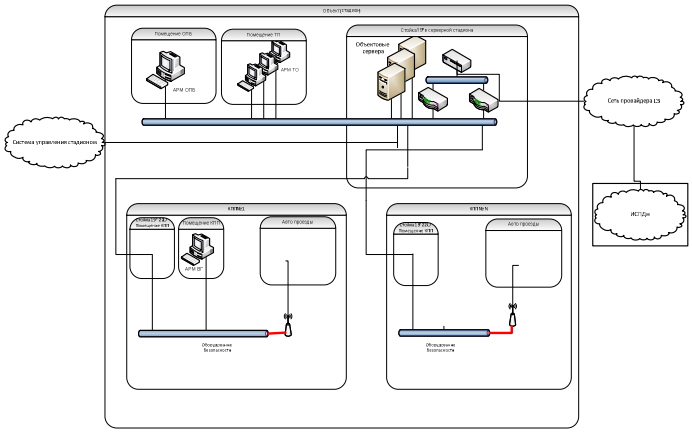

Рисунок 2 - Структура объектового сегмента распределенной ИСПДн размещения на спортивном объекте

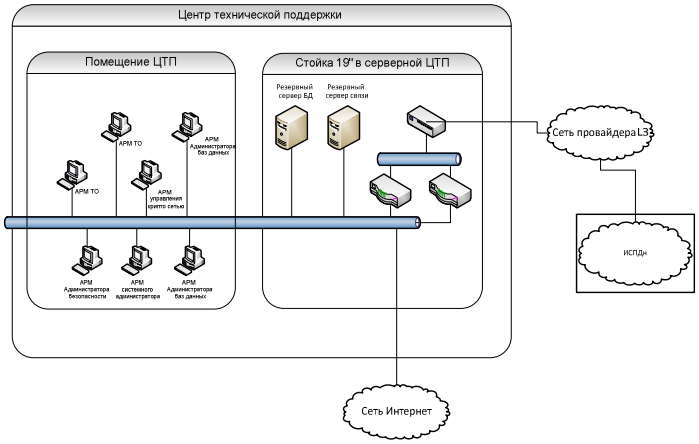

Рисунок 3 - Архитектура центра управления технической поддержки распределенной ИСПДн

3 Информационные потоки, циркулирующие в ИСПДн

3.1 Информационные потоки, циркулирующие в сегменте локально вычислительной сети размещаемом в дата центре

Сегмент локально вычислительной сети размещаемый в дата центре состоит из:

– основной сервер связи, в котором выполняется временное хранение информации из внешних систем (аккредитации, регистрации зрителей, билетной и др.), поступающей в СКД, передача информации в БД, обмен информацией с внешними системами (в том числе передача информации через сеть Интернет (не ПДн)), удаление переданной информации;

– центральный кластер БД, в котором выполняется хранение и обработка информации поступающей от оконечного оборудования, информации поступающей из внешних систем (аккредитации, регистрации зрителей, билетной и др.), обработка поступающих запросов от АРМ, формирование и отправка ответов на запросы; архивирование и хранение архивов БД;

– сервер “Контроллер домена”, в котором происходит внутрисетевое взаимодействие рабочих станций и серверов, разграничение прав доступа пользователей к АРМ, серверам и БД, администрирование учетных записей пользователей и машин, выполнение сервисных функций по управление ролью отказоустойчивого кластера, систем мониторинга, а также участие домена в обновлении систем и служб на АРМ и серверах.

Между основным сервером связи, центральным кластером БД и сервер “Контроллер домена” происходит передача данных в линиях связи и коммутационном оборудовании. Дата-центр обменивается информацией с билетной системой и выделенной сетью провайдера.

С билетной системой дата-центр обменивается информацией о билетах (штрих-код, код соревнования и т.д.), происходит обмен квитанциями,

информацией об использованных билетах. Вся информация проходит через межсетевой экран.

Для взаимодействия дата-цента с другими сегментами ИСПДн существует соединение с сетью MPLS. С помощью этого соединения происходит передача информации (ФИО, ФОТО, данные документов удостоверяющих личность, номер пропуска, и т.д.), получение подтверждающих квитанций и передача служебной информации.

3.2 Информационные потоки, циркулирующие в помещение ЦТП

В помещение ЦТП располагаются:

– АРМ ТО, предназначенное для обновления файлов периферийного оборудования, хранения архивных копий СПО, управления периферийным оборудованием, отображения информации о состоянии периферийного оборудования в режиме реального времени и обмена текстовыми и звуковыми сообщениями между сотрудниками;

– АРМ администратора безопасности, обеспечивает хранение архивов событий, вывод на печать информации о событиях ИСПДн, хранение файлов конфигурации;

– АРМ системного администратора, отвечает за обновление систем, мониторинг состояния и удаленное управление парком серверов, ИСПДн, администрирование домена и отказоустойчивых кластеров;

– АРМ администратора БД. Администратор базы данных ИСПДн производит настройку и конфигурацию БД, просмотр и формирование отчетов состояния БД, мониторинг и удаленное управление БД;

– АРМ управления криптосетью, предназначено для хранения архивов событий, вывода на печать информации о событиях криптоситсемы, хранение файлов конфигурации и ключевой информации;

– резервный сервер связи, выполняет роль временного хранилища информации, поступающей из внешних систем (аккредитации, регистрации

зрителей, билетной и др.), поступающей в аварийных ситуациях (выход из строя основного сервера связи, нарушения в работе каналов связи с основным сервером, проведение ремонтных работ и пр.), передача информации в БД, обмен информацией с внешними системами (в том числе передача информации через сеть Интернет (не ПДн)), удаление переданной информации;

– резервный кластер БД это хранилище информации из внешних систем (аккредитации, регистрации зрителей, билетной и др.), поступающей в аварийных ситуациях (выход из строя основного сервера БД, нарушения в работе каналов связи с основным сервером, проведение ремонтных работ и пр.);

– сервер домена, обеспечивает внутрисетевое взаимодействие рабочих станций и серверов, разграничение прав доступа пользователей к АРМ, серверам и БД, администрирование учетных записей пользователей и машин, выполнение сервисных функций по управление ролью отказоустойчивого кластера, систем мониторинга, а также участие домена в обновлении систем и служб на АРМ и серверах.

Все оборудование центра управления и технической поддержки ИСПДн объединено и взаимодействует со всеми сегментами сети через предоставленную сеть провайдера, а так же имеет выход в сеть интернет. Взаимодействие с сетью интернет необходимо для обмена информацией с отдаленными сегментами, а так же для отправки электронных писем и СМС оповещений о работе персоналу технической поддержки.

С билетной системой центр управления и технической поддержки обменивается информацией о билетах (штрих-код, код соревнования и т.д.), обмен квитанциями, информация об использованных билетах.

Обмен информацией с сетью интернет и билетной системой производится только через оборудование с функцией межсетевого экрана.

3.3 Информационные потоки, циркулирующие в сегментах спортивных объектов

Все сегменты спортивных объектов для обмена данными с другими сегментами ИСПДн так же имеют подключение к сети провайдера.

Сегменты спортивных объектов состоят из:

- помещение СБ;
- помещение ТП;
- серверная спортивного объекта;
- КПП №1…N.

В помещение СБ находится АРМ ОПБ, предназначенное для формирования запросов к объектовому и центральному кластеру БД, обработки полученных ответов.

В помещение ТП находится АРМ ТО и АРМ администратора. АРМ ТО предназначено для:

- обновления файлов периферийного оборудования;
- хранения архивных копий СПО;
- управления периферийным оборудованием;
- отображения информации о состоянии периферийного оборудования в режиме реального времени;
- обмена текстовыми и звуковыми сообщениями между сотрудниками.

АРМ администратора предназначено для:

- обновления систем;
- мониторинга состояния и удаленного управления парком серверов;
- администрирование домена, отказоустойчивых кластеров;
- настройки и конфигурации БД;
- просмотра и формирования отчетов состояния БД;
- хранения архивов событий, вывод на печать информации о событиях, хранение файлов конфигурации.

В серверной спортивного объекта находятся различные сервера, одними из которых являются сервер домена и объектовый кластер БД.

Сервер домена предназначен для:

– внутрисетевого взаимодействия рабочих станций и серверов;

– разграничения прав доступа пользователей к АРМ, серверам и БД;

– администрирования учетных записей пользователей и машин;

– выполнения сервисных функций по управление ролью отказоустойчивого кластера, систем мониторинга, а также участие домена в обновлении систем и служб на АРМ и серверах.

Объектовый кластер БД предназначен для:

– хранения и обработки информации, поступающей от оконечного оборудования;

– хранения и обработки информации, поступающей из основного (резервного) кластера БД;

– обработка поступающих запросов от АРМ;

– формирование и отправка ответов на запросы;

– архивирование и хранение архивов БД.

КПП №1…N состоит из:

– оборудования безопасности;

– мобильных терминалов;

– контроллеров турникетов.

Оборудование безопасности предназначено для:

– считывания пропусков;

– временного хранения информации о считанных, удаления после отправки информации в объектовую базу данных.

Мобильные терминалы и контроллеры турникетов предназначены для:

– считывания пропусков;

– отправки запросов в объектовую базу данных;

– обработки ответов из объектовой БД;

– временного хранения и отображения информации на дисплее устройства (фотографию и ФИО);

– отправки информации о результатах прохода.

Информационное взаимодействие распределенной ИСПДн представлено на рисунке 4.

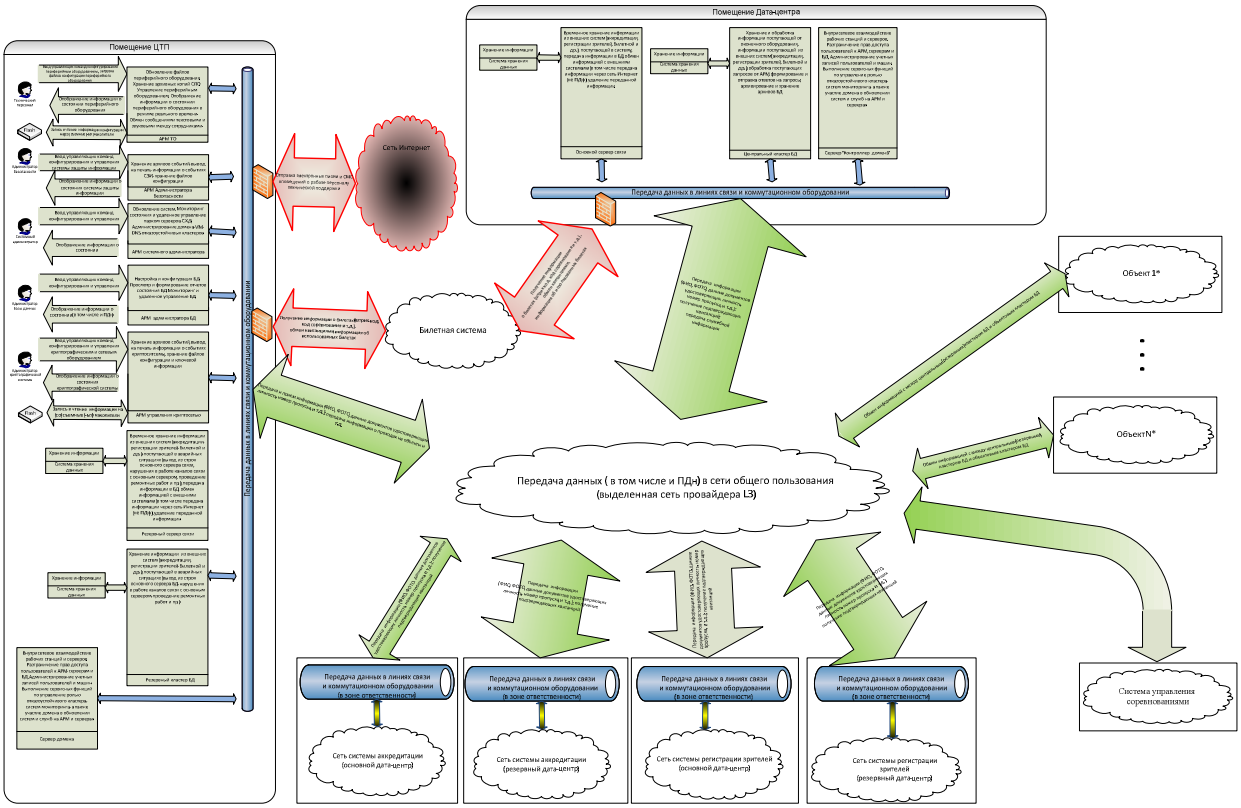

Рисунок 4 - Информационное взаимодействие распределенной ИСПДн

4 Определение уровня защищенности ПДн и актуальных угроз

В распределенной ИСПДн обрабатываются ПДн в составе:

- фамилия, имя, отчество (на русском и латинице);
- дата рождения;
- гражданство;
- фото;
- тип ДУЛ;
- серия и номер ДУЛ;
- дата выдачи ДУЛ;
- организация, выдавшая ДУЛ;
- уникальный номер билета на мероприятие из распределенной ИСПДн.

В общей сложности в ИСПДн обрабатываются ПДн более чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора.

Согласно положениям Постановления Правительства Российской Федерации от 02 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[11], уровень защищенности ПДн определяется исходя из:

- объема обрабатываемых ПДн;
- категории обрабатываемых ПДн;
- принадлежности обрабатываемых ПДн (оператору или иным лицам);
- типа угроз безопасности ПДн.

Исходя из предположения о том, что в ИСПДн уязвимости, внесенные преднамеренно разработчиком (недекларированные возможности) в общее и/или прикладное ПО, являются неактуальными в связи с тем, что административным персоналом ИСПДн обеспечивается:

– контроль за составом ПО, установленного на серверах и рабочих станциях;

– управление запуском компонентов ПО серверов и рабочих станций путем настройки параметров запуска, а также контроля запуска данных компонентов;

– своевременное выявление уязвимостей и установка критических обновлений, выпускаемых производителем ПО;

– контроль целостности ПО серверов и рабочих станций, в том числе используемых СЗИ, для ИСПДн, в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», будут актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО, используемом в информационной системе (угрозы 3-го типа).

Таким образом, учитывая, что для распределенной ИСПДн, как информационной системы персональных данных, будут актуальны угрозы 3-го типа, в них производится обработка иных категорий ПДн (не являющиеся общедоступными, специальными или биометрическими) более чем 100 000 субъектов ПДн и обрабатываемые ПДн принадлежат лицам, не являющимся сотрудниками оператора ПДн, распределенной ИСПДН может быть классифицирована как информационная система персональных данных, для которой необходимо обеспечение 3-го уровня защищенности ПДн.

Перечень актуальных угроз безопасности ПДн в распределенной ИСПДн и состав применяемых для их блокирования мер защиты информации, на основании приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащихся в государственных информационных системах»[7], приведен в таблице 3.

Был рассмотрен банк данных угроз безопасности информации, из которого были выбраны актуальные угрозы для разрабатываемой распределенной ИСПДн. На основании приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащихся в государственных информационных системах»[7], были определены меры защиты информации.

Актуальные угрозы:

угроза утечки видовой информации;

вход в систему в обход средств защиты;

Таблица 3 - Перечень актуальных угроз безопасности ПДн в распределенной ИСПДН и состав применяемых для их блокирования мер защиты информации

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
1. Угрозы утечки информации по техническим каналам	
1.1. Угрозы утечки видовой информации	Защита обратной связи при вводе аутентификационной информации (ИАФ.5). Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (ЗТС.2). Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3). Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4)

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
2. Угрозы НСД к информации в распределенной ИСПДН	
2.1. Угрозы непосредственного доступа	
2.1.1. Вход в систему в обход средств защиты	Идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1). Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) (ИАФ.6). Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) (УПД.6). Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10). Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	программного обеспечения (ОПС.2). Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов (ОПС.3). Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (ЗТС.2). Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3)
2.1.2. НСД к АРМ пользователя и нелегальное использование	Идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1). Защита обратной связи при вводе

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
нарушителем прав легального пользователя	аутентификационной информации (ИАФ.5). Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) (ИАФ.6). Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10). Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения (ОПС.2). Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов (ОПС.3). Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей (АНЗ.1). Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	(ЗТС.2). Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3). Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4)
2.1.3. Использование легальным пользователем незарегистрированных носителей информации с целью несанкционированного копирования	Учет машинных носителей информации (ЗНИ.1). Управление доступом к машинным носителям информации (ЗНИ.2)

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
информации	
2.1.4. Нелегальное внедрение и использование неучтенных программ	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения (ОПС.2). Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов (ОПС.3). Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1). Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций (ОЦЛ.3). Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации (АНЗ.2). Контроль работоспособности, параметров настройки и правильности функционирования

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	программного обеспечения и средств защиты информации (АНЗ.3). Контроль состава технических средств, программного обеспечения и средств защиты информации (АНЗ.4).
2.1.5. Разглашение, передача или утрата атрибутов разграничения доступа	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (УПД.4). Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы (УПД.5). Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них (РСБ.5). Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1). Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3). Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы (ЗИС.1).
2.1.6. Действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, саботаж, и т.п.)	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них (РСБ.5). Контроль состава технических средств, программного обеспечения и средств защиты информации (АНЗ.4). Использование отказоустойчивых технических средств (ОДТ.1). Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы (ОДТ.2). Контроль безотказного функционирования

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование (ОДТ.3). Периодическое резервное копирование информации на резервные машинные носители информации (ОДТ.4). Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала (ОДТ.5). Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (ЗТС.2). Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3). Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы (ЗИС.1). Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации (ЗИС.15).
2.1.7. Проявление ошибок программно-аппаратных средств	Использование отказоустойчивых технических средств (ОДТ.1). Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы (ОДТ.2). Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	тестирование (ОДТ.3). Периодическое резервное копирование информации на резервные машинные носители информации (ОДТ.4). Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала (ОДТ.5). Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации (ЗИС.15).
2.1.8. Действия, приводящие к частичному или полному отказу СВТ или разрушению аппаратных, программных, информационных ресурсов СВТ (порча оборудования,	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них (РСБ.5). Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (АНЗ.3). Использование отказоустойчивых технических средств (ОДТ.1). Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
носителей информации, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.)	функционирования информационной системы (ОДТ.2). Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование (ОДТ.3). Периодическое резервное копирование информации на резервные машинные носители информации (ОДТ.4). Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала (ОДТ.5). Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (ЗТС.2). Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены,

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3). Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) (ЗТС.5). Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации (ЗИС.15).
2.1.9. Угрозы внедрения вредоносного ПО	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения (ОПС.2). Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов (ОПС.3). Мониторинг (просмотр, анализ) результатов

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	регистрации событий безопасности и реагирование на них (РСБ.5). Реализация антивирусной защиты (АВЗ.1). Обновление базы данных признаков вредоносных компьютерных программ (вирусов) (АВЗ.2). Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации (АНЗ.2). Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (АНЗ.3). Контроль состава технических средств, программного обеспечения и средств защиты информации (АНЗ.4). Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1). Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций (ОЦЛ.3). Реализация и управление антивирусной

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	защитой в виртуальной инфраструктуре (ЗСВ.9).
2.2. Угрозы удаленного доступа (в локальной сети)	
2.2.1. Анализ сетевого трафика	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (ПД.3). Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (УПД.13). Регламентация и контроль использования в информационной системе технологий беспроводного доступа (УПД.14). Регламентация и контроль использования в информационной системе мобильных технических средств (УПД.15). Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы (ЗИС.17).

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
2.2.2. Угрозы выявления паролей	Идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1). Защита обратной связи при вводе аутентификационной информации (ИАФ.5). Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) (ИАФ.6). Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) (УПД.6). Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения (ОПС.2). Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов (ОПС.3). Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	функционирования (ЗТС.2). Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3). Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4).
2.2.3. Угрозы внедрения вредоносного ПО	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения (ОПС.2). Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов (ОПС.3). Мониторинг (просмотр, анализ) результатов

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	регистрации событий безопасности и реагирование на них (РСБ.5). Реализация антивирусной защиты (АВЗ.1). Обновление базы данных признаков вредоносных компьютерных программ (вирусов) (АВЗ.2). Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации (АНЗ.2). Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (АНЗ.3). Контроль состава технических средств, программного обеспечения и средств защиты информации (АНЗ.4). Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1). Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций (ОЦЛ.3). Реализация и управление антивирусной

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	защитой в виртуальной инфраструктуре (ЗСВ.9).
2.2.4. Администрирование с нарушением требований нормативной и технической документации, в т.ч. ошибки администрирования	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (УПД.4). Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы (УПД.5). Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них (РСБ.5). Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (АНЗ.3). Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1). Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций (ОЦЛ.3). Периодическое резервное копирование информации на резервные машинные носители

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	информации (ОДТ.4). Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала (ОДТ.5). Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы (ЗИС.1). Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации (ЗИС.15).
2.2.5. Незаконное подключение к линиям связи с целью модификации передаваемых сообщений, подмены законного	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3). Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
пользователя, перехвата всего потока данных с целью его дальнейшего анализа и т.п.	сети (УПД.13). Регламентация и контроль использования в информационной системе технологий беспроводного доступа (УПД.14). Регламентация и контроль использования в информационной системе мобильных технических средств (УПД.15). Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (ЗТС.2). Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3). Разбиение информационной системы на

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы (ЗИС.17).
2.2.6. Навязывание ложного маршрута сети	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных (ИАФ.2). Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3). Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (УПД.13). Регламентация и контроль использования в информационной системе технологий беспроводного доступа (УПД.14). Контроль состава технических средств, программного обеспечения и средств защиты информации (АНЗ.4). Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	сервисов (ЗИС.11).
2.2.7. Повреждение линий связи	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы (ОДТ.2). Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование (ОДТ.3).
2.3. Угрозы удаленного доступа (из внешних сетей)	
2.3.1. Анализ сетевого трафика	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3). Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	сети (УПД.13). Регламентация и контроль использования в информационной системе технологий беспроводного доступа (УПД.14). Регламентация и контроль использования в информационной системе мобильных технических средств (УПД.15). Обнаружение вторжений (СОВ.1). Обновление базы решающих правил (СОВ.2). Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы (ЗИС.17).
2.3.2. Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3). Обнаружение вторжений (СОВ.1). Обновление базы решающих правил (СОВ.2). Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы (ЗИС.17).

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
2.3.3. Угрозы выявления паролей	Идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1). Защита обратной связи при вводе аутентификационной информации (ИАФ.5). Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) (ИАФ.6). Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) (УПД.6). Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения (ОПС.2). Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов (ОПС.3). Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	функционирования (ЗТС.2). Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3). Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4).
2.3.4. Подмена доверенного объекта сети	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных (ИАФ.2). Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3). Реализация защищенного удаленного доступа

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (УПД.13). Регламентация и контроль использования в информационной системе технологий беспроводного доступа (УПД.14). Регламентация и контроль использования в информационной системе мобильных технических средств (УПД.15). Контроль состава технических средств, программного обеспечения и средств защиты информации (АНЗ.4). Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1). Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (ЗИС.11). Защита беспроводных соединений, применяемых в информационной системе (ЗИС.20).
2.3.5. Навязывание ложного маршрута сети	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных (ИАФ.2). Управление (фильтрация, маршрутизация,

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3). Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (УПД.13). Регламентация и контроль использования в информационной системе технологий беспроводного доступа (УПД.14). Контроль состава технических средств, программного обеспечения и средств защиты информации (АНЗ.4). Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование (ОДТ.3). Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (ЗИС.11). Защита беспроводных соединений,

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	применяемых в информационной системе (ЗИС.20).
2.3.6. Отказ в обслуживании путем частичного исчерпания ресурсов	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3). Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (УПД.13). Регламентация и контроль использования в информационной системе технологий беспроводного доступа (УПД.14). Регламентация и контроль использования в информационной системе мобильных технических средств (УПД.15). Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование (ОДТ.3).
2.3.7. Отказ в обслуживании путем полного	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
исчерпания ресурсов	потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3). Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (УПД.13). Регламентация и контроль использования в информационной системе технологий беспроводного доступа (УПД.14).
2.3.8. Угрозы внедрения вредоносного ПО	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения (ОПС.2). Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов (ОПС.3). Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них (РСБ.5). Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	информации (АНЗ.2). Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (АНЗ.3). Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1). Реализация и управление антивирусной защитой в виртуальной инфраструктуре (ЗСВ.9).
2.4. Угрозы, направленные на среду виртуализации	
2.4.1. Нарушение процедуры аутентификации субъектов виртуализированного информационного взаимодействия	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации (ЗСВ.1). Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин (ЗСВ.2). Регистрация событий безопасности в виртуальной инфраструктуре (ЗСВ.3).
2.4.2. Атака на	Идентификация и аутентификация субъектов

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
гипервизор с виртуальной машины	доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации (ЗСВ.1). Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин (ЗСВ.2). Регистрация событий безопасности в виртуальной инфраструктуре (ЗСВ.3).
2.4.3. Нарушение работоспособности информационных систем, построенных на основе технологии виртуализации, за счет НСД к средствам виртуализации	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации (ЗСВ.1). Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин (ЗСВ.2). Регистрация событий безопасности в виртуальной инфраструктуре (ЗСВ.3).
2.4.4. Перехват управления в сети виртуализации	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации (ЗСВ.1). Управление доступом субъектов доступа к

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин (ЗСВ.2). Регистрация событий безопасности в виртуальной инфраструктуре (ЗСВ.3).
2.5. Угрозы, направленные на дополнительные программно-аппаратные СЗИ	
2.5.1. Визуальный съем информации при вводе аутентифицирующих данных	Защита обратной связи при вводе аутентификационной информации (ИАФ.5). Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (ЗТС.2). Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3). Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4).
3. Прочие угрозы	
3.1. Нелегальное подключение неучтенных технических средств	Учет машинных носителей информации (ЗНИ.1). Управление доступом к машинным носителям информации (ЗНИ.2). Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (ЗТС.2). Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам

Продолжение таблицы 3

Наименование угрозы	Применяемые для нейтрализации угрозы меры защиты
	обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3).
3.2.Хищение съемных носителей с защищаемой информацией	Учет машинных носителей информации (ЗНИ.1). Управление доступом к машинным носителям информации (ЗНИ.2). Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) (ЗНИ.8).

5 Организационные технические мероприятия и требования для обеспечения требуемого уровня защищенности ИСПДн

5.1 Угрозы утечки информации по техническим каналам

Угроза утечки видовой информации.

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптика электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Кроме этого, просмотр (регистрация) ПДн возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

Угрозы безопасности ПДн, связанные с их перехватом при использовании специальных электронных устройств съема видовой информации (видео закладок), определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Перехват ПДн может вестись:

– стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;

– портативной возимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;

– портативной носимой аппаратурой – физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них.

Перехват (просмотр) ПДн может осуществляться посторонними лицами путем их непосредственного наблюдения в служебных помещениях либо с расстояния прямой видимости из-за пределов ИСПДн с использованием оптических (оптика электронных) средств.

Для нейтрализации угроз утечки видовой информации решено использовать организационно-технические мероприятия:

– установить средства, исключающие несанкционированный просмотр;

– помещения, в которых размещены средства вычислительной техники, вход в помещение должен быть оснащен средствами управления доступом;

– установить жалюзи на окна;

– должны быть разработаны инструкции для всех пользователей системы включающие требования по блокированию при оставлении рабочего места.

5.2 Угрозы непосредственного доступа

5.2.1 Описание угрозы

Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к ПДн связаны с доступом:

– к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) ИСПДн, с возможностью перехвата управления загрузкой операционной системы и получением прав доверенного пользователя;

– в операционную среду, то есть в среду функционирования локальной операционной системы отдельного технического средства ИСПДн с

возможностью выполнения несанкционированного доступа путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;

– в среду функционирования прикладных программ (например, к локальной системе управления базами данных);

– непосредственно к информации пользователя (к файлам, текстовой, аудио- и графической информации, полям и записям в электронных базах данных) и обусловлены возможностью нарушения ее конфиденциальности, целостности и доступности.

Эти угрозы могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн. Их можно объединить по условиям реализации на три группы.

Первая группа включает в себя угрозы, реализуемые в ходе загрузки операционной системы. Эти угрозы безопасности информации направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду ИСПДн. Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации.

Вторая группа – угрозы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем. Эти угрозы, как правило, направлены на выполнение непосредственно несанкционированного доступа к информации. При получении доступа в операционную среду нарушитель может воспользоваться как стандартными функциями операционной системы или какой-либо прикладной программы общего пользования (например, системы управления базами данных), так и специально созданными для выполнения несанкционированного доступа программами, например:

– программами просмотра и модификации реестра;

– программами поиска текстов в текстовых файлах по ключевым словам и копирования;

– специальными программами просмотра и копирования записей в базах данных;

– программами быстрого просмотра графических файлов, их редактирования или копирования;

– программами поддержки возможностей реконфигурации программной среды (настройки ИСПДн в интересах нарушителя) и др.

Наконец, третья группа включает в себя угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. Большая часть таких угроз – это угрозы внедрения вредоносных программ.

5.2.2 Вход в систему в обход средств защиты

При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации - определенной комбинации указанных средств.

В информационной системе должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

В информационной системе должно быть установлено и зафиксировано в организационно-распорядительных документах оператора по защите информации (задокументировано) ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за период времени, установленный оператором, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе).

В информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в информационной системе или по запросу пользователя.

Администратором безопасности в соответствии с инструкциями должны быть реализованы функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы.

Администратором в соответствии с инструкциями должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе программного обеспечения и (или) его компонентов.

Персоналом ИСПДн должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

Оператором должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам

обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

Для нейтрализации угроз входа в систему в обход средств защиты решено предпринять следующие организационные меры защиты:

- помещения, в которых размещены средства вычислительной техники, вход в помещение должен быть оснащен средствами управления доступом;
- установка программно-аппаратных СЗИ (Secret Net 7);
- опечатывание помещений с АРМ;
- усиленная идентификации/аутентификации пользователей.

5.2.3 НСД к АРМ пользователя и нелегальное использование нарушителем прав легального пользователя

В информационной системе должна обеспечиваться идентификация и аутентификация пользователей.

В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

В информационной системе должна осуществляться однозначная идентификация и аутентификация пользователей, не являющихся работниками ИСПДн (внешних пользователей), или процессов, запускаемых от имени этих пользователей.

В информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после установленного администратором времени его бездействия (неактивности) в информационной системе или по запросу пользователя.

Администратором в соответствии с инструкциями должны быть реализованы функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы.

Администратором в соответствии с инструкциями должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе программного обеспечения и (или) его компонентов.

Администратором должно осуществляться выявление (поиск), анализ и устранение уязвимостей в информационной системе.

В ИСПДн должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

В ИСПДн должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

В ИСПДн должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

Для нейтрализации угроз НСД к СВТ и нелегальное использование нарушителем прав легального пользователя решено предпринять следующие организационные меры защиты:

- применение технических средств защиты (Secret Net);
- установка "жёсткого" режима работы СЗИ;
- опломбирование стоек со средствами вычислительной техники и коммутационным оборудованием;
- распределение полномочий администраторов;

– блокирования сеанса доступа пользователя после установленного времени его бездействия (неактивности) или по запросу пользователя;

– должны быть разработаны инструкции для всех пользователей системы включающие требования по блокированию при оставлении рабочего места.

5.2.4 Использование легальным пользователем незарегистрированных носителей информации с целью несанкционированного копирования информации

В ИСПДн должен обеспечиваться учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации.

В ИСПДн в соответствии с инструкциями должны быть реализованы функции по управлению доступом к машинным носителям информации, используемым в информационной системе.

Для нейтрализации угроз использование легальным пользователем незарегистрированных носителей информации с целью несанкционированного копирования информации решено предпринять следующие методы защиты:

– настройка в СЗИ списка разрешённых внешних устройств;

– запрет в СЗИ копирования информации на внешние устройства;

– занесение в журналы учета машинных носителей информации или журналы материально-технического учета пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации;

– раздельный учет в журналах учета съемных (в том числе портативных) перезаписываемых машинных носителей информации (флэш-накопителей, съемных жестких дисков);

– определения должностных лиц, имеющих физический доступ к машинным носителям информации;

– предоставления физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей.

5.2.5 Нелегальное внедрение и использование неучтенных программ

Подсистемой защиты информации должны быть реализованы функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы.

Администратором в соответствии с инструкциями должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе программного обеспечения и (или) его компонентов.

В информационной системе должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

В ИСПДн должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

Администратором должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

Администратор должен проводиться контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

Администратор должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация).

Для нейтрализации угроз нелегальное внедрение и использование неучтенных программ решено предпринять следующие методы защиты:

– использование технических средств защиты информации;

– ограничение прав на установку программного обеспечения для пользователей ИСПДн, кроме администраторов, под контролем администратора безопасности;

– в ИСПДн предусмотреть отключение неиспользуемых портов и устройств чтения накопителей (при необходимости);

– установки программного обеспечения и его компонентов только от имени администратора;

– периодический контроль установленного (инсталлированного) программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке.

5.2.6 Разглашение, передача или утрата атрибутов разграничения доступа

В ИСПДн должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).

Администратором должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к

объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

Администратором должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

В информационной системе должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

В ИСПДн должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

В информационной системе должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации.

Для нейтрализации угроз разглашение, передача или утрата атрибутов разграничения доступа решено предпринять следующие методы защиты:

- разделения полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИСПДн, в соответствии с их должностными обязанностями (функциями);
- доступ к объектам доступа с учетом разделения полномочий;
- применение технических средств защиты от НСД (Secret Net);
- применение антивирусного ПО (антивирус Касперского)

– планирования и проведения мероприятий по реагированию на выявленные инциденты безопасности, в случае выявление признаков инцидентов безопасности;

– учета физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

– периодическая смена атрибутов доступа.

5.2.7 Действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, саботаж, и т.п.)

В ИСПДн должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

Администратором должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация).

В ИСПДн должно обеспечиваться использование отказоустойчивых технических средств.

В ИСПДн должно обеспечиваться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы.

Администратором должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

В ИСПДн должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации.

В ИСПДн должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала.

В ИСПДн должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

В ИСПДн должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

В информационной системе должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации.

В информационной системе должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

Для нейтрализации угроз действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, саботаж, и т.п.) решено предпринять следующие методы защиты:

– использование технических средств защиты информации (Secret Net);

– применение антивирусного ПО (антивирус Касперского);

– планирования и проведения мероприятий по реагированию на выявленные инциденты безопасности, в случае выявление признаков инцидентов безопасности;

– контроля соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ИСПДн и принятие мер, направленных на устранение выявленных недостатков;

– настройка в СЗИ системы контроля целостности;

– настройка режима мониторинга системы в процессе работы;

– определения сегментов ИСПДн, в которых должно осуществляться резервирование технических средств, программного обеспечения, каналов передачи информации и средств обеспечения функционирования, а также перечня резервируемых средств.

5.2.8 Проявление ошибок программно-аппаратных средств

В ИСПДн должно обеспечиваться резервирование технических средств.

В ИСПДн должно обеспечиваться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы.

Администратором должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

В ИСПДн должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации.

В ИСПДн должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала.

В информационной системе должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

Для нейтрализации угроз проявление ошибок программно-аппаратных средств решено предпринять следующие методы защиты:

- определения сегментов ИСПДн, в которых должно осуществляться резервирование технических средств, программного обеспечения, каналов передачи информации и средств обеспечения функционирования, а также перечня резервируемых средств;
- ввод в действие резервного технического средства, программного обеспечения, канала передачи информации или средства обеспечения функционирования при нарушении функционирования ИСПДн;
- тестирование ПО на соответствие нормативной документации;
- настройка системы мониторинга работы ПО.

5.2.9 Действия, приводящие к частичному или полному отказу СВТ или разрушению аппаратных, программных, информационных ресурсов СВТ (порча оборудования, носителей информации, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.)

В ИСПДн должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

Администратором должен проводиться контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

В ИСПДн должно обеспечиваться использование отказоустойчивых технических средств.

В ИСПДн должно обеспечиваться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы.

Администратор должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

В ИСПДн должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации.

В ИСПДн должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала.

В ИСПДн должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

Администратором должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования

информационной системы и помещения и сооружения, в которых они установлены.

В ИСПДн должна осуществляться защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

В информационной системе должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

Для нейтрализации угроз действий, приводящих к частичному или полному отказу СВТ или разрушению аппаратных, программных, информационных ресурсов СВТ (порча оборудования, носителей информации, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.) решено предпринять следующие методы защиты:

– для защиты аппаратных СВТ необходимо предпринять организационные меры, включающие в себя установку замков на дверях, определение контролируемой зоны, организация постов охраны, а так же меры по разграничению доступа в помещения;

– для защиты программных СВТ необходимо проводить контроль целостности через СЗИ, резервное копирование и запрет на изменение настроек через запрет на системные диски и в панель управления;

– для защиты от искажения файлов необходимо ограничить прямой и косвенный доступ к ним.

5.2.10 Угрозы внедрения вредоносного ПО

В ИСПДн должны быть реализованы функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы.

Администратором должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе программного обеспечения и (или) его компонентов.

В ИСПДн должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

В ИСПДн должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Администратором должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов).

Администратором должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

В ИСПДн должен проводиться контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

Администратором должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация).

В информационной системе должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

В ИСПДн должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

В информационной системе должны обеспечиваться реализация и управление антивирусной защитой в виртуальной инфраструктуре.

Для нейтрализации угрозы внедрения вредоносного ПО решено предпринять следующие методы защиты:

– использование технических средств защиты (Secret Net);

– применение антивирусного ПО (антивирус Касперского);

– необходимо предпринять организационные меры по запрету на использование незарегистрированных носителей;

– необходимо установить выделенный ПК, не подключенный к сети в котором необходимо производить предварительную проверку носителя.

5.3 Угрозы удаленного доступа (в локальной сети)

5.3.1 Описание

Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Эти угрозы реализуются относительно ИСПДн как на базе автоматизированного рабочего места, не включенного в сети связи общего пользования, так и применительно ко всем ИСПДн, имеющим подключение к сетям связи общего пользования и сетям международного информационного обмена.

Угрозы создания нештатных режимов работы программных (программноаппаратных) средств – это угрозы «Отказа в обслуживании». Как правило, данные угрозы рассматриваются применительно к ИСПДн на базе

локальных и распределенных информационных систем вне зависимости от подключения информационного обмена. Их реализация обусловлена тем, что при разработке системного или прикладного программного обеспечения не учитывается возможность преднамеренных действий по целенаправленному изменению:

– содержания служебной информации в пакетах сообщений, передаваемых по сети;

– условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);

– форматов представления данных (с несоответствием измененных форматов, установленных для обработки по протоколам сетевого взаимодействия);

– программного обеспечения обработки данных.

5.3.2 Анализ сетевого трафика

В информационной системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы.

В ИСПДн должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

В ИСПДн должны обеспечиваться регламентация и контроль использования в информационной системе технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в информационной системе.

В ИСПДн должны обеспечиваться регламентация и контроль использования в информационной системе мобильных технических средств, направленные на защиту информации в информационной системе.

В ИСПДн должно осуществляться разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечиваться защита периметров сегментов информационной системы.

Для нейтрализации угрозы анализа сетевого трафика решено предпринять следующие методы защиты:

– использование технических средств защиты (Secret Net, межсетевой экран – ССПТ-2);

– ограничения на использование технологий беспроводного доступа и предоставление его только тем пользователям которым он необходим;

– использование физически защищённых выделенных сетей.

5.3.3 Угрозы выявления паролей

В информационной системе должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками оператора.

В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

В информационной системе должна осуществляться однозначная идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей), или процессов, запускаемых от имени этих пользователей.

В информационной системе должно быть установлено и зафиксировано в организационно-распорядительных документах оператора по защите информации (задокументировано) ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за период времени, установленный оператором, а также обеспечено

блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе).

Администратором должны быть реализованы функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы.

Администратором должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе программного обеспечения и (или) его компонентов.

В ИСПДн должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

В ИСПДн должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

В ИСПДн должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

Для нейтрализации угрозы выявления паролей решено предпринять следующие методы защиты:

– использование двойных паролей;

– установление организационных требований к длине пароля и к его синтаксису;

– периодическая смена паролей.

5.3.4Администрирование с нарушением требований нормативной и технической документации, в т.ч. ошибки администрирования

В ИСПДн должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).

В ИСПДн должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

В ИСПДн должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

Администратором должен проводиться контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

В информационной системе должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

В ИСПДн должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

В ИСПДн должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации.

В ИСПДн должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала.

В информационной системе должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации(функций безопасности) и функциональных возможностей пользователей по обработке информации.

В информационной системе должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

Для нейтрализации угрозы администрирования с нарушением требований нормативной и технической документации, в т.ч. ошибки администрирования решено предпринять следующие методы защиты:

– организовать ведение журналов, регистрируя действия администраторов и другого персонала;

– организовать экспертные комиссии по проверке и анализу правильности настроек.

5.3.5 Незаконное подключение к линиям связи с целью модификации передаваемых сообщений, подмены законного пользователя, перехвата всего потока данных с целью его дальнейшего анализа и т.п.

В информационной системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы.

В ИСПДн должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

В ИСПДн должны обеспечиваться регламентация и контроль использования в информационной системе технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в информационной системе.

В ИСПДн должны обеспечиваться регламентация и контроль использования в информационной системе мобильных технических средств, направленные на защиту информации в информационной системе.

В ИСПДн должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

В ИСПДн должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

В ИСПДн должно осуществляться разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечиваться защита периметров сегментов информационной системы.

Для нейтрализации угрозы незаконного подключения к линиям связи с целью модификации передаваемых сообщений, подмены законного пользователя, перехвата всего потока данных с целью его дальнейшего анализа и т.п. решено предпринять следующие методы защиты:

– использование технических средств защиты (Secret Net, межсетевой экран – ССПТ-2);

– сегментирование локально вычислительной сети с использованием межсетевых экранов ССПТ-2, позволяющие разделить локально вычислительную сеть объекта на сегменты обрабатывающие персональные данные и не обрабатывающие персональные данные;

– управления информационными потоками, обеспечивающим блокирование передачи защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи;

– использование физически защищённых выделенных сетей.

5.3.6 Навязывание ложного маршрута сети

В информационной системе до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

В информационной системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы.

В ИСПДн должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего

пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

В ИСПДн должны обеспечиваться регламентация и контроль использования в информационной системе технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в информационной системе.

В ИСПДн должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация).

В информационной системе должно осуществляться обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов.

Для нейтрализации угрозы навязывания ложного маршрута сети решено предпринять следующие методы защиты:

– использование выделенных линий;

– использование протоколов статической маршрутизации (по заранее разработанным таблицам маршрутизации).

5.3.7 Повреждение линий связи

В ИСПДн должно обеспечиваться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы.

В ИСПДн должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

Для нейтрализации угрозы повреждения линий связи необходимо построение альтернативной локально вычислительной сети с использованием резервирования коммутационного оборудования и линий связи.

5.3.8 Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.

В информационной системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы.

В ИСПДн должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием систем обнаружения вторжений.

Администратором должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений, применяемой в информационной системе.

В ИСПДн должно осуществляться разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечиваться защита периметров сегментов информационной системы.

5.3.9 Нарушение процедуры аутентификации субъектов виртуализированного информационного взаимодействия

Для нейтрализации угрозы нарушение процедуры аутентификации субъектов виртуализированного информационного взаимодействия решено предпринять следующие методы защиты:

- использование технических средств защиты (vGate, Secret Net);

– идентификации и аутентификации администраторов управления средствами виртуализации;

– идентификации и аутентификации субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;

– блокировки доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации.

5.3.10 Атака на гипервизор с виртуальной машины

Для нейтрализации угрозы атака на гипервизор с виртуальной машины решено предпринять следующие методы защиты:

– установка ограничения числа входящих запросов;

– применение сертифицированных средств защиты виртуальной среды (vGate);

– контроль расхода ресурсов.

5.3.11 Нарушение работоспособности информационных систем, построенных на основе технологии виртуализации, за счет НСД к средствам виртуализации

Перехват управления в сети виртуализации

В информационной системе должны обеспечиваться идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.

В информационной системе должно обеспечиваться управление доступом субъектов доступа к объектам доступа, в том числе внутри виртуальных машин.

В информационной системе должна обеспечиваться регистрация событий безопасности в виртуальной инфраструктуре.

Для нейтрализации угрозы перехват управления в сети виртуализации решено предпринять следующие методы защиты:

- защита среды виртуализации средствами СЗИ (vGate, Secret Net);
- установка ограничения числа допустимых процессов;
- мониторинг целостности среды виртуализации;
- периодическая аутентификация устройства управления при взаимодействии с средой виртуализации.

5.3.12 Визуальный съем информации при вводе аутентифицирующих данных

В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

В ИСПДн должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

В ИСПДн должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

В ИСПДн должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

Для нейтрализации угрозы визуального съема информации при вводе аутентифицирующих данных решено предпринять следующие методы защиты:

– запрет на отображение информации о вводимом пароле на экран монитора;

– исключение нахождения посторонних лиц при вводе аутентифицирующих данных;

– усиленная аутентификация(етокен);

– ограничение доступа в помещение;

– установка на окна жалюзи.

5.4 Прочие угрозы

5.4.1 Нелегальное подключение неучтенных технических средств

В ИСПДн должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации.

В ИСПДн должны быть реализованы функции по управлению доступом к машинным носителям информации, используемым в информационной системе.

В ИСПДн должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

В ИСПДн должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

Для нейтрализации угрозы нелегальное подключение неучтенных технических средств решено предпринять следующие методы защиты:

– отключение неиспользуемых портов коммутационного оборудования;

– опечатывание и опломбирование шкафов с коммутационным оборудованием;

– настройка отключения на аппаратном уровне неиспользуемых портов.

5.4.2 Хищение съемных носителей с защищаемой информацией

В ИСПДн должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации.

В ИСПДн должны быть реализованы функции по управлению доступом к машинным носителям информации, используемым в информационной системе.

В ИСПДн должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

Для нейтрализации угрозы хищение съемных носителей с защищаемой информацией решено предпринять следующие методы защиты:

– необходимо установить сейфы для хранения носителей;

– выдачу носителей с отметкой в журнале.

6 Средства защиты информации для обеспечения требуемого уровня защищенности распределенной ИСПДн

6.1 Средства защиты от НСД

6.1.1 Secret Net 7

Secret Net 7 — сертифицированное средство защиты информации от несанкционированного доступа (СЗИ от НСД) для операционных систем (ОС) семейства Microsoft Windows.

Назначение Secret Net 7

Secret Net является сертифицированным средством защиты информации от несанкционированного доступа и позволяет привести автоматизированные системы в соответствие требованиям регулирующего документа №152-ФЗ («О персональных данных»);

Возможности Secret Net 7:

- аутентификация пользователей;
- разграничение доступа пользователей к информации и ресурсам автоматизированной системы;
- доверенная информационная среда;
- контроль утечек и каналов распространения конфиденциальной информации;
- контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации;
- централизованное управление системой защиты, оперативный мониторинг и аудит безопасности;
- масштабируемая система защиты, возможность применения Secret Net (сетевой вариант) в организации с большим количеством филиалов;

– защита терминальной инфраструктуры и поддержка технологий виртуализации рабочих столов (VDI).

Варианты развертывания Secret Net 7:

– автономный режим – предназначен для защиты небольшого количества (до 20-25) рабочих станций и серверов. При этом каждая машина администрируется локально;

– сетевой режим (с централизованным управлением) – предназначен для развертывания в доменной сети с Active Directory. Данный вариант имеет средства централизованного управления и позволяет применить политики безопасности в масштабах организации. Сетевой вариант Secret Net может быть успешно развернут в сложной доменной сети (domain tree/forest).

6.1.2 Dallas Lock 8.0

СЗИ Dallas Lock 8.0-C – система защиты информации от несанкционированного доступа и от раскрытия информации ограниченного доступа до уровня «совершенно секретно». Представляет собой программный комплекс средств защиты информации в ОС семейства Windows с возможностью подключения аппаратных идентификаторов.

Назначение:

– создание защищенных автоматизированных систем до класса защищенности 1Б включительно (Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992))[12];

– обеспечение 1 уровня защищенности персональных данных (Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных»)[13];

– защита информации в государственных информационных системах 1 класса защищенности (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»)[7];

– создании защищенных информационных систем управления производственными и технологическими процессами (АСУ ТП) на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»)[14].

Обеспечивает:

– защиту информации от несанкционированного доступа на персональных компьютерах, портативных и мобильных компьютерах (ноутбуках и планшетных ПК), серверах (файловых, контроллерах домена и терминального доступа), работающих как автономно, так и в составе ЛВС. Поддерживает виртуальные среды;

– дискреционный и мандатный принципы разграничения доступа к информационным ресурсам и подключаемым устройствам;

– аудит действий пользователей – санкционированных и без соответствующих прав, ведение журналов регистрации событий;

– контроль целостности файловой системы, программно-аппаратной среды и реестра;

– объединение защищенных ПК для централизованного управления механизмами безопасности;

– приведение АС, ГИС, АСУ ТП и систем обработки ПДн в соответствие законодательству РФ по защите информации.

После рассмотрения на рынке средств защиты от НСД, а именно Secret Net 7 и Dallas Lock, и рассмотрев их возможности можно сделать вывод, что для разрабатываемой ИСПДн и нейтрализации в ней актуальных угроз больше подходит средство Secret Net 7. Secret Net 7 подходит из-за то что, его возможности более обширные и оно способно обхватывать больший круг угроз. С помощью Secret Net 7 возможно предотвратить такие актуальные угрозы как:

– вход в систему в обход средств защиты;

– НСД к АРМ пользователя и нелегальное использование нарушителем прав легального пользователя;

– разглашение, передача или утрата атрибутов разграничения доступа;

– действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, саботаж, и т.п.);

– угрозы внедрения вредоносного ПО;

– анализ сетевого трафика;

– незаконное подключение к линиям связи с целью модификации передаваемых сообщений, подмены законного пользователя, перехвата всего потока данных с целью его дальнейшего анализа и т.п.;

– нарушение процедуры аутентификации субъектов виртуализированного информационного взаимодействия;

– перехват управления в сети виртуализации.

Установка и настройка средства защиты от НСД (Secret Net 7) описаны в приложение А.

6.2 Антивирусное обеспечение

6.2.1 Назначение антивирусного обеспечения

Антивирусная программа (антивирус) — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Компьютерная сеть современных крупных компаний состоит, как правило, из серверных кластеров, терминальных серверов и файловых хранилищ. Подобная инфраструктура требует высочайшего уровня защиты. Для защиты файловых серверов необходимо специальное ПО, которое не просто защищает данные от новейших вредоносных программ, но также обеспечивает бесперебойную работу сервера в условиях значительных нагрузок, и при этом оказывает минимальное влияние на работу сети. Рассмотрим такие антивирусные средства как Kaspersky Security Center 10 и Dr.Web.

6.2.2 Kaspersky Security Center 10

Kaspersky Endpoint Security предоставляет средства повышения эффективности системного администрирования и передовые технологии обеспечения безопасности. Единая консоль управления сочетает в себе простоту и удобство защиты корпоративной IT-инфраструктуры.

Эффективность технологий «Лаборатории Касперского» для защиты от вредоносного ПО признана во всем мире. Продукт Kaspersky Endpoint Security сочетает в себе сигнатурные, проактивные и облачные технологии, что обеспечивает предприятию высочайшую степень защиты от вредоносных программ.

Kaspersky Endpoint Security предоставляет защиту от вредоносных программ для широкого спектра платформ, в том числе Mac, Linux и Windows (включая Windows 8). Это позволяет обеспечивать комплексную безопасность мультиплатформенной сети.

В мире постоянно появляются так называемые угрозы «нулевого дня», для которых еще не разработаны защитные механизмы. «Лаборатория Касперского» выпускает обновления соответствующей базы данных намного чаще, чем многие другие поставщики средств защиты. Технология сигнатур-шаблонов повышает эффективность обнаружения угроз и позволяет создавать меньшие по размеру файлы обновлений. Это обеспечивает надежную защиту и снижает нагрузку на системы.

Информация о новых вредоносных программах появляется в базе системы быстрого обнаружения (UDS) еще до выпуска сигнатур, что обеспечивает своевременную и эффективную защиту от самых новых угроз IT-безопасности.

Функция проактивной защиты Мониторинг системы «Лаборатории Касперского» анализирует поведение каждой программы, которая запускается на компьютере корпоративной сети. При обнаружении подозрительной активности программа будет автоматически заблокирована.

Технология лечения активного заражения «Лаборатории Касперского» нейтрализует вредоносные объекты, работая на самых низких уровнях операционной системы.

Миллионы пользователей продуктов «Лаборатории Касперского» разрешили облачной сети Kaspersky Security Network автоматически собирать информацию о возможных заражениях вредоносным ПО или о подозрительном поведении программ в их системах. Каждый день «Лаборатории Касперского» получает более 25 миллионов образцов в режиме реального времени, анализирует новые IT-угрозы и разрабатывает необходимые для эффективной защиты обновления баз и программных модулей. Кроме того, использование Kaspersky Security Network минимизирует ложных срабатываний. Продукт реагирует только на вредоносное ПО, не мешая работе пользователя.

Система предотвращения вторжений (Host-based Intrusion Prevention System, HIPS) и сетевой экран позволяют контролировать входящий и исходящий трафик, задавая параметры для отдельных портов, IP-адресов или программ.

Функция защиты от сетевых атак служит для отслеживания подозрительной сетевой активности. При обнаружении попытки атаки она реагирует согласно заранее определенным критериям.

Kaspersky Endpoint Security обеспечивает защиту файловых серверов под управлением Windows, Linux, Novell NetWare и FreeBSD, терминальных серверов, таких как Citrix или Microsoft, а также работает на кластерных серверах. Благодаря мощному антивирусному ядру и оптимизированному процессу проверки решение не оказывает существенного влияния на производительность систем.

Гибкие возможности управления и формирования отчетов помогают эффективно обеспечивать безопасность файловых серверов, при этом сокращая временные затраты на администрирование и отчетность.

Предоставляя удаленный доступ к любому компьютеру в корпоративной сети, Kaspersky Endpoint Security помогает администраторам эффективно решать различные проблемы. Более того, если вам необходимо развертывать

новое программное обеспечение в другом офисе, вы можете назначить одну из локальных рабочих станций узлом для приема и распределения обновлений для всего офиса и таким образом уменьшить нагрузку на вашу сеть.

При подключении гостевых устройств к вашей сети Kaspersky Endpoint Security защитит ее от проникновения вредоносного программного обеспечения. Все устройства, автоматически обнаруживаемые в сети, разделяются на личные и гостевые. Личные устройства сотрудников проверяются на соответствие политикам безопасности, а для гостевых устройств определяются ограничения доступа. Гостевой доступ можно настроить, например, разрешая только выход в интернет, а не в корпоративную локальную сеть, или совсем запретить доступ.

6.2.3 Dr.Web

Dr.Web (рус. Доктор Веб) — общее название семейства программного антивирусного ПО для различных платформ (Windows, OS X, Linux, мобильные платформы) и линейки программно-аппаратных решений (Dr.Web Office Shield), а также решений для обеспечения безопасности всех узлов корпоративной сети (Dr.Web Enterprise Suite). Разрабатывается компанией «Доктор Веб».

Продукты предоставляют защиту от вирусов, троянского, шпионского и рекламного ПО, червей, руткитов, хакерских утилит, программ-шуток, а также неизвестных угроз с помощью различных технологий реального времени и превентивной защиты.

Особенности:

– возможность установки на зараженную машину;

– обнаружение и лечение сложных полиморфных, шифрованных вирусов и руткитов;

– возможность настройки копирования важных данных в защищённое хранилище позволяет пользователям версии Dr.Web для Windows самостоятельно восстанавливать поврежденные данные без необходимости обращения в службу технической поддержки «Доктор Веб»;

– поддержка большинства существующих форматов упакованных файлов и архивов, в том числе многотомных и самораспаковывающихся архивов;

– компактная вирусная база и небольшой размер обновлений. Одна запись в вирусной базе позволяет определять до тысячи подобных вирусов;

– обновления вирусных баз производятся немедленно по мере выявления новых вирусов, до нескольких раз в час. Разработчики антивирусного продукта отказались от выпуска обновлений вирусных баз по какому-либо графику, поскольку вирусные эпидемии не подчиняются таковым;

– кроссплатформенность — используется единая вирусная база и единое ядро антивирусного сканера на разных платформах ОС;

– низкое влияние на производительность системы. Благодаря технологиям оптимизации, заведомо чистые файлы не проверяются компонентами Dr.Web, что снижает нагрузку на систему.

Рассмотрев на рынке вышеуказанные средства антивирусной защиты и сравнив их возможности следует, что для разрабатываемой распределенной ИСПДн больше подходит антивирусное средство защиты Kaspersky Security Center 10. Так как именно он способен нейтрализовать все актуальные угрозы.

Антивирус Kaspersky Security Center 10 способен нейтрализовать такие угрозы как:

– действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, саботаж, и т.п.);

– действия, приводящие к частичному или полному отказу СВТ или разрушению аппаратных, программных, информационных ресурсов СВТ (порча оборудования, носителей информации, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

– угрозы внедрения вредоносного ПО;

– администрирование с нарушением требований нормативной и технической документации, в т.ч. ошибки администрирования.

Установка и настройка антивирусного средства защиты (Kaspersky Security Center 10) описаны в приложение Б.

6.3 Средства защиты виртуальной среды

6.3.1 Описание виртуальной среды

Виртуальная среда представляет собой динамическую и сложную инфраструктуру, контроль которой с точки зрения ИБ – непростая задача. Этот класс решений предназначен для управления конфигурацией виртуальной среды и мониторинга состояния информационной безопасности, что зачастую не реализуется обычными средствами управления. К лидирующим продуктам здесь можно отнести Reflex VMC и vGate. Оба решения имеют центр правления и виртуальные устройства, размещаемые на серверах ESX/ESXi.

6.3.2 Reflex VMC

В Reflex VMC входят компоненты, которые позволяют повышать эффективность эксплуатации ресурсов виртуальной среды, обеспечивать ее защиту, расширенный мониторинг с точки зрения как ИБ, так и ИТ-операций, и управление конфигурациями. Реализует расширенные функции аудита, инвентаризацию объектов и программного обеспечения виртуальной инфраструктуры (включая установленное ПО на сами ВМ), сетевой контроль и защиту гипервизора от сетевых атак, управление конфигурациями. Решение также гарантирует применение заданных с точки зрения ИБ параметров и позволяет управлять изменениями и уязвимостями. Можно констатировать, что

это комплексные многокомпонентные продукты, отличающиеся быстрым развертыванием за счет использования virtual appliance и требующие кропотливой работы по их настройке, так как они регламентируют работу среды в целом. Решения в том числе полезны для автоматизации операций по настройке компонентов среды и контроля этого процесса с точки зрения ИБ. На текущий момент не каждая российская компания готова к применению подобных решений, но интерес к ним, несомненно, повысится с общим развитием отрасли.

6.3.3 vGate

vGate - сертифицированное средство защиты информации от несанкционированного доступа и контроля выполнения политик информационной безопасности для виртуальных инфраструктур.

Предназначен для решения следующих типовых задач:

– усиленный контроль доступа к управлению системой виртуализации;

– приведение защиты среды виртуализации в соответствие требованиям российского законодательства.

Преимущества:

– выполнение требований ФСТЭК России к защите среды виртуализации;

– ограничение доступа администраторов к данным виртуальных машин;

– автоматическая проверка и шаблоны настроек на соответствие стандартам и требованиям по безопасности;

– простота внедрения в существующую инфраструктуру.

Возможна поддержка распределённых инфраструктур, например поддержка режима VMware vCenter Linked Mode. Также есть возможность использования аппаратных ключей аутентификации администраторов, переработана система отчётов. Возможность контроля целостности файлов гостевых систем виртуальных машин и просмотра информации об изменениях в файлах и настройках виртуальных машин.

Возможности vGate

– усиленная аутентификация администраторов виртуальной инфраструктуры и администраторов информационной безопасности;
– защита средств управления виртуальной инфраструктурой от НСД;
– защита ESX-серверов от НСД;
– мандатное управление доступом;
– контроль целостности конфигурации виртуальных машин и доверенная загрузка;
– контроль доступа администраторов ВИ к данным виртуальных машин;
– регистрация событий, связанных с информационной безопасностью;
– контроль целостности и доверенная загрузка ESX-серверов;
– контроль целостности и защита от НСД компонентов СЗИ;
– централизованное управление и мониторинг.

Рассмотрев на рынке вышеуказанные средства защиты виртуальной среды и сравнив их возможности делается вывод, что для разрабатываемой нами распределенной ИСПДн больше подходит средство защиты vGate. Так как именно оно способен нейтрализовать все актуальные угрозы разрабатываемой ИСПДн.

Средство защиты виртуальной среды vGate способно нейтрализовать такие угрозы как:

– нарушение процедуры аутентификации субъектов виртуализированного информационного взаимодействия;

– атака на гипервизор с виртуальной машины;

– нарушение работоспособности информационных систем, построенных на основе технологии виртуализации, за счет НСД к средствам виртуализации;

– перехват управления в сети виртуализации.

Установка и настройка средства защиты виртуальной среды (vGate) описаны в приложение В.

6.4 Межсетевой экран

6.4.1 Назначение межсетевого экрана

Межсетевой экран, сетевой экран — это программный или программно-аппаратный комплекс компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Основная задача, которую решают межсетевые экраны — защита сети или её отдельных узлов от несанкционированного доступа посредством уязвимых мест, существующих в семействе протоколов сетевой модели OSI. Дополнительно, они помогают решать проблемы безопасности, связанные с наличием уязвимостей в ПО, которое установлено на компьютерах в сети. Большинство межсетевых экранов расположено на границе сетевого периметра, так как, в первую очередь, они предназначены для защиты внутренних хостов от внешних атак. Однако, атаки могут начинаться и с внутренних хостов, не проходя при этом через межсетевые экраны, расположенные на границе сетевого периметра. Поэтому, в настоящее время, межсетевые экраны

размещают не только на границе сетевого периметра, но и между различными сегментами сети: это обеспечивает дополнительный уровень безопасности.

6.4.2 ССПТ-2

FNP типа ССПТ-2 является межсетевым экраном нового поколения (патент РФ 2214623, патент US 7281129), реализующим функции межсетевого экрана, но при этом остающимся «невидимым» для любых протоколов и тестовых воздействий, что достигается за счет отсутствия физических и логических адресов на его фильтрующих интерфейсах.

Скрытность функционирования межсетевого экрана повышает надежность системы защиты в целом и существенно упрощает процедуру установки ССПТ-2 в существующие компьютерные сети и функционирующие на их основе информационные и телематические системы.

Технические характеристики:

– многоуровневая скрытная фильтрация пакетов по совокупности критериев;

– контроль транспортных соединений (до 40000 TCP сессий) на основе проверки соответствия каждого пакета контексту выбранной TCP сессии;

– трансляция сетевых адресов (режим NAT) в режиме «стелс» для сокрытия структуры внутренней сети с выделением «демилитаризованной зоны»;

– блокировка компьютерных flood-атак на основе фильтрации аномальной активности сетевых потоков данных;

– регистрация системных событий и полных заголовков обработанных пакетов на всех уровнях межсетевого взаимодействия;

– ведение журналов регистрации пакетов и их выгрузкапо запросам администратора сети с использованием протоколов FTP и SYSlog;

– защита каналов управления с использованием алгоритмов шифрования, реализованных в OpenSSL;

– аутентификация и авторизация администратора с помощью протокола RADIUS;

– контроль доступа к интерфейсу управления на основе списка доверенных сетевых адресов;

– синхронизация системного времени по протоколу NTP.

6.4.3 Cisco ASA 5520

Cisco ASA 5520, 5540 и 5550 являются модульными высокопроизводительными межсетевыми экранами, которые реализуют в сетях предприятий среднего бизнеса сервисы защиты в режиме высокой доступности «активный/активный» и с использованием подключения Gigabit Ethernet. Благодаря интерфейсам Gigabit Ethernet и поддержке до 200 сетей VLAN организации могут без труда развертывать устройства Cisco ASA 5520, 5540 и 5550 в нескольких зонах своей сети. По мере роста требований к обеспечению безопасности сети предприятия могут наращивать мощность устройств Cisco ASA 5520, 5540 и 5550 в соответствии с темпом своего развития, надежно защищая при этом имеющиеся инвестиции. Компании могут расширить функциональность SSL и IPsec VPN, если необходимо увеличить количество поддерживаемых мобильных сотрудников, удаленных объектов и бизнес-партнеров. Можно поддерживать до 5000 клиентов Cisco AnyConnect и (или) бесклиентских туннелей VPN. Мощность и устойчивость VPN можно повысить за счет преимуществ интегрированной кластеризации и распределения нагрузки. Cisco ASA 5520, 5540 и 5550 поддерживает до 10 межсетевых экранов в кластере, предлагая до 50 000 клиентов AnyConnect и (или) бесклиентских туннелей VPN или 2 500 туннелей IPsec VPN на кластер. В целях обеспечения непрерывности бизнеса и планирования деятельности для устройств Cisco ASA 5520, 5540 и 5550 можно использовать лицензии Cisco

VPN Flex, которые позволят администраторам планировать или работать с кратковременными «всплесками» количества одновременно подключенных удаленных пользователей Premium VPN длительностью до двух месяцев.

Современные возможности обеспечения безопасности на уровне приложений и защиты контента, предлагаемые этими межсетевыми экранами, можно расширить путем развертывания высокоэффективных функций предотвращения вторжений и нейтрализации атак, предоставляемых модулем адаптивной проверки и предотвращения атак (AIP SSM), или функций комплексной защиты от вредоносных программ, предоставляемых модулем обеспечения безопасности контента и управления услугами безопасности (CSC SSM). Используя эти дополнительные возможности учета контекста, организации могут развертывать в физическом устройстве до 100 виртуальных межсетевых экранов, поддерживающих сегментированное управление политиками безопасности на уровне подразделений. Технология виртуализации повышает степень безопасности и сокращает общие расходы на управление и поддержку при одновременной консолидации нескольких устройств защиты в единый комплекс.

Рассмотрев рынок таких СЗИ как межсетевые экраны, был выбран ССПТ2. Межсетевой экран ССПТ2 является сертифицированным средством защиты имеет НСД - 3 класс НДВ - 3 класс, а это и является главными требованиями выбора средств для разрабатываемой ИСПДн.

Межсетевой экран ССПТ-2 способен нейтрализовать такие угрозы как:

- навязывание ложного маршрута сети;
- анализ сетевого трафика;
- незаконное подключение к линиям связи с целью модификации передаваемых сообщений, подмены законного пользователя, перехвата всего потока данных с целью его дальнейшего анализа и т.п.;

– угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.

Настройка межсетевого экрана ССПТ-2 описана в приложение Г.

6.5 Система обнаружения вторжений

6.5.1 Назначение системы обнаружения вторжения

Система обнаружения вторжений (СОВ) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Соответствующий английский термин — Intrusion Detection System (IDS). Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем.

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей)

6.5.2 ФОРПОСТ 2.0

ФОРПОСТ 2.0 предназначен для автоматического выявления воздействий на контролируемую данным средством автоматизированную информационную систему, которые могут быть классифицированы как компьютерные атаки или вторжения, и блокирования развития выявленных компьютерных атак.

Возможности:

– защита информационного обмена между территориально распределёнными компонентами СОВ/СОА "Форпост" с помощью средств криптографической защиты информации (СКЗИ), в том числе отечественных, до класса КС 3 включительно;

– предотвращение развития сетевых компьютерных атак путем блокирования источников атак на активном сетевом оборудовании, удаленно управляемым по защищенному каналу управления, организованному с использованием средств криптографической защиты информации (СКЗИ), в том числе отечественных, до класса КС 3 включительно;

– контроль целостности файлов серверов и АРМов защищаемой автоматизированной информационной системы, в том числе файлов не только ОС, но и файлов, содержащих информацию, на которой и базируются информационные ресурсы;

– отслеживание действий нарушителей по отношению к информации и правам пользователей, на серверах и АРМах защищаемой автоматизированной информационной системы;

– оценка успешности компьютерной атаки и выявление успешных попыток скомпрометировать информацию в защищаемой автоматизированной информационной системы;

– отслеживание появления новых сообщений системных журналов информационных ресурсов защищаемой автоматизированной информационной системы;

– генерацию отчетов на основе содержимого журналов СОА;

– возможность неограниченной иерархической интеграции между системами обнаружения компьютерных атак на базе СОА "Форпост" версии 2.0;

– возможность централизованного обновления базы сигнатур компьютерных атак в иерархических системах на базе СОА "Форпост" версии 2.0.

6.5.3 Аргус

Аппаратно-программный комплекс обнаружения компьютерных атак «Аргус» может использоваться в АИС, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну, органов государственной власти Российской Федерации, органов государственного управления и других государственных учреждений Российской Федерации. Также может использоваться для создания автоматизированных систем до класса защищенности 1Г включительно, а также для защиты информации в информационных системах персональных данных до 1 класса включительно

Функциональность, удобство обслуживания АПК «Аргус», существенно доработана и в настоящее время он обладает широкими возможностями, предназначенными для обнаружения сетевых компьютерных атак на компоненты в АИС, построенных с использованием стека протоколов TCP/IP. Комплекс позволяет выявлять подозрительные воздействия, которые могут нанести вред наиболее критичным компонентам АИС — операционным системам и приложениям, реализующим сетевые сервисы информационной системы.

Для решения данной задачи Комплекс проводит анализ протоколов в реальном масштабе времени на скорости канала до 1 Гбит/сек. Следует отметить, что при использовании нескольких АПК «Аргус» в организации появляется возможность анализа трафика, превышающего 1Гбит/сек. В этом случае в одном сегменте сети устанавливается несколько Комплексов, данные от которых аккумулируются на сервере Система РАМС ИБ.

Для поиска компьютерных атак АПК «Аргус» выполняет сигнатурный анализ сетевого трафика, анализ протоколов, анализ аномалий, анализ по

накопленной статистике для протоколов 3-7 уровней эталонной модели взаимодействия открытых систем (ЭМВОС).

Для управления доступны два физических канала: COM-порт и Ethernet-интерфейс. По каналу Ethernet возможен доступ по протоколу Telnet и HTTP (Web-интерфейс). Web-интерфейс значительно упрощает работу оператора. Набор команд по обоим каналам управления совпадает. В случае канала управления Ethernet соответствующий порт рекомендуется включать в сеть управления, которая физически или логически (на уровне ТКО) разделена с сетью мониторинга. Комплекс представляет собой замкнутую защищенную аппаратно-программную среду на базе модифицированного ядра OpenBSD 4.7.

Комплекс дает возможность получения широкого набора статистических данных. в виде диаграмм и таблиц, которые доступны для анализа через Web-интерфейс.

Рассмотрев рынок таких СЗИ как средства обнаружения вторжения, было выбрано «ФОРПОСТ» версии 2.0.. «ФОРПОСТ» версии 2.0. является сертифицированным средством защиты. А так же возможность обработки ПДн.

Средство обнаружения вторжения «ФОРПОСТ» версии 2.0. способно нейтрализовать такие угрозы как:

– анализ сетевого трафика;

– угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др..

Настройка средства обнаружения вторжения «ФОРПОСТ» версии 2.0. описана в приложение Д.

В данном разделе выпускной квалификационной работы был произведен анализ рынка средств защиты информации для обеспечения защищенности сети передачи данных. Для анализа были взяты по несколько средств защиты каждого из раздела.

Все средства сертифицированы и в входят в «Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00», но для нашей разрабатываемый сети передачи данных распределенной ИСПДн, по определенным требованиям, были выбраны следующие средства защиты:

- средства защиты от НСД - Secret Net 7;
- антивирусные средства защиты – Kaspersky Security Center 10;
- средства защиты виртуальной среды - vGate;
- межсетевой экран – ССПТ-2;
- система обнаружения вторжения – Форпост 2.0.

Структура системы защиты объектового сегмента распределенной ИСПДн размещения на спортивном объекте с применением средств защиты представлена на рисунке 5.

Архитектура центра управления технической поддержки распределенной ИСПДн с применением средств защиты представлена на рисунке 6.

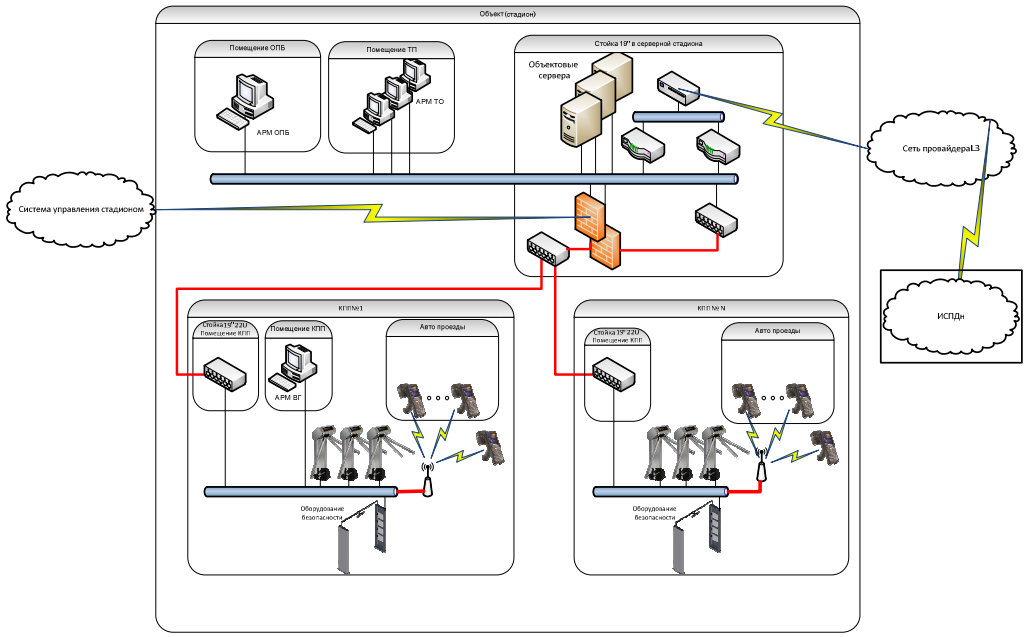

Рисунок 5 - Структура системы защиты объектового сегмента распределенной ИСПДн размещения на спортивном объекте с применением средств защиты

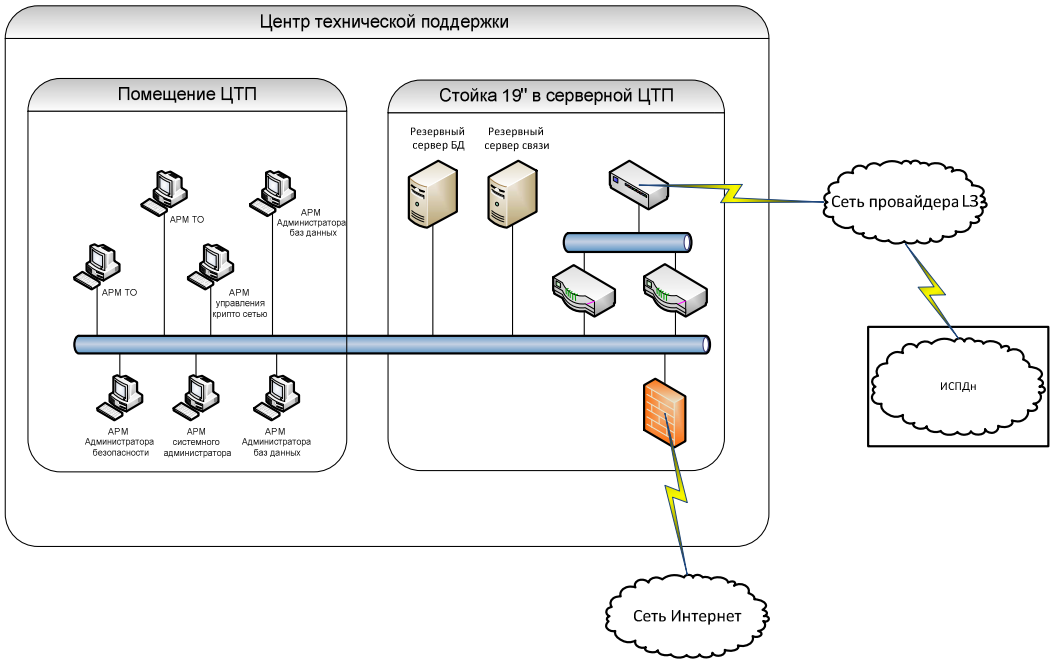

Рисунок 6 - Архитектура центра управления технической поддержки распределенной ИСПДн с применением средств защиты

ЗАКЛЮЧЕНИЕ

В ходе выполнения ВКР была достигнута цель, заданная в техническом задании, а именно – была разработана подсистема защиты информации от несанкционированного доступа в распределенной информационной системе персональных данных.

В ВКР были рассмотрены следующие вопросы:

- структура распределенной ИСПДн;
- состав распределенной ИСПДн;
- информационные потоки, циркулирующие в ИСПДн;
- на основании модели угроз были определены и выбраны средства защиты информации, обеспечивающие нейтрализацию угроз в распределенной ИСПДн;
- были разработаны требования к конфигурированию средств защиты информации;
- были разработаны организационные технические мероприятия и требования для обеспечения требуемого уровня защищенности ИСПДн.

Разработанная подсистема защиты информации от НСД в распределенной информационной системе, нейтрализует следующие актуальные угрозы:

- НСД к информации в распределенной информационной системе;
- прочие угрозы.

Средства защиты используемые в подсистеме защиты информации обеспечивают:

- выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;
- контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

– контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

– контроль состава технических средств, программного обеспечения и средств защиты информации;

– контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе.

ВКР была выполнена в полном объеме и в соответствии со всеми требованиями технического задания.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 ГОСТ 34.003-90 «Автоматизированные системы. Термины и определения».

2 Федеральный закон от 27 июля 2006 г. № 149 ФЗ «Об информации, информационных технологиях и защите информации».

3 Федеральный закон от 27 июля 2006 г. № 152 ФЗ «О персональных данных».

4 Указ Президента Российской Федерации от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

5 Постановление Правительства Российской Федерации от 02 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6 Приказ Министерства связи и массовых коммуникаций Российской Федерации от 09 января 2008 года № 1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации».

7 Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащихся в государственных информационных системах».

8 Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

9 «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 2008 г.

10 «Методика определения актуальных угроз безопасности персональных данных, обрабатываемых информационных системах персональных данных» (ФСТЭК России, 2008 г.).

11 Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

12 Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992)).

13 Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

14 Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

ПРИЛОЖЕНИЕ А

(обязательное)

Установка и настройка Secret Net 7

Варианты развертывания Secret Net 7:

- автономный режим – предназначен для защиты небольшого количества (до 20-25) рабочих станций и серверов. При этом каждая машина администрируется локально.

- сетевой режим (с централизованным управлением) – предназначен для развертывания в доменной сети с Active Directory. Данный вариант имеет средства централизованного управления и позволяет применить политики безопасности в масштабах организации. Сетевой вариант Secret Net может быть успешно развернут в сложной доменной сети (domain tree/forest).

В разрабатываемой ИСПДН Secret Net 7 будет использоваться в сетевом режиме.

Установка

1. На всех компьютерах, где будет установлено программное обеспечение СЗИ Secret Net, должен быть указан русский язык в качестве языка программ, не поддерживающих Юникод. Необходимо проверить выполнение данного требования на компьютерах. Для просмотра и изменения состояния параметра необходимо вызвать диалоговое окно "Язык и региональные стандарты" в Панели управления ОС Windows.

2. Выполним начальную установку компонентов СЗИ Secret Net:

- хранилище объектов централизованного управления будет размещаться в Active Directory, выполним модификацию схемы Active Directory;

- на серверах, которые будут функционировать в качестве серверов безопасности, устанавливаем компонент "Secret Net 7 — Сервер безопасности"

и компонент "Secret Net 7" с подчинением, установленному на компьютере серверу безопасности;

- устанавливаем компонент "Secret Net 7" на рабочем месте администратора безопасности;

- устанавливаем компонент "Secret Net 7 — Программа управления" на рабочем месте администратора безопасности.

3. Создаем папку, которая будет являться общедоступным сетевым ресурсом. Открываем общий доступ к этой папке. Дополнительно предоставляем права доступа к папке всем учетным записям компьютеров, на которые планируется устанавливать ПО клиента, или для группы "Прошедшие проверку" ("Authenticated Users"). Необходимые права обеспечиваются установленными разрешениями на чтение, чтение и выполнение и просмотр содержимого.

4. С установочного компакт-диска СЗИ Secret Net копируем в папку \Distrib содержимое следующих каталогов (сохраняя их структурную вложенность): \Setup\Client и \Tools\Microsoft. Если в системе имеются компьютеры, на которых будет использоваться средство аппаратной поддержки Secret Net Card или Secret Net Touch Memory Card, дополнительно копируем в папку \Distrib содержимое каталога \Setup\SnTmCard.

5. Создаем файл со сценарием установки, используя доменный компьютер, на котором не установлено клиентское ПО СЗИ Secret Net. Для создания файла сценария войдём в систему с правами локального администратора компьютера и выполните следующие действия:

- на локальном диске создается папка C:\ClientSN и с установочного компакт-диска СЗИ Secret Net копируется в эту папку содержимое следующих каталогов (сохраняя их структурную вложенность): \Setup\Client и \Tools\Microsoft;

- запускаем консоль командной строки (cmd.exe);

- вводим команду для запуска программы установки в режиме создания файла сценария:

а) на компьютере под управлением 32-разрядной версии Windows: start C:\ClientSN\Setup\Client\Win32\Setup.exe /script:3;

б) на компьютере под управлением 64-разрядной версии Windows: start C:\ClientSN\Setup\Client\x64\Setup.exe /script:3.

- в программе установки выполняем требуемые действия до появления на экране диалога "Готова к установке программы", после чего отмените дальнейшую установку;

- убедившись, что файл сценария SnInstall.script добавлен в каталог размещения дистрибутивных файлов (соответственно C:\ClientSN\Setup\Client\Win32 или C:\ClientSN\Setup\Client\x64).

6. Копируем файл SnInstall.script в подкаталоги \Setup\Client\Win32 и \Setup\Client\x64 общедоступной папки \Distrib на контроллере домена. После копирования файла можно удалить папку C:\ClientSN на компьютере, который использовался для создания файла сценария.

7. На рабочем месте администратора безопасности запускаем программу оперативного управления в режиме конфигурирования. Необходимо убедится в том, что на сервере безопасности зарегистрировано достаточное число лицензий для запланированного количества клиентов — для этого выбираем сервер и переходим на вкладку "Лицензии". При необходимости регистрируем дополнительные серийные номера.

8. Формируем в программе структуру оперативного управления — подчиняем серверу безопасности все компьютеры, на которых будет выполняться автоматическая установка клиента Secret Net.

9. Создаем в доменах безопасности организационные подразделения для группирования компьютеров, на которых будет выполняться автоматическая

установка ПО. Для этого на компьютере контроллера домена выполняются следующие действия:

а) в ОС Windows Server 2012/2008 — в оснастке "Управление групповой политикой" выбираем последовательно каждый контейнер, которому сопоставлен домен безопасности (весь домен Active Directory или отдельное организационное подразделение), и активируйте команду меню "Действие | Создать подразделение". В появившемся диалоге введите имя организационного подразделения "Secret Net Autosetup";

б) в ОС Windows Server 2003 — в оснастке "Active Directory — пользователи и компьютеры" выбираем последовательно каждый контейнер, которому сопоставлен домен безопасности (весь домен Active Directory или отдельное организационное подразделение), и активируйте команду меню "Действие | Создать | Подразделение". В появившемся диалоге введите имя организационного подразделения "Secret Net Autosetup".

10. Создаем групповые политики автоматической установки для подразделения (подразделений) "Secret Net Autosetup". Политики создаются отдельно для применения на 32- и 64-разрядных версиях ОС Windows. Для создания политик на компьютере контроллера домена выполняем следующие действия:

а) в ОС Windows Server 2012/2008 — в оснастке "Управление групповой политикой" выбираем последовательно каждое подразделение "Secret Net Autosetup" и создаем политики "SNAutosetup Policy Win32" и "SNAutosetup Policy x64" с помощью команды меню "Дей- ствие | Создать объект групповой политики в этом домене и связать его" (вариант англоязычного названия: "Create a GPO in this domain, and Link it here");

б) в ОС Windows Server 2003 — в оснастке "Active Directory — пользователи и компьютеры" последовательно вызываем диалоговое окно настройки свойств каждого подразделения "Secret Net Autosetup", переходим на

вкладку "Групповая политика" и создаем политики "SNAutosetup Policy Win32" и "SNAutosetup Policy x64" с помощью кнопки "Создать".

11. Настраиваем параметры выполнения сценариев групповых политик. Для этого на компьютере контроллера домена выполняем следующие действия:

а) В ОС Windows Server 2012/2008:

1. В оснастке "Управление групповой политикой" последовательно выбираем созданные политики (являются подчиненными объектами в организационных подразделениях "Secret Net Autosetup") и вызываем для каждой из них окно редактора групповых политик с помощью команды меню "Действие | Изменить".

2. В дереве объектов редактора переходим к разделу "Конфигурация компьютера\Политики\Административные шаблоны:…\Система\Сценарии". Вызовите диалоговое окно настройки свойств параметра "Указать максимальное время выполнения сценариев групповой политики" ("Specify maximum wait time for Group Policy scripts" для ОС Windows Server 2012 или "Maximum wait time for Group Policy scripts" для ОС Windows Server 2008), установливаем отметку в поле "Включено" и указываем значение "7200".

3. Вызываем диалоговое окно настройки свойств параметра "Отображать команды сценариев завершения работы во время их выполнения" ("Display instructions in shutdown scripts as they run") для ОС Windows Server 2012 или "Выполнять сценарии завершения работы с отображением команд" ("Run shutdown scripts visible") для ОС Windows Server 2008 и устанавливаем отметку в поле "Включено".

б) В ОС Windows Server 2003:

1. В оснастке "Active Directory — пользователи и компьютеры" последовательно вызоваем диалоговое окно настройки свойств каждого

подразделения "Secret Net Autosetup" и переходим на вкладку "Групповая политика".

2. Последовательно выбираем в списке каждую созданную политику и вызоваем для нее окно редактора групповых политик с помощью кнопки "Изменить".

3. В дереве объектов редактора переходим к разделу "Конфигурация компьютера\Административные шаблоны\Система\Сценарии". Вызываем диалоговое окно настройки свойств параметра "Maximum wait time for Group Policy scripts", устанавливаем отметку в поле "Включен" и указываем значение "7200".

4. Вызываем диалоговое окно настройки свойств параметра "Выполнять сценарии завершения работы с отображением команд" ("Run shutdown scripts visible") и устанавливаем отметку в поле "Включен".

12. В созданные групповые политики добавляем сценарии завершения работы. Для этого в окне редактора групповых политик (открытом на предыдущем действии) выполняем следующие действия:

в) В ОС Windows Server 2012/2008:

1. В дереве объектов редактора переходим к разделу "Конфигурация компьютера\Политики\Конфигурация Windows\Сценарии" и вызываем диалоговое окно настройки свойств параметра "Завершение работы".

2. Добавляем сценарий с помощью кнопки "Добавить". В появившемся диалоге указываем следующие значения:

- в поле "Имя сценария": \\\Distrib\Setup\Client\\Setup.exe где в качестве подкаталога необходимо указать папку размещения дистрибутивных файлов соответствующей разрядности: для политики "SNAutosetup Policy Win32" укажи- те подкаталог \Win32, а для политики "SNAutosetup Policy x64" — подкаталог \x64;

- в поле "Параметры сценария": /autoinstall.

г) В ОС Windows Server 2003:

1. В дереве объектов редактора переходим к разделу "Конфигурация компьютера\Конфигурация Windows\Сценарии" и вызываем диалоговое окно настройки свойств параметра "Завершение работы".

2. Добавляем сценарий с помощью кнопки "Добавить". В появившемся диалоге указываем следующие значения:

- в поле "Имя сценария": \\\Distrib\Setup\Client\\Setup.exe где в качестве подкаталога необходимо указать папку размещения дистрибутивных файлов соответствующей разрядности: для политики "SNAutosetup Policy Win32" указываем подкаталог \Win32, а для политики "SNAutosetup Policy x64" — подкаталог \x64;

- в поле "Параметры сценария": /autoinstall.

13. Переместим в подразделение (подразделения) "Secret Net Autosetup" те компьютеры, на которых необходимо выполнить автоматическую установку ПО. Перемещение компьютеров из других контейнеров выполняется в оснастке "Active Directory — пользователи и компьютеры" методом "Drag-and-Drop" или с помощью команды "Переместить" в контекстном меню компьютеров.

14. На рабочем месте администратора безопасности запускаем программу оперативного управления в режиме мониторинга. Используя программу для контроля процесса установки ПО на компьютерах. После успешной установки и перезагрузки компьютеров соответствующие объекты структуры оперативного управления изменяют свое состояние. В частности, изменяются пиктограммы объектов и признаки состояния.

15. После того как установка ПО произошла на всех компьютерах, в оснастке "Active Directory — пользователи и компьютеры" перемещаем компьютеры из подразделения (подразделений) "Secret Net Autosetup" обратно в исходные контейнеры.

16. После завершения автоматической установки ПО на всех предусмотренных компьютерах удалите объекты, созданные для обеспечения автоматической установки:

1. На контроллере домена удаляем папку \Distrib.

2. Удаляем подразделение (подразделения) "Secret Net Autosetup" и созданные групповые политики автоматической установки (после перемещения в исходные контейнеры всех компьютеров). Для этого на компьютере контроллера домена выполняем следующие действия:

- в ОС Windows Server 2012/2008 — в оснастке "Управление групповой политикой" переходим к разделу "Объекты групповой политики" в иерархии объектов домена и удалите политики "SNAutosetup Policy Win32" и "SNAutosetup Policy x64" с помощью команды контекстного меню "Удалить". Затем аналогичным образом удаляем подразделение (подразделения) "Secret Net Autosetup";

- в ОС Windows Server 2003 — в оснастке "Active Directory — пользователи и компьютеры" удаляем подразделение (подразделения) "Secret Net Autosetup" с помощью команды контекстного меню "Удалить".

Настройка Secret Net 7

Усиленная аутентификация пользователей

Для предотвращения НСД к СВТ и для нейтрализации актуальных угроз необходима усиленная аутентификация пользователей. Для этого в Secret Net используются:

- iButton (серия DS199x)*;
- eToken PRO, eToken PRO Java (USB, смарт-карта);
- Rutoken, Rutoken ЭЦП и Rutoken Lite;
- iKey;
- JaCarta;
- ESMART Token (USB, смарт-карта).

Рисунок А.1 - Идентификаторы

Рассмотрим усиленную настройку с использованием идентификатора eToken. Выполнив данную настройку доступ в учетную запись пользователь сможет осуществит только с использованием идентификатора.

1. В политике безопасности устанавливаем идентификацию «только по идентификатору».

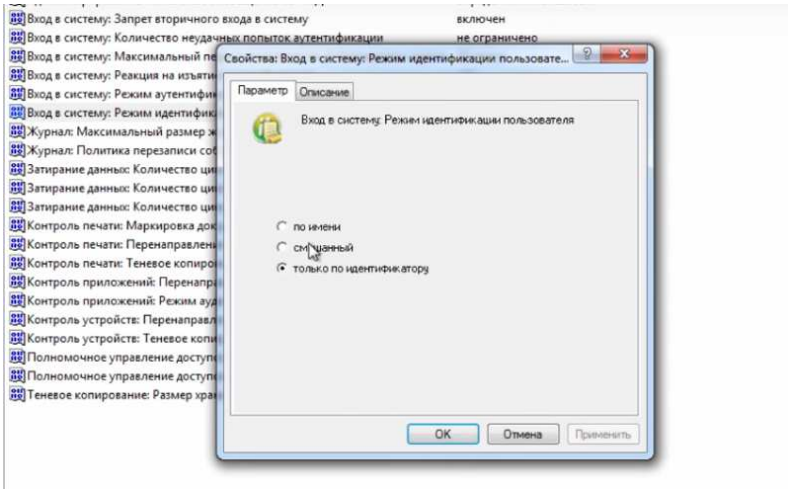

Рисунок А.2 - Выбор режима идентификации пользователя

2. Далее необходимо пользователю присвоить новый аппаратный идентификатор

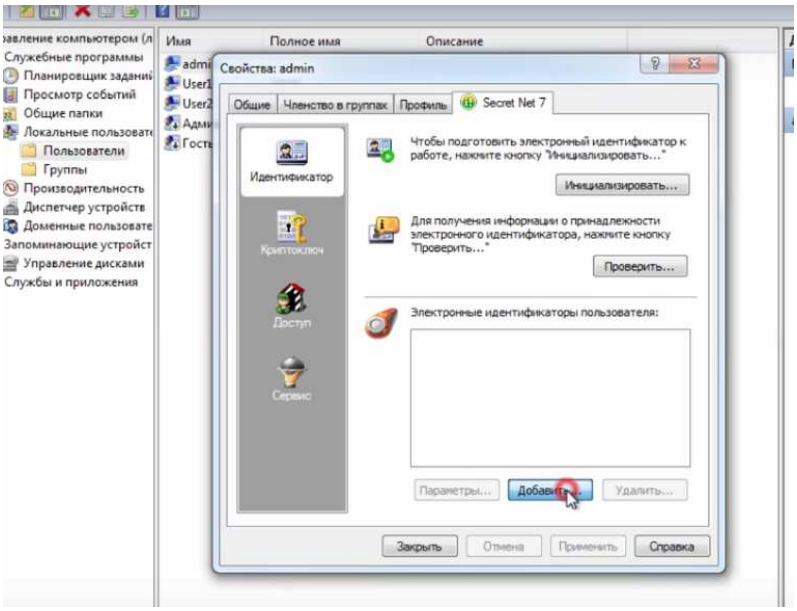

Рисунок А.3 - Присвоение нового идентификатора

3. В новый идентификатор необходимо записать закрытый ключ пользователя.

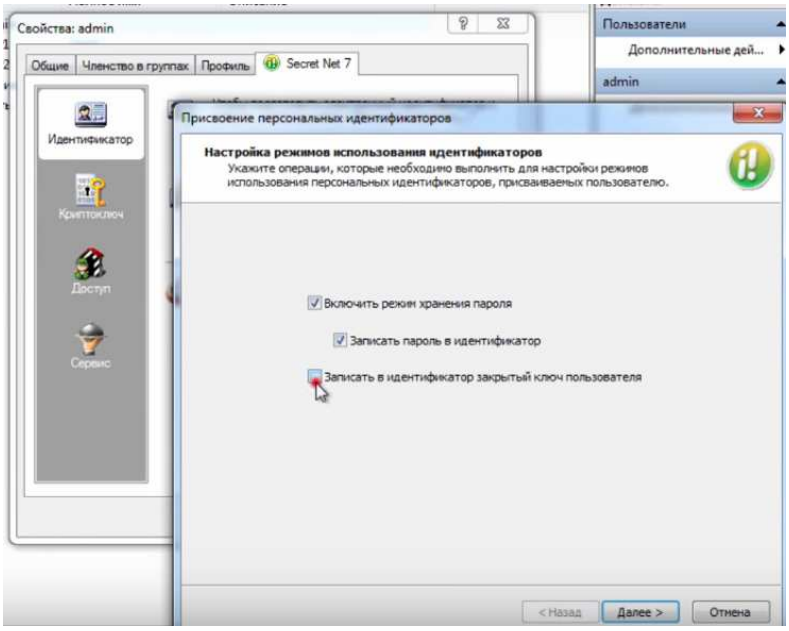

Рисунок А.4 - Настройка режимов использования идентификаторов

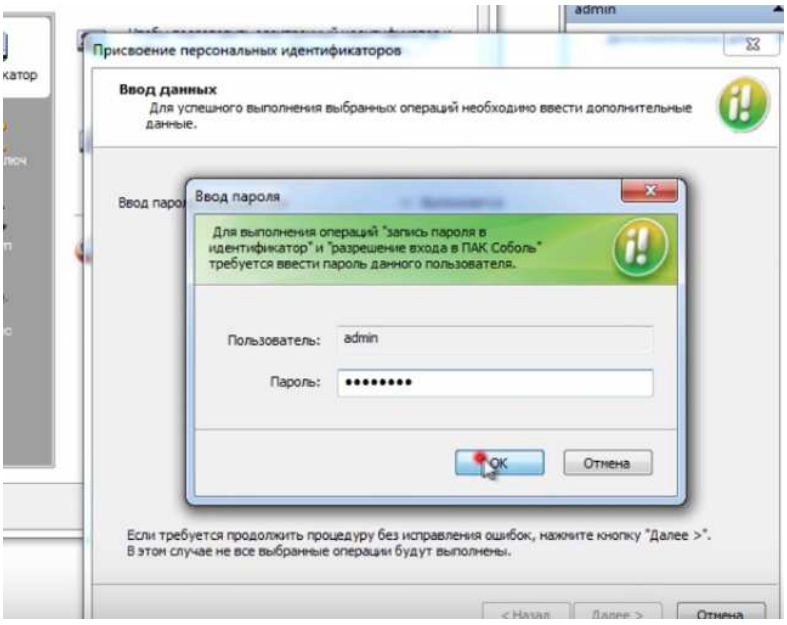

Рисунок А.5 - Присвоение пароля идентификатору

4. При успешном присвоении для пользователя пароля идентификатора программа выдает сообщение, представленное на рисунке А.6.

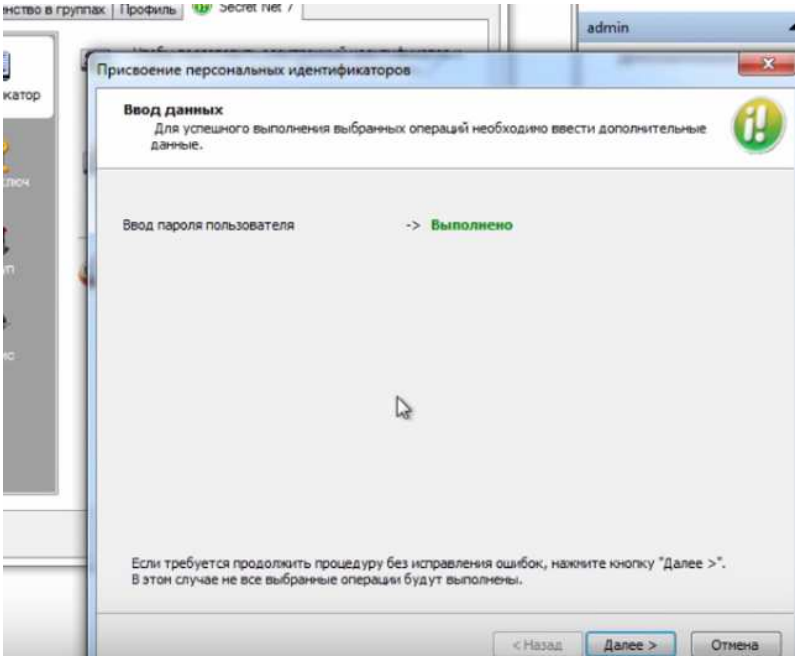

Рисунок А.6 - Сообщение об успешном присвоении для пользователя пароля идентификатора

5. Затем необходимо предъявить идентификатор для записи на него данных (закрытого ключа)

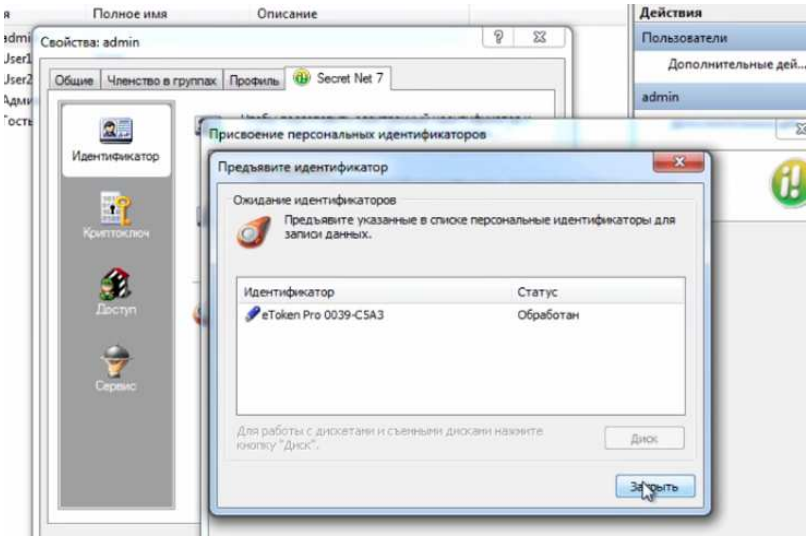

Рисунок А.7 - Запись закрытого ключа на идентификатор

При успешной записи закрытого ключа на идентификатор программа выдает сообщение, представленное на рисунке А.8.

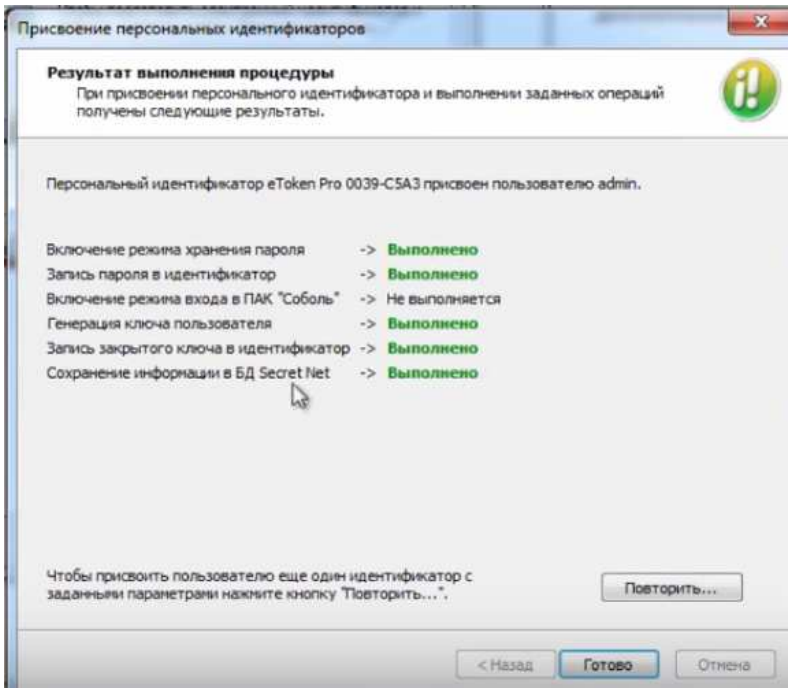

Рисунок А.8 - Сообщение об успешной записи закрытого ключа на идентификатор

6. После успешного добавления электронного идентификатора и записи на него закрытого ключа он появляется в списке

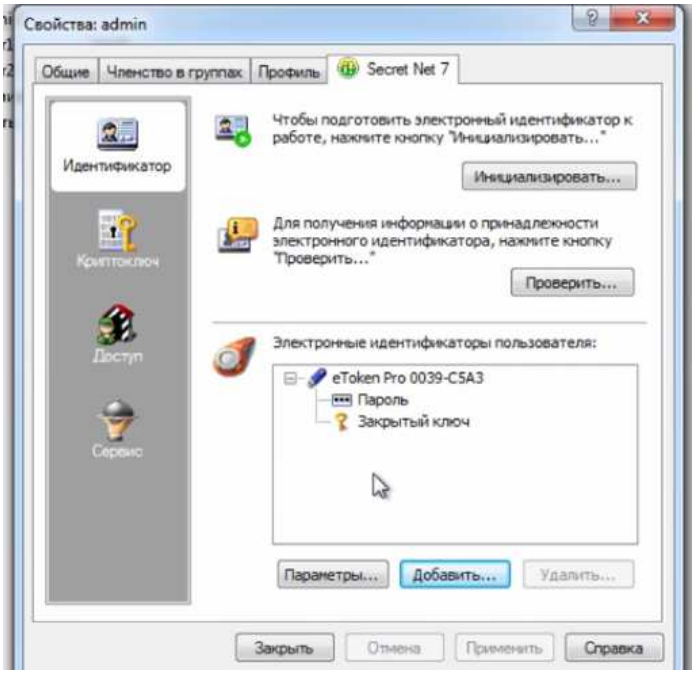

Рисунок А.9 - Окно «свойства администратора»

7. После успешного добавления нового идентификатора и записи на него закрытого ключа, необходимо в политике безопасности установить «усиленная аутентификация по ключу» как представлено на рисунке А.10.

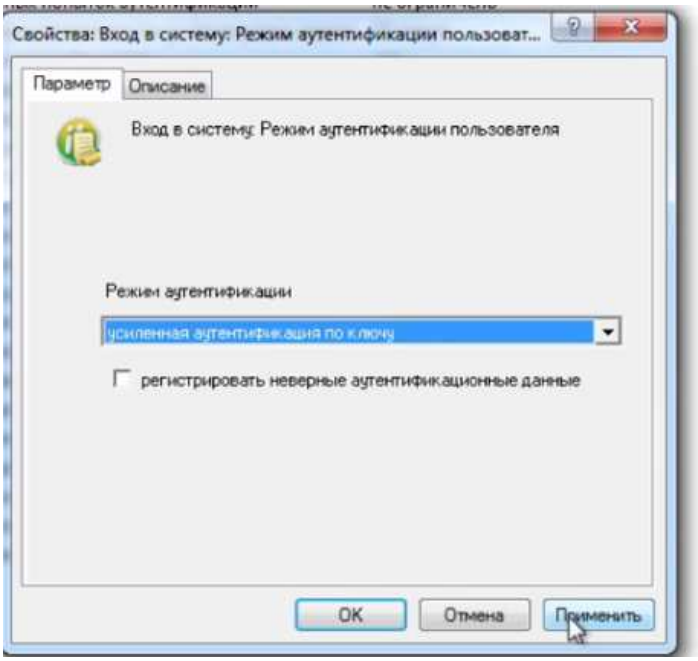

Рисунок А.10 - Настройка режима аутентификации

8. Проверка входа в систему с помощью присвоенного идентификатора представлена на рисунках А.11, А.12, А.13 и А.14.

Рисунок А.11 - Окно выбора пользователя для входа в систему

Рисунок А.12 - Сообщение, сигнализирующее о предъявление идентификатора

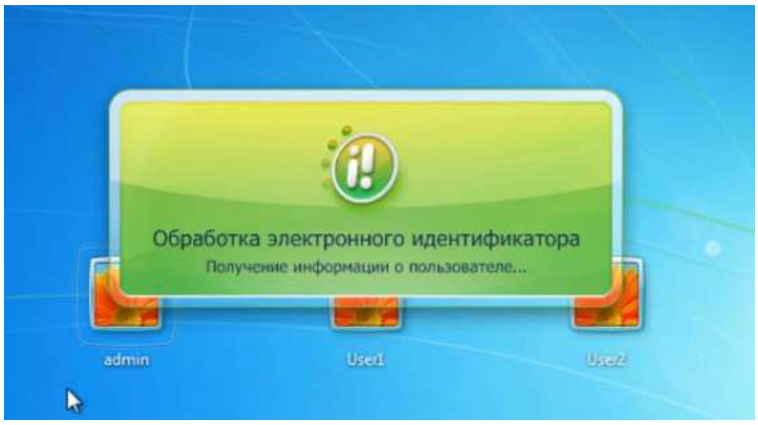

Рисунок А.13 - Обработка идентификатора

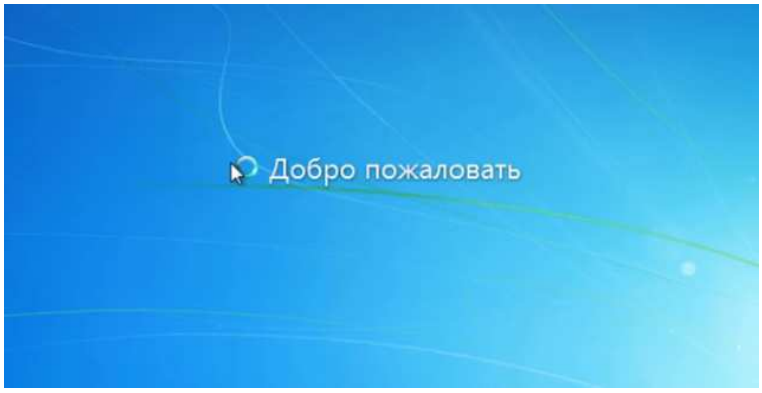

Рисунок А.14 - Успешный вход в систему

Как видно из представленных рисунков аутентификация выполнена успешно, а это значит что идентификатор и программа настроены верно.

Блокировка компьютера

Средства блокировки компьютера предназначены для предотвращения его несанкционированного использования. В этом режиме блокируются устройства ввода (клавиатура и мышь) и экран монитора.

Предусмотрены следующие варианты:

- блокировка при неудачных попытках входа в систему;

- временная блокировка компьютера;

- блокировка компьютера при срабатывании защитных подсистем (например, при нарушении функциональной целостности системы Secret Net);

- блокировка компьютера администратором оперативного управления.

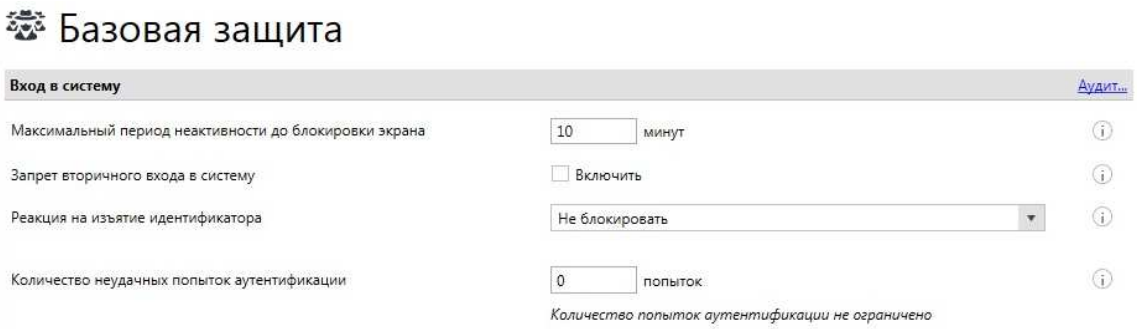

Рисунок А.15 - Настройка средств блокировки в Secret Net

Контроль целостности

Механизм контроля целостности следит за неизменностью контролируемых объектов. Контроль проводится в автоматическом режиме в соответствии с заданным расписанием. Объектами контроля могут быть файлы, каталоги, элементы системного реестра и секторы дисков (последние только при использовании ПАК «Соболь»).

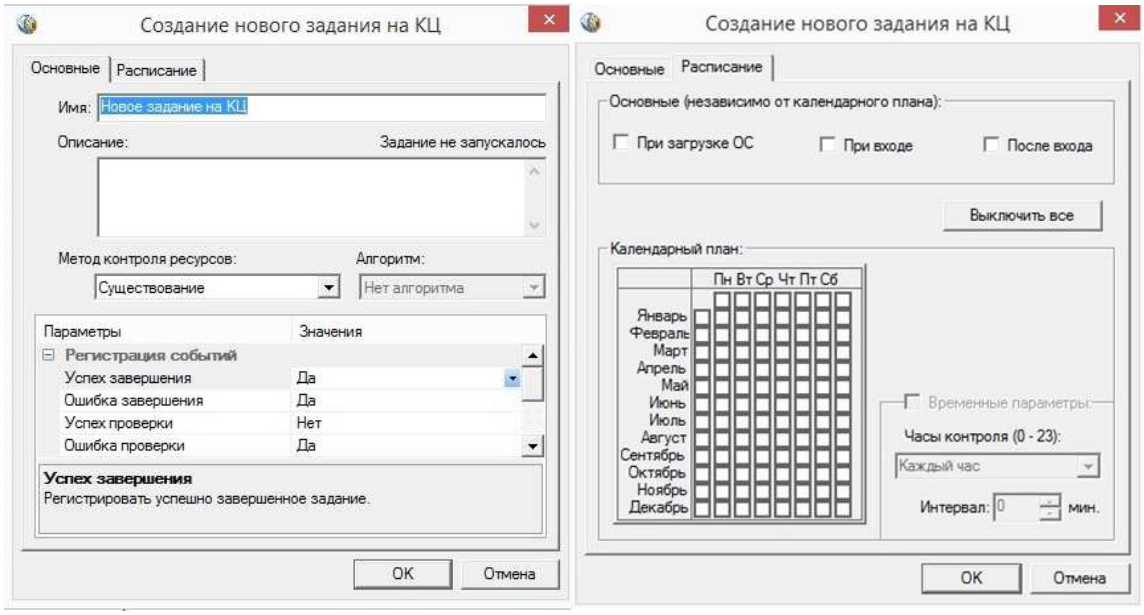

Рисунок А.6 - Создание нового задания для контроля целостности в Secret Net

При обнаружении несоответствия возможны различные варианты реакции на ситуации нарушения целостности. Например, регистрация события в журнале Secret Net и блокировка компьютера.

Вся информация об объектах, методах, расписаниях контроля сосредоточена в модели данных. Она хранится в локальной базе данных системы Secret Net и представляет собой иерархический список объектов с описанием связей между ними.

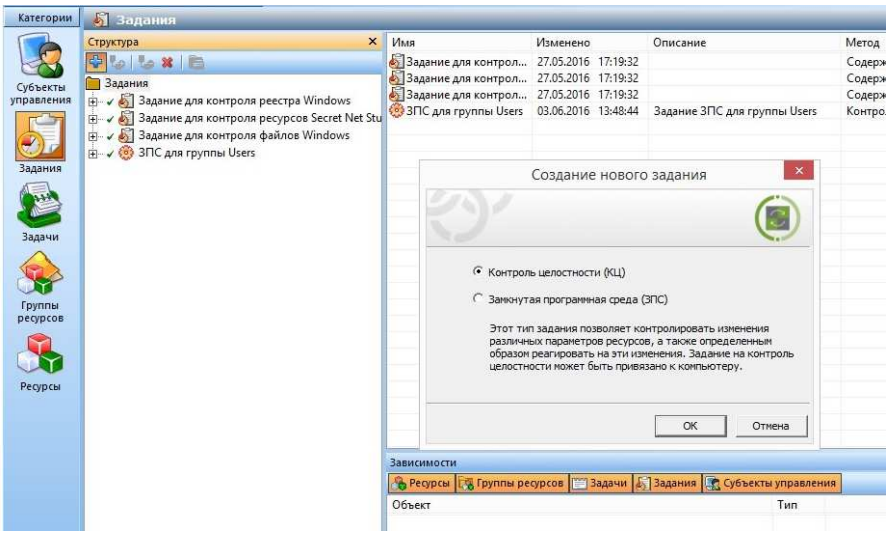

Рисунок А.17 - Создание модели данных для контроля целостности в Secret Net

Дискреционное управление доступом к ресурсам файловой системы

В состав системы Secret Net входит механизм дискреционного управления доступом к ресурсам файловой системы.

Этот механизм обеспечивает:

- разграничение доступа пользователей к каталогам и файлам на локальных дисках на основе матрицы доступа субъектов (пользователей, групп) к объектам доступа;

- контроль доступа к объектам при локальных или сетевых обращениях, включая обращения от имени системной учетной записи;

- запрет доступа к объектам в обход установленных прав доступа;

- независимость действия от встроенного механизма избирательного разграничения доступа ОС Windows.

То есть установленные права доступа к файловым объектам в системе Secret Net не влияют на аналогичные права доступа в ОС Windows и наоборот.

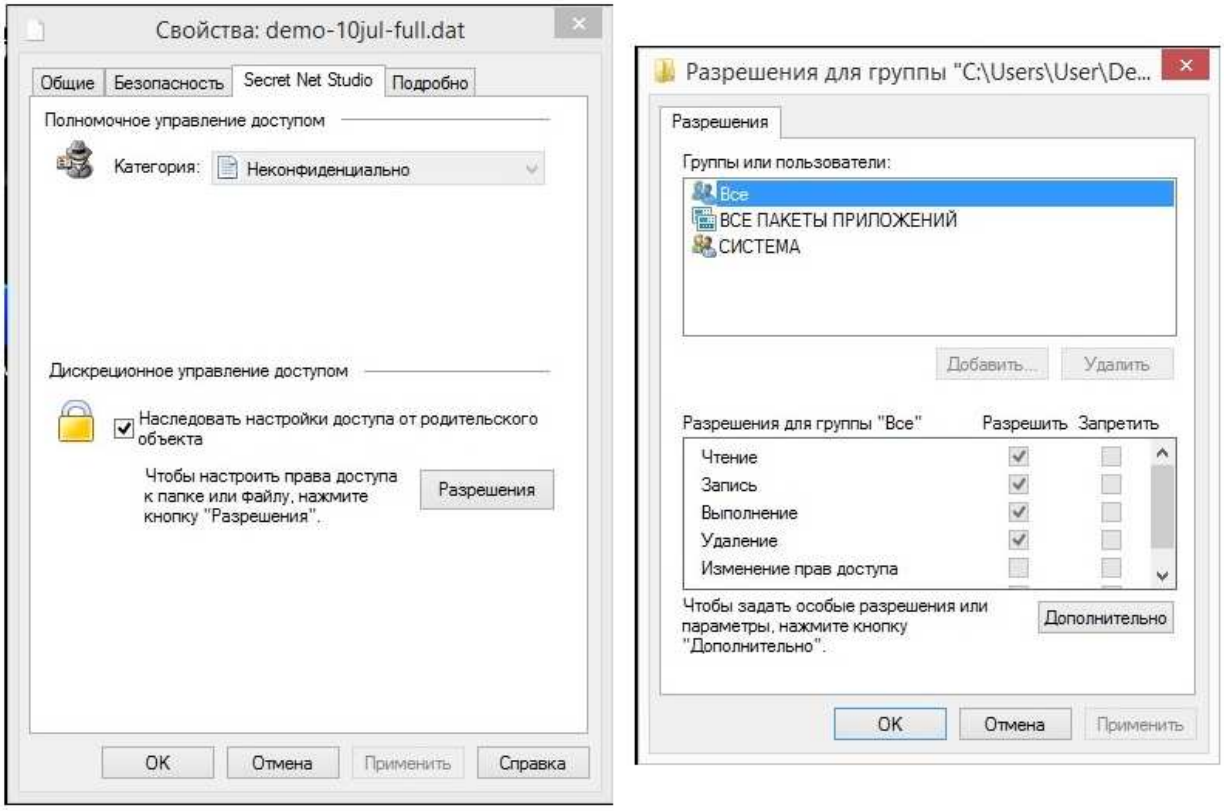

Рисунок А.18 - Настройка дискреционных прав доступа в Secret Net

Кроме того, пользователю предоставляется возможность определения учетных записей, которым даны привилегии по управлению правами доступа.

Контроль подключения и изменения устройств компьютера

Механизм контроля подключения и изменения устройств компьютера обеспечивает:

- своевременное обнаружение изменений аппаратной конфигурации компьютера и реагирование на эти изменения;

- поддержание в актуальном состоянии списка устройств компьютера, который используется механизмом разграничения доступа к устройствам.

Начальная аппаратная конфигурация компьютера определяется на этапе установки системы. Настройку политики контроля можно выполнить индивидуально для каждого устройства или применять к устройствам наследуемые параметры от моделей, классов и групп, к которым относятся устройства.

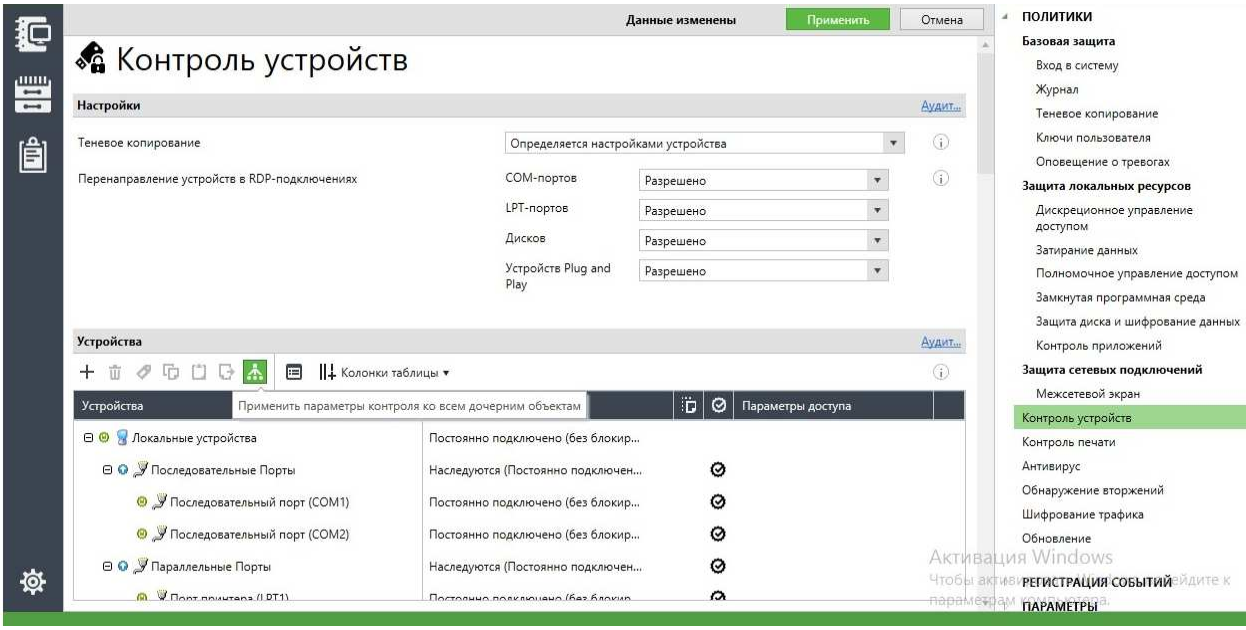

Рисунок А.19 - Настройка политики контроля устройств компьютера

При обнаружении изменений аппаратной конфигурации система требует у администратора безопасности утверждение этих изменений.

На основании формируемых списков устройств осуществляется разграничение доступа пользователей к ним: разрешение/запрет на выполнение операций и настройки уровней конфиденциальности.

Теневое копирование выводимых данных

Механизм теневого копирования обеспечивает создание в системе дубликатов данных, выводимых на отчуждаемые носители информации. Дубликаты (копии) сохраняются в специальном хранилище, доступ к которому имеют только уполномоченные пользователи. Действие механизма распространяется на те устройства, для которых включен режим сохранения копий при записи информации.

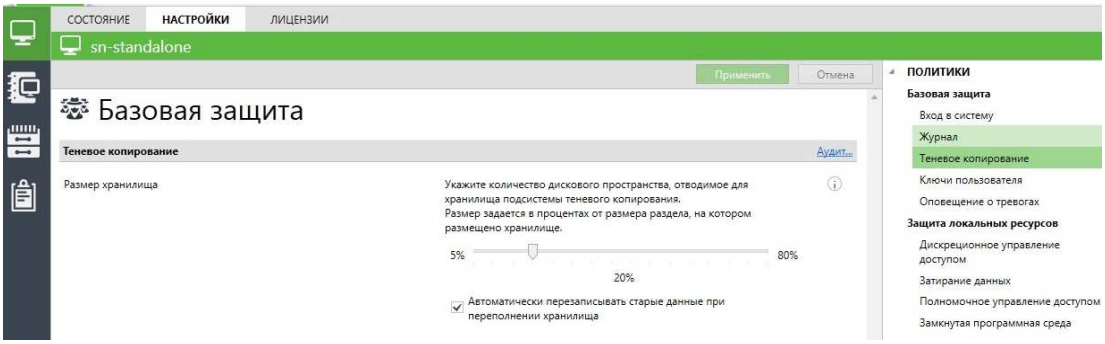

Рисунок А.20 - Настройка теневого копирования

При включенном режиме сохранения копий вывод данных на внешнее устройство возможен только при условии создания копии этих данных в хранилище теневого копирования. Если по каким-либо причинам создать дубликат невозможно, операция вывода данных блокируется.

Теневое копирование поддерживается для устройств следующих видов:

- подключаемые по USB жесткие диски, флешки и др. накопители;
- дисководы CD- и DVD-дисков с функцией записи;
- принтеры;
- дисководы гибких дисков.

ПРИЛОЖЕНИЕ Б

(обязательное)

Установка и настройка Kaspersky Security Center 10

Kaspersky Security Center 10 для Windows может быть установлен на компьютер несколькими способами:

– локальная установка – установка программы на отдельном компьютере. Для запуска и проведения локальной установки требуется непосредственный доступ к этому компьютеру. Локальная установка может быть проведена в одном из двух режимов:

а) интерактивном, с помощью мастера установки программы. Этот режим требует нашего участия в процессе установки;

б) тихом, запуск установки программы в этом режиме выполняется из командной строки, наше участие в процессе установки не требуется.

– удаленная установка – установка программы на компьютеры сети, выполняемая удаленно с рабочего места администратора с использованием:

а) программного комплекса Kaspersky Security Center;

б) редактора управления групповыми доменными политиками Microsoft Windows Server.

Перед началом установки Kaspersky Endpoint Security (в том числе и удаленной) рекомендуется закрыть все работающие программы.

Установка программы с помощью мастера установки программы

Интерфейс мастера установки программы состоит из последовательности окон (шагов). Чтобы переключаться между окнами мастера установки программы, требуется использовать кнопки Назад и Далее. Работа мастера установки программы завершается нажатием на кнопку Завершить. Чтобы прекратить работу мастера установки программы на любом этапе, следует нажать на кнопку Отмена.

ШАГ 1. Проверка соответствия системы необходимым условиям установки

Перед установкой Kaspersky Security Center 10 для Windows на компьютер или обновлением предыдущей версии программы проверяются следующие условия:

– соответствие операционной системы и пакета обновлений (Service Pack) программным требованиям для установки;

– выполнение аппаратных и программных требований;

– наличие прав на установку программного обеспечения.

Если какое-либо из перечисленных условий не выполнено, на экран выводится соответствующее уведомление. Если компьютер соответствует предъявляемым требованиям, мастер установки программы выполняет поиск программ «Лаборатории Касперского», одновременная работа которых привести к возникновению конфликтов. Если такие программы найдены, вам предлагается удалить их вручную.

ШАГ 2. Стартовое окно процедуры установки

Если условия для установки программы полностью соответствует предъявляемым требованиям, после запуска установочного пакета на экране открывается стартовое окно. Стартовое окно содержит информацию о начале установки Kaspersky Security Center на компьютер. Чтобы продолжить работу мастера установки программы, нажимаем на кнопку Далее. Чтобы прекратить работу мастера установки программы, необходимо нажать на кнопку Отмена.

ШАГ 3. Просмотр лицензионного соглашения

На этом шаге следует ознакомиться с Лицензионным соглашением, которое заключается между пользователем и «Лабораторией Касперского». Необходимо внимательно прочесть Лицензионное соглашение и, если мы согласны со всеми его пунктами, установливаем флажок **Я принимаю условия Лицензионного соглашения**. Чтобы вернуться к предыдущему шагу мастера

установки программы, нажмаем на кнопку **Назад**. Чтобы продолжить работу мастера установки программы, нажимаем на кнопку **Далее**. Чтобы прекратить работу мастера установки программы, необходимо нажать на кнопку **Отмена**.

ШАГ 4. Соглашение об участии в Kaspersky Security Network

На этом шаге предлагается принять участие в программе Kaspersky Security Network.

Ознакомимся с положением о Kaspersky Security Network:

– если согласны со всеми его пунктами, в окне мастера установки программы выбираем вариант **Я согласен участвовать в Kaspersky Security Network**;

– если не согласны с условиями участия в Kaspersky Security Network, в окне мастера установки программы выбираем вариант **Я не согласен участвовать в Kaspersky Security Network**.

Чтобы вернуться к предыдущему шагу мастера установки программы, необходимо нажать на кнопку **Назад**. Чтобы продолжить работу мастера установки программы, на кнопку **Далее**. Чтобы прекратить работу мастера установки программы, на кнопку **Отмена**.

ШАГ 5. Выбор типа установки

На этом шаге необходимо выбрать подходящий тип установки Kaspersky Security Center:

– базовая установка. Если выбирать этот тип установки, на компьютер пользователя устанавливаются только компоненты защиты с параметрами, рекомендуемыми специалистами «Лаборатории Касперского»;

– стандартная установка. Если выбирать этот тип установки, на компьютер пользователя устанавливаются компоненты защиты и компоненты контроля с параметрами, рекомендуемыми специалистами «Лаборатории Касперского»;

– полная установка. Если выбирать этот тип установки, на компьютер пользователя устанавливаются все компоненты программы с параметрами, рекомендуемыми специалистами «Лаборатории Касперского», включая функциональность шифрования данных. Функциональность шифрования данных недоступна до тех пор, пока отдельно не установлен модуль шифрования;

– выборочная установка. Если выбирать этот тип установки, необходимо выбрать компоненты для установки и указать папку, в которую будет установлена программа.

По умолчанию выбрана базовая установка.

Чтобы вернуться к предыдущему шагу мастера установки программы, необходимо нажать на кнопку **Назад**. Чтобы продолжить работу мастера установки программы, нажать на кнопку **Далее**. Чтобы прекратить работу мастера установки программы, нажать на кнопку **Отмена**.

ШАГ 6. Выбор компонентов программы для установки

Этот шаг выполняется, если была выбрана **Выборочную установку программы**.

На этом шаге можно выбрать компоненты Kaspersky Endpoint Security 10 для Windows, которые хотите установить. По умолчанию для установки выбраны все компоненты программы.

Чтобы выбрать компонент для установки, необходимо открыть контекстное меню по левой клавише мыши на значке рядом с названием компонента и выбрать пункт **Компонент будет установлен на локальный жесткий диск**. Информацию о том, какие задачи выполняет выбранный компонент и сколько места на жестком диске требуется для установки компонента, можно посмотреть в нижней части окна мастера установки программы.

Чтобы получить информацию о свободном месте на жестких дисках компьютера, необходимо нажать **Диск**. Информация будет предоставлена в открывшемся окне **Доступное дисковое пространство**.

Чтобы отказаться от установки компонента, в контекстном меню выберем пункт **Компонент будет недоступен**.

Чтобы вернуться к списку устанавливаемых по умолчанию компонентов, нажмем на кнопку **Сброс**.

Чтобы вернуться к предыдущему шагу мастера установки программы, необходимо нажать на кнопку **Назад**. Чтобы продолжить работу мастера установки программы, на кнопку **Далее**. Чтобы прекратить работу мастера установки программы, на кнопку **Отмена**.

ШАГ 7. Выбор папки для установки программы

Этот шаг доступен, если была выбрана **Выборочную установку программы**.

На этом шаге нужно указать путь к папке назначения, в которую будет установлена программа. Для выбора папки для установки программы нажимаем на кнопку **Обзор**.

Для просмотра информации о свободном месте на жестких дисках компьютера, нажмем на кнопку **Диск**. Информация будет предоставлена в открывшемся окне Доступное дисковое пространство.

Чтобы вернуться к предыдущему шагу мастера установки программы, нажмем на кнопку Назад. Чтобы продолжить работу мастера установки программы, на кнопку Далее. Чтобы прекратить работу мастера установки программы, на кнопку Отмена.

ШАГ 8. Добавление исключений из антивирусной проверки

Этот шаг доступен, если была выбрана **Выборочную установку программы**.

На этом шаге можно указать, какие исключения из антивирусной проверки требуется добавить в параметры программы.

Флажок **Исключить из антивирусной проверки области, рекомендованные компанией Microsoft / Исключить из антивирусной проверки области, рекомендованные компанией «Лаборатория Касперского»** включает / исключает из доверенной зоны области, рекомендованные компанией Microsoft / «Лаборатория Касперского».

Если флажок установлен, то Kaspersky Endpoint Security включает области, рекомендованные компанией Microsoft / «Лаборатория Касперского», в доверенную зону. Такие области Kaspersky Endpoint Security не проверяет на наличие вирусов и других программ, представляющих угрозу.

Флажок Исключить из антивирусной проверки области, рекомендованные компанией Microsoft доступен при установке Kaspersky Endpoint Security на компьютер под управлением операционной системы Microsoft Windows для файловых серверов.

Чтобы вернуться к предыдущему шагу мастера установки программы, необходимо нажать на кнопку **Назад**. Чтобы продолжить работу мастера установки программы, на кнопку **Далее**. Чтобы прекратить работу мастера установки программы, на кнопку **Отмена**.

ШАГ 9. Подготовка к установке программы

Поскольку на компьютере могут присутствовать вредоносные программы, способные помешать установке Kaspersky Endpoint Security 10 для Windows, процесс установки рекомендуется защищать.

По умолчанию защита процесса установки включена.

Выключать защиту процесса установки рекомендуется в том случае, когда невозможно выполнить установку программы (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop). Причиной этому может быть включенная защита установки программы. В этом

случае прервите установку и запустите мастер установки программы с начала. На шаге «Подготовка к установке программы» снимем флажок **Защитить процесс установки**.

Флажок **Добавить путь к файлу avp.com в системную переменную %PATH% включает / выключает функцию, которая добавляет в системную переменную %PATH% путь к файлу avp.com**.

Если флажок установлен, то для запуска Kaspersky Endpoint Security или любых задач программы из командной строки не требуется вводить путь к исполняемому файлу. Достаточно ввести название исполняемого файла и команду для запуска соответствующей задачи.

Чтобы вернуться к предыдущему шагу мастера установки программы, необходимо нажать на кнопку **Назад**. Для установки программы на кнопку **Установить**. Чтобы прекратить работу мастера установки программы, на кнопку **Отмена**.

При установке программы на компьютер возможен разрыв текущих сетевых соединений. Большинство разорванных соединений восстанавливается через некоторое время.

ШАГ 10. Установка программы

Установка программы занимает некоторое время. Необходимо дождаться ее завершения.

Если выполняется обновление предыдущей версии программы, то на этом шаге также выполняется миграция параметров и удаление предыдущей версии программы.

После завершения установки Kaspersky Endpoint Security 10 для Windows запускается мастер первоначальной настройки программы.

АКТИВАЦИЯ ПРОГРАММЫ

На этом шаге нужно выбрать один из следующих вариантов активации Kaspersky Endpoint Security:

– активировать с помощью кода активации;

– активировать с помощью файла ключа;

– активировать пробную версию;

– активировать позже.

Чтобы продолжить работу мастера первоначальной настройки программы, необходимо выбрать вариант активации программы и нажмите на кнопку Далее. Чтобы прекратить работу мастера первоначальной настройки программы, нажать на кнопку Отмена.

АКТИВАЦИЯ ОНЛАЙН

На этом шаге Kaspersky Endpoint Security отправляет данные на сервер активации, чтобы проверить введенный код активации:

– если код активации успешно проходит проверку, мастер первоначальной настройки программы автоматически переходит к следующему окну;

– если код активации не проходит проверку, на экране появляется соответствующее уведомление. В этом случае вам следует обратиться за информацией в компанию, где вы приобрели лицензию на Kaspersky Endpoint Security;

– если число активаций с помощью кода активации превышено, на экране появляется соответствующее уведомление. Работа мастера первоначальной настройки программы прерывается, и программа предлагает вам обратиться в Службу технической поддержки «Лаборатории Касперского».

Чтобы вернуться к предыдущему шагу мастера первоначальной настройки программы, нажмите на кнопку Назад. Чтобы прекратить работу мастера первоначальной настройки программы, нажмите на кнопку Отмена.

АКТИВАЦИЯ С ПОМОЩЬЮ ФАЙЛА КЛЮЧА

На этом шаге требуется указать путь к файлу ключа. Для этого нажмите на кнопку Обзор и выберите файл ключа, имеющий вид **<ID файла>.key**. После

того как вы выбрали файла ключа, в нижней части окна отобразится следующая информация:

– ключ;

– тип лицензии (коммерческая или пробная) и количество компьютеров, на которые эта лицензия распространяется;

– дата активации программы на компьютере;

– дата окончания срока действия лицензии;

– функциональность программы, которая доступна по лицензии;

– сообщение о каких-либо проблемах, связанных с лицензированием, при их наличии. Например, Поврежден черный список ключей.

Чтобы вернуться к предыдущему шагу мастера первоначальной настройки программы, нажмите на кнопку Назад. Чтобы продолжить работу мастера первоначальной настройки программы, нажмите на кнопку Далее. Чтобы прекратить работу мастера первоначальной настройки программы, нажмите на кнопку Отмена.

ВЫБОР АКТИВИРУЕМОЙ ФУНКЦИОНАЛЬНОСТИ

На этом шаге предлагается выбрать вариант защиты компьютера, которая будет доступна после активации программы:

– базовая защита. Если выбран этот вариант, то после активации программы будут доступны только компоненты защиты;

– стандартная защита. Если выбран этот вариант, то после активации программы будут доступны компоненты защиты и контроля;

– расширенная защита. Если выбран этот вариант, то после активации программы будут доступны все компоненты программы, включая функциональность шифрования данных.

По умолчанию выбрана базовая защита.

Чтобы вернуться к предыдущему шагу мастера первоначальной настройки программы, нажмите на кнопку Назад. Чтобы продолжить работу

мастера первоначальной настройки программы, нажмите на кнопку Далее. Чтобы прекратить работу мастера первоначальной настройки программы, нажмите на кнопку Отмена.

ЗАВЕРШЕНИЕ АКТИВАЦИИ ПРОГРАММЫ

На этом шаге мастер первоначальной настройки программы информирует вас об успешном завершении активации Kaspersky Endpoint Security. Кроме того, приводится информация о лицензии:

– тип лицензии (коммерческая или пробная) и количество компьютеров, на которые распространяется лицензия;

– дата окончания срока действия лицензии;

– функциональность программы, которая доступна по лицензии.

Чтобы продолжить работу мастера первоначальной настройки программы, нажмите на кнопку Далее. Чтобы прекратить работу мастера первоначальной настройки программы, нажмите на кнопку Отмена.

АНАЛИЗ ОПЕРАЦИОННОЙ СИСТЕМЫ

На этом шаге производится сбор информации о программах, входящих в состав операционной системы. Эти программы попадают в список доверенных программ, которые не имеют ограничений на действия, совершаемые в операционной системе.

Анализ других программ происходит после первого их запуска после установки Kaspersky Endpoint Security.

Чтобы прекратить работу мастера первоначальной настройки программы, нажмите на кнопку Отмена.

ЗАВЕРШЕНИЕ РАБОТЫ МАСТЕРА ПЕРВОНАЧАЛЬНОЙ НАСТРОЙКИ ПРОГРАММЫ

Окно завершения мастера первоначальной настройки содержит информацию об окончании процесса установки Kaspersky Security Center. Если нужно запустить Kaspersky Security Center, нажмите на кнопку Завершить. Если

вы хотите выйти из мастера первоначальной настройки программы без последующего запуска Kaspersky Security Center, снимите флажок Запустить Kaspersky Security Center 10 для Windows и нажмите на кнопку Завершить.

Настройка Kaspersky Security Center

Веб - контроль

Задача веб-контроля — фильтровать доступ пользователей к ресурсам Интернет согласно внутренней политике организации. Обычно это означает блокирование сайтов социальных сетей, музыки и видео, некорпоративной веб-почты, эротики и порно в рабочее время.

Таким образом, если пользователь захочет обратиться к такому серверу, он получит уведомление о блокировке, или предупреждение о нежелательности доступа к нему — в зависимости от строгости запрета.

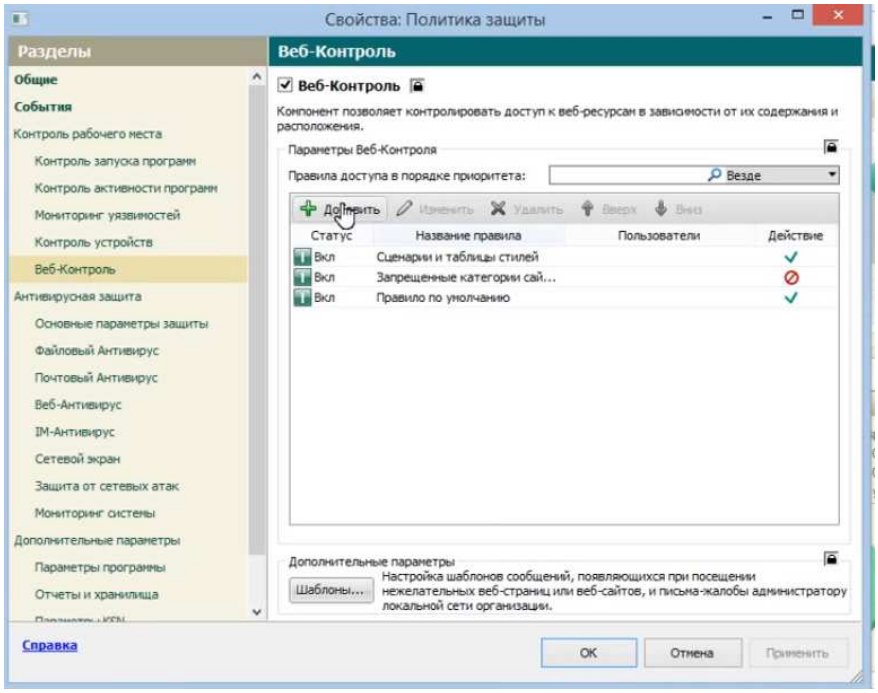

Рисунок Б.1 - Окно веб- контроля

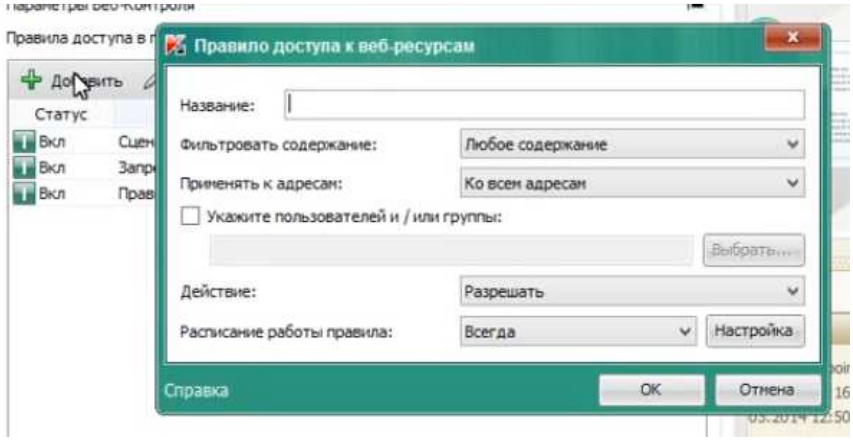

Рисунок Б.2 - Добавление в список интернет ресурсов и установка действий для них

Контроль устройств

Основная задача контроля устройств легко угадывается из названия — обеспечить администратора средством, позволяющим отследить и, по необходимости, запретить использование в корпоративной сети устройств разных типов.

Наиболее известный сценарий использования компонента – запрет на подключение съемных носителей. Пользователь может принести из дома зараженный файл или же просто домашнее задание отпрыска, и посвятить ему рабочий день. Случайно или преднамеренно пользователь может унести домой на съемном носителе или USB-диске файлы, представляющие коммерческую ценность для компании. Во избежание подобных проблем и вводятся различные запреты.

Компонент Контроль устройств Kaspersky Endpoint Security позволяет администратору ввести корпоративный стандарт, указав кому, когда и какие устройства можно использовать на своем компьютере. Правила могут применяться к съемным носителям, принтерам, CD/DVD, подключению к посторонним сетям, WiFi, Bluetooth.

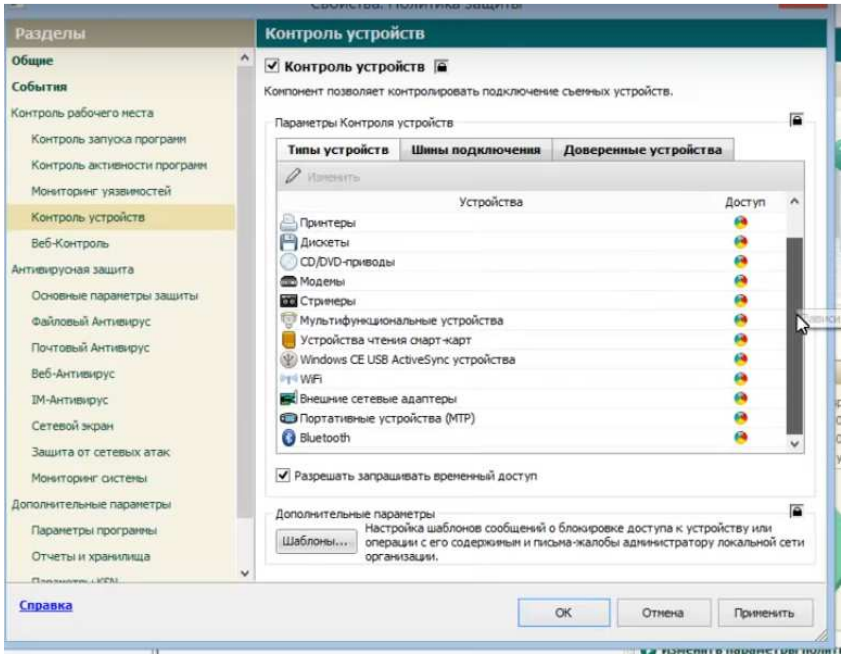

Рисунок Б.3 - Окно контроля устройствами

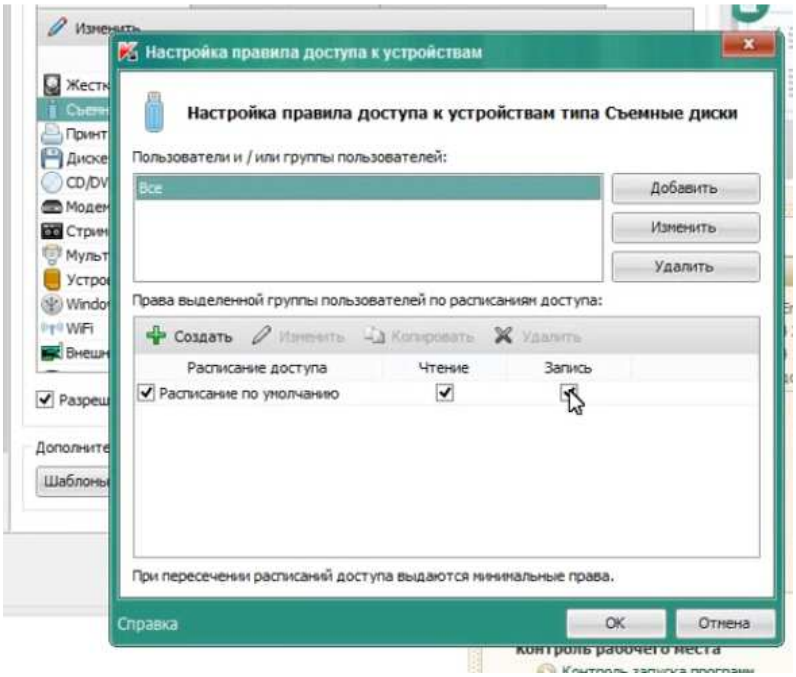

Рисунок Б.4 - Установка прав доступа для съемных носителей

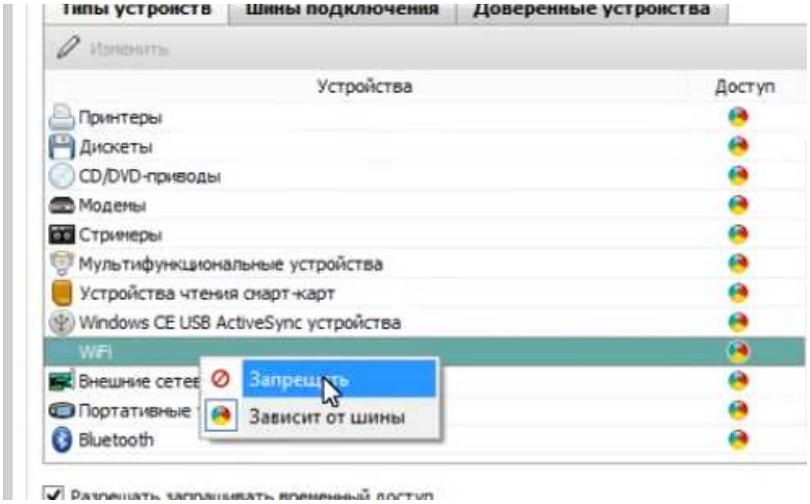

Рисунок Б.5 - Установка запрета на использование Wi-Fi соединения

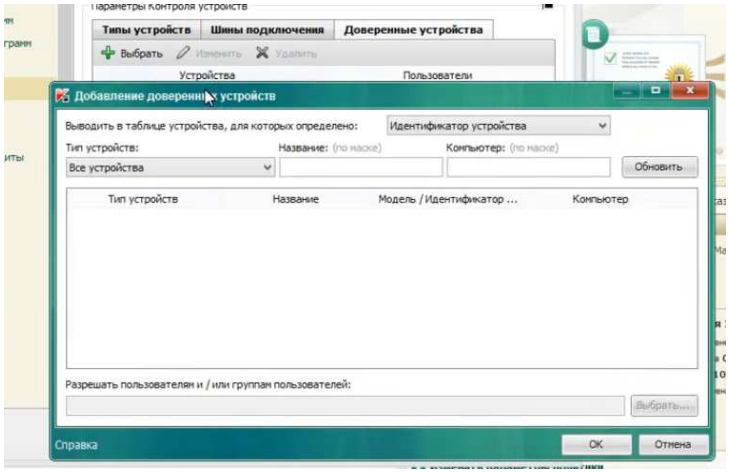

Рисунок Б.6 - Добавление доверенного устройства

Контроль активности программ

Основное назначение контроля активности программ — регулировать действия уже запущенных программ, а именно, доступ к файловой системе, системному реестру и взаимодействие с другими программами.

Так же, как и в контроле запуска программ, приложения делятся на категории, для которых и задаются ограничения. Но принцип деления иной. Все программы делятся по уровню доверия, на четыре заранее фиксированные группы:

- доверенные;
- слабые ограничения;

- сильные ограничения;

- не доверенные.

Для каждой из категорий заранее заданы стандартные ограничения активности. Администратор может, как изменять существующие ограничения для категорий в целом, так и настраивать индивидуальные ограничения на уровне программы. Ограничения задаются с помощью политики.

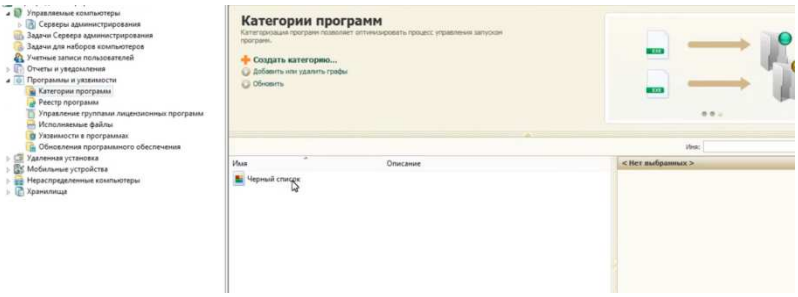

Рисунок Б.7 - Создание категорий программ

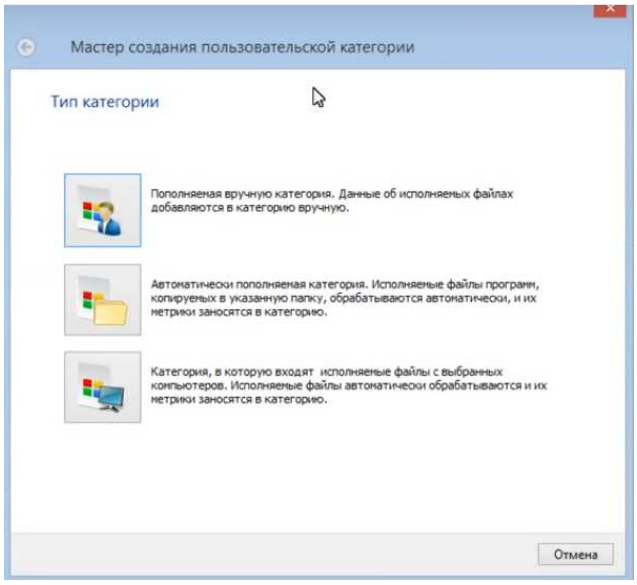

Рисунок Б.8 - Выбор типа категории

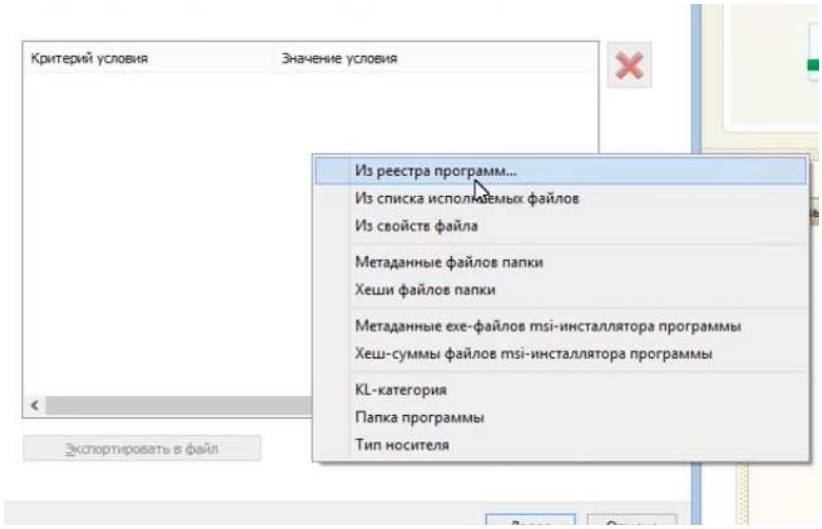

Рисунок Б.9 - Добавление программ в категорию

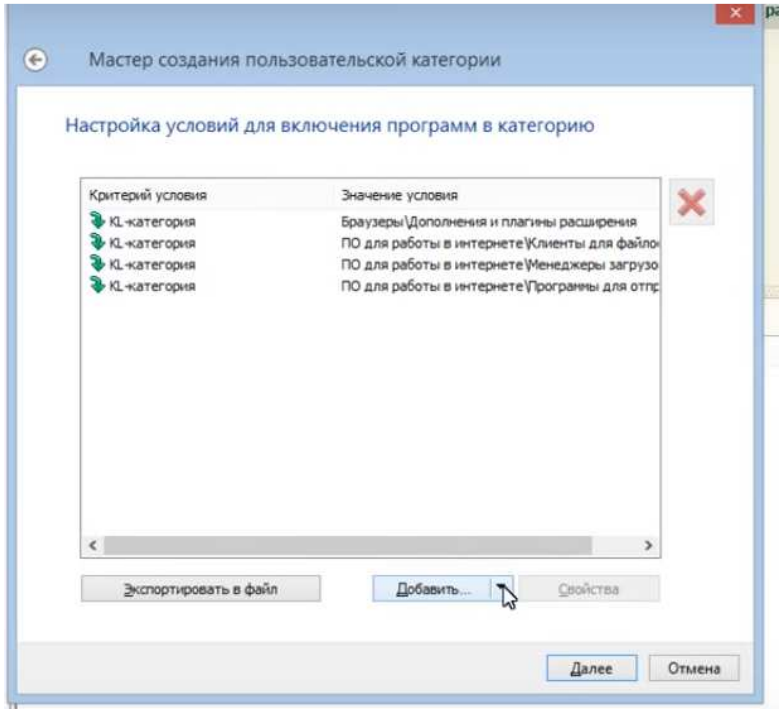

Рисунок Б.10 - Выбранные программы для включения в категорию

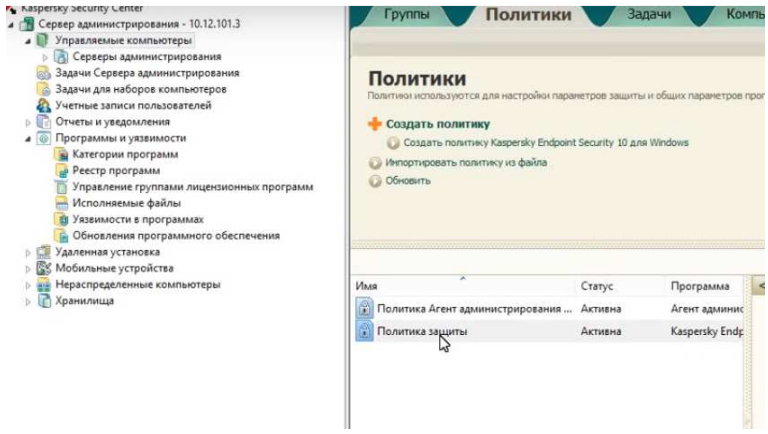

Рисунок Б.11 - Созданные политики

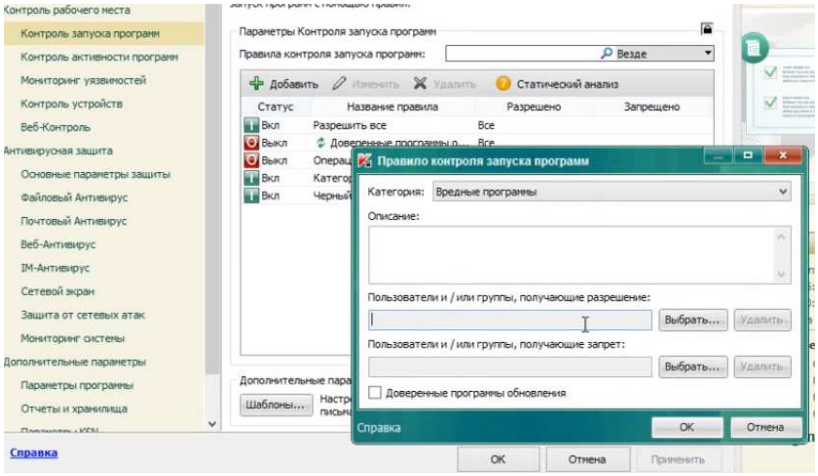

Рисунок Б.12 - Установка правила контроля для политики

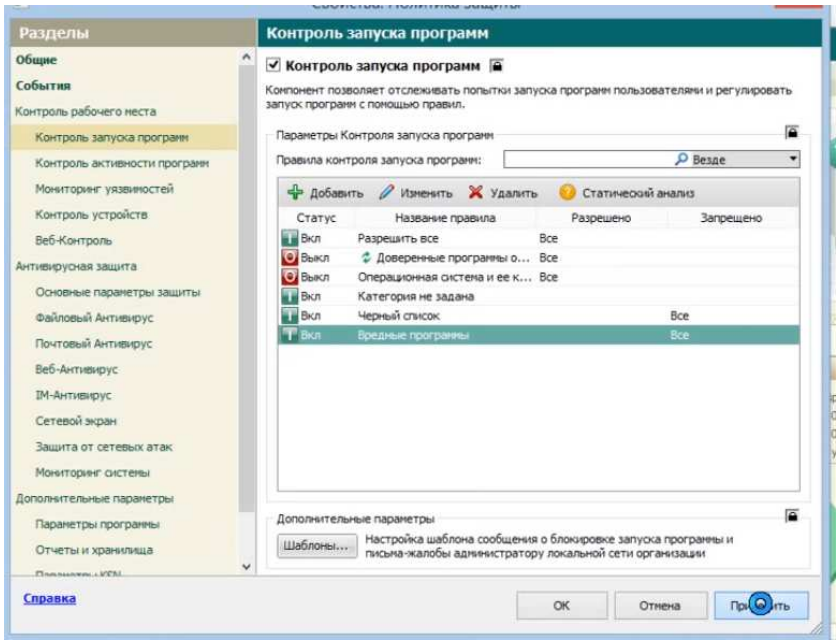

Рисунок Б.13 - Окно контроля запуска программ

ПРИЛОЖЕНИЕ В

(обязательное)

Установка и настройка vGate

Агент авторизации vGate Client

vGate Client устанавливается на рабочие места АИБ и АВИ во внешнем периметре сети и выполняет следующие функции:

– идентификация и аутентификация пользователя;

– идентификация и аутентификация компьютера;

– контроль целостности компонентов агента аутентификации;

– выбор уровня сессии при работе с конфиденциальными ресурсами (уровень доступа можно изменять во время работы);

– регистрация событий безопасности.

Процедура установки vGate Client начинается стандартно с приветственного сообщения и предложения принять лицензионное соглашение. Среди дополнительных компонентов, которые входят в состав дистрибутива vGate Client, находится Консоль управления vGate, которая также входит в состав дистрибутива vGate Server. Это облегчает процесс организации рабочих мест АИБ и АВИ.

На следующем шаге установки vGate Client требуется указать IP-адрес сервера авторизации vGate, а также параметры учётной записи АИБ.

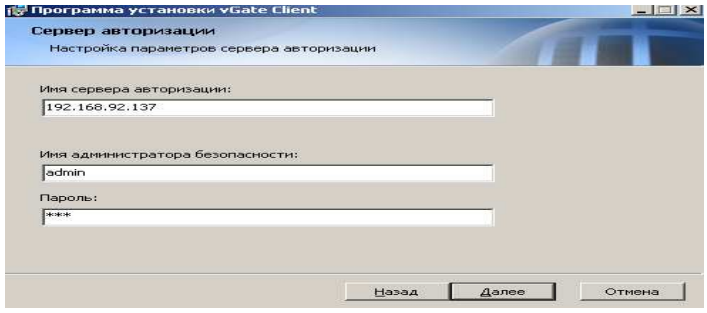

Рисунок В.1 - Указание параметров учётной записи АИБ

Дальнейшая установка агента авторизации vGate происходит без вмешательства пользователя.

На данном этапе установки и настройки компонентов vGate можно легко убедиться в том, что объекты виртуальной инфраструктуры защищаются от несанкционированного доступа. Если пользователь не авторизуется с помощью vGate Client, то, при попытке получить доступ к vCenter Server, с помощью vCenter Client выводится сообщение об ошибке. Если же авторизация на vGate Client произведена успешно, подключение к vCenter-серверу происходит без проблем.

Рисунок В.2 - Попытка несанкционированного доступа к серверу vCenter

Сервер отчётов Сервер отчётов vGate может быть установлен на любой компьютер внешнего периметра сети, включая компьютер, на котором работает vGate Server. Сервер отчётов служит для формирования отчётов о состоянии параметров безопасности ВИ, произошедших событиях и внесённых в конфигурацию изменениях.

Перед установкой сервера отчётов vGate необходимо установить MS SQL Server 2005, при этом Express-редакция этой СУБД не поддерживается, а, в качестве обязательного компонента SQL Server 2005, должен быть установлен

Reporting Services. В свою очередь, установка Reporting Services требует, чтобы в системе был установлен и функционировал веб-сервер IIS (Internet Information Services).

Также перед установкой сервера отчётов vGate требуется установить Microsoft Visual C++ 2008 Redistributable Package, который расположен на установочном диске vGate.

Установка сервера отчётов vGate заключается в запуске утилиты report_setup.exe, которая также расположена на установочном диске vGate. В случае, если сервер отчётов vGate устанавливается на тот же компьютер, где функционирует vGate Server, для установки достаточно ввести команду ‘report_setup.exe –server 127.0.0.1’, и через несколько минут отработает скрипт, который произведёт все необходимые действия.

Рассмотрим, какие возможности для аудита и создания отчётов предлагает vGate.

Все события, происходящее в защищаемом периметре сети, собраны в окне «Аудит» консоли управления vGate. В этом окне можно фильтровать события по типу (успех, уведомление, предупреждение, ошибка), по компьютерам, к которым относятся события, а также по дате, когда события произошли. Также доступны дополнительные фильтры – по защищаемым компонентам и по категориям. Наличие достаточного количества фильтров облегчают задачу аудита при расследовании инцидентов, возникающих в защищаемом периметре.

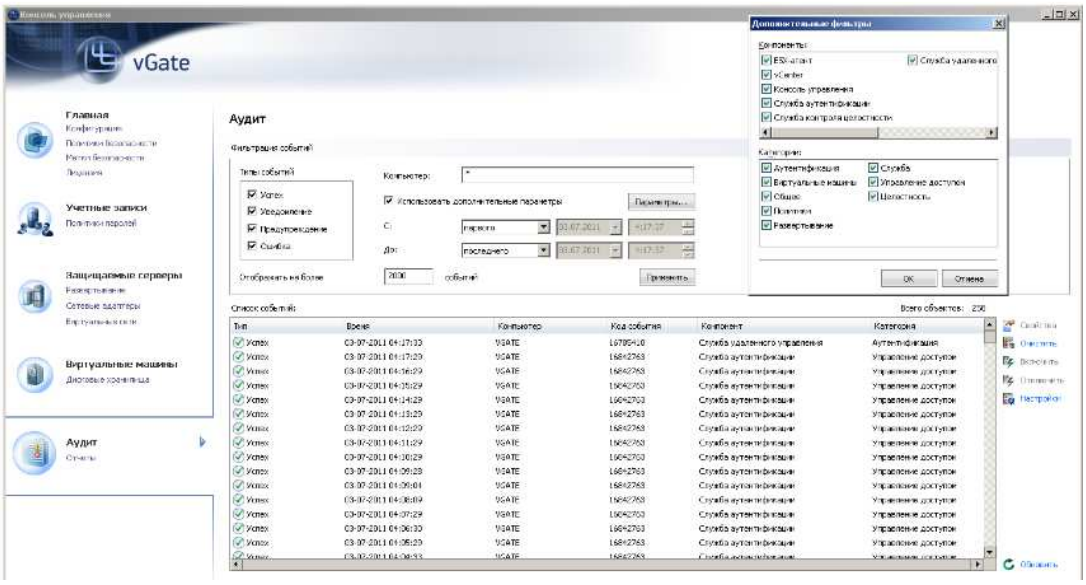

Рисунок В.3 - Окно «Аудит» консоли управления vGate

В окне «Отчёты» консоли управления vGate задаются настройки, связанные с работой сервера отчётов vGate. В частности, можно загрузить логотип предприятия, который будет отображаться в отчётах, указать адрес сервера отчётов, название компании, её описание и цветовую схему отчётов (синюю, зелёную или красную).

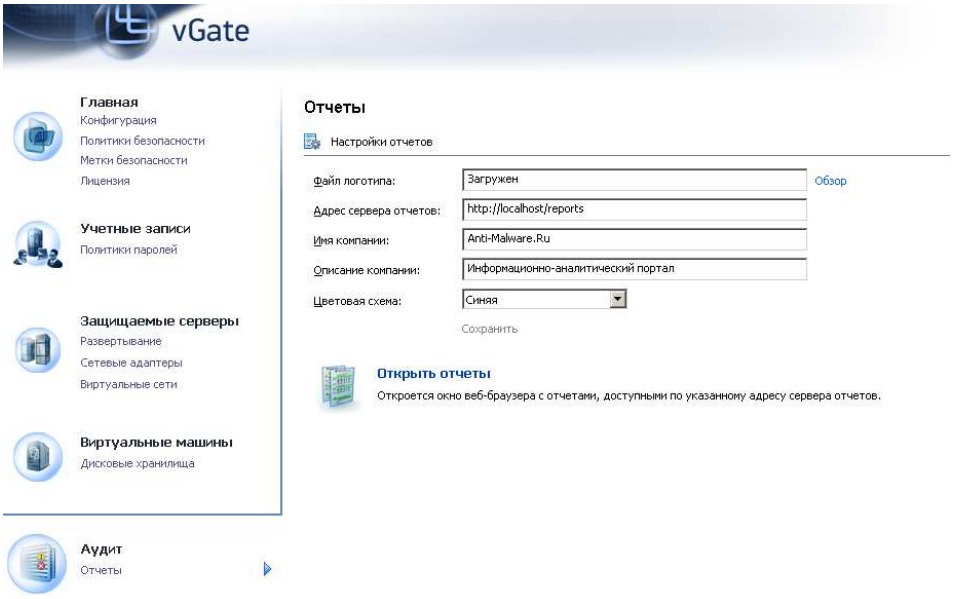

Рисунок В.4 - Окно «Отчёты» консоли управления vGate

При нажатии на ссылку «Открыть отчёты» в браузере отображается интерфейс сервера отчётов. Если в нём выбрать папку vGate, то в ней будут находиться шаблоны возможных типов отчётов.

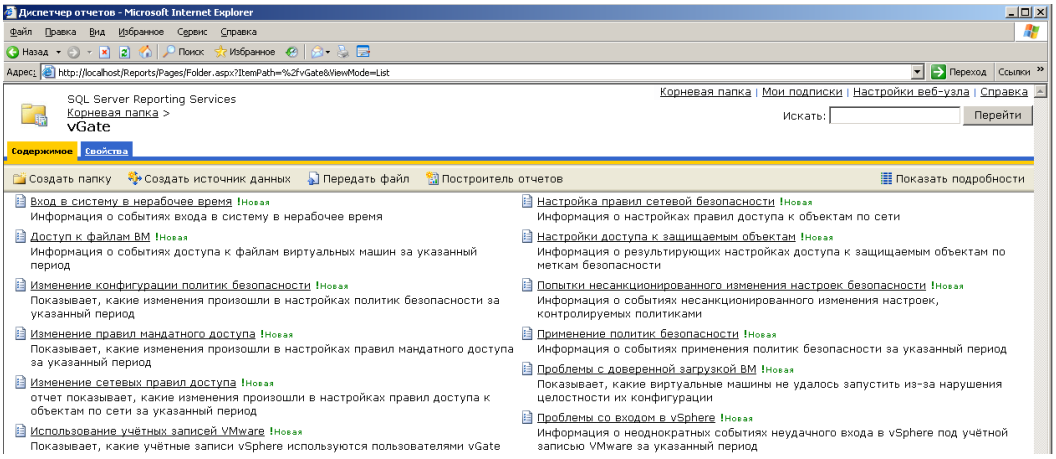

Рисунок В.5 - Типы отчётов vGate

При нажатии на название необходимого отчёта он тут же формируется. В частности, на рисунке 6 изображён достаточно интересный тип отчёта, в котором отображаются наиболее часто происходящие события информационной безопасности.

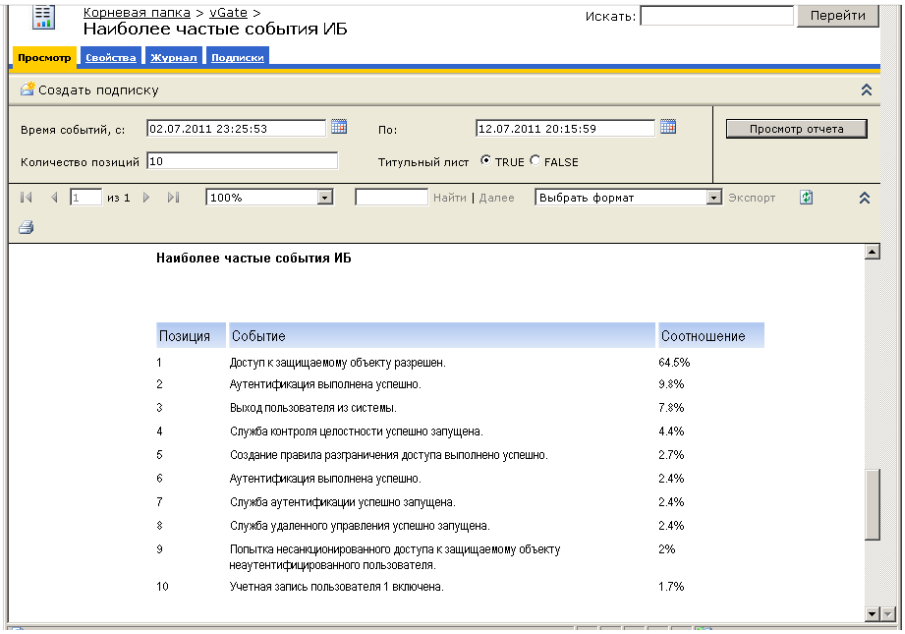

Рисунок В.6 - Отчёт vGate о наиболее частых событиях ИБ, произошедших в защищаемом периметре сети

ПРИЛОЖЕНИЕ Г

(обязательное)

Настройка межсетевого экрана ССПТ-2

Режим трансляции сетевых адресов (NAT) и аутентификация сетевых пользователей с сохранением скрытности

NAT (от англ. *Network Address Translation* — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

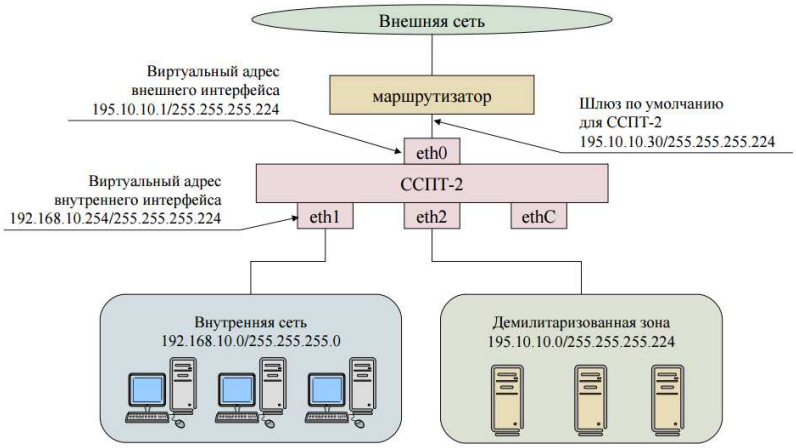

Рисунок Г.1 - Схема режима трансляции сетевых адресов NAT

Системная авторизация выполняется средствами операционной системы ССПТ-2. Для системной авторизации используется следующие начальные параметры:

имя пользователя – fnpsh. Это имя пользователя не может быть изменено;

пароль пользователя – FilterD. Пароль системного пользователя fnpsh может быть изменен администратором ССПТ-2.

Авторизация ССПТ-2 выполняется после успешной системной авторизации. Первоначально существует один пользователь ССПТ-2, имеющий полный набор привилегий:

имя пользователя – admin. Это имя пользователя также не может быть изменено;

пароль пользователя – FilterD.

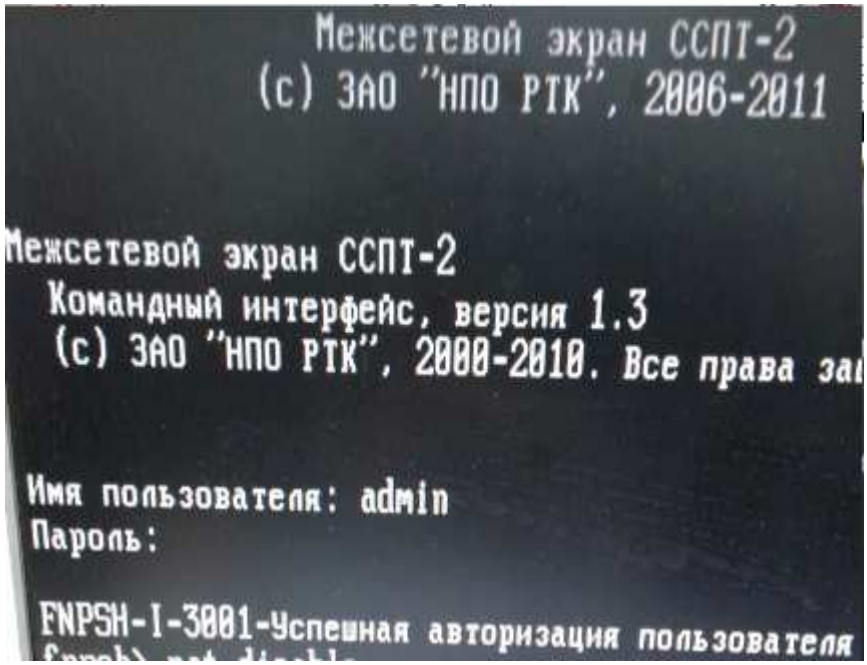

Рисунок Г.2 - Авторизация

Перед включением режима NAT необходимо выполнить следующие установки:

– установка шлюза по умолчанию для внешнего интерфейса NAT – команда nat public gateway (представлено на рисунке Г.3);

– установка IP-адреса внутреннего интерфейса NAT – команда nat private ip (представлено на рисунке Г.5);

– установка IP-адреса внешнего интерфейса NAT – команда nat public ip (представлено на рисунке Г.4);

– добавление в статическую ARP таблицу записи об IP и MAC-адресах шлюза по умолчанию для внешнего интерфейса NAT – команда nat arp add (представлено на рисунке Г.8).

Перед выполнением настройки NAT, режим должен быть отключен (представлено на рисунке 3).

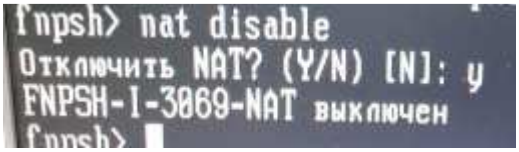

Рисунок Г.3 - Отключение режима NAT

Рисунок Г.4 - Установка шлюза по умолчанию для внешнего интерфейса NAT

Рисунок Г.4 - Установка IP-адреса внутреннего интерфейса NAT

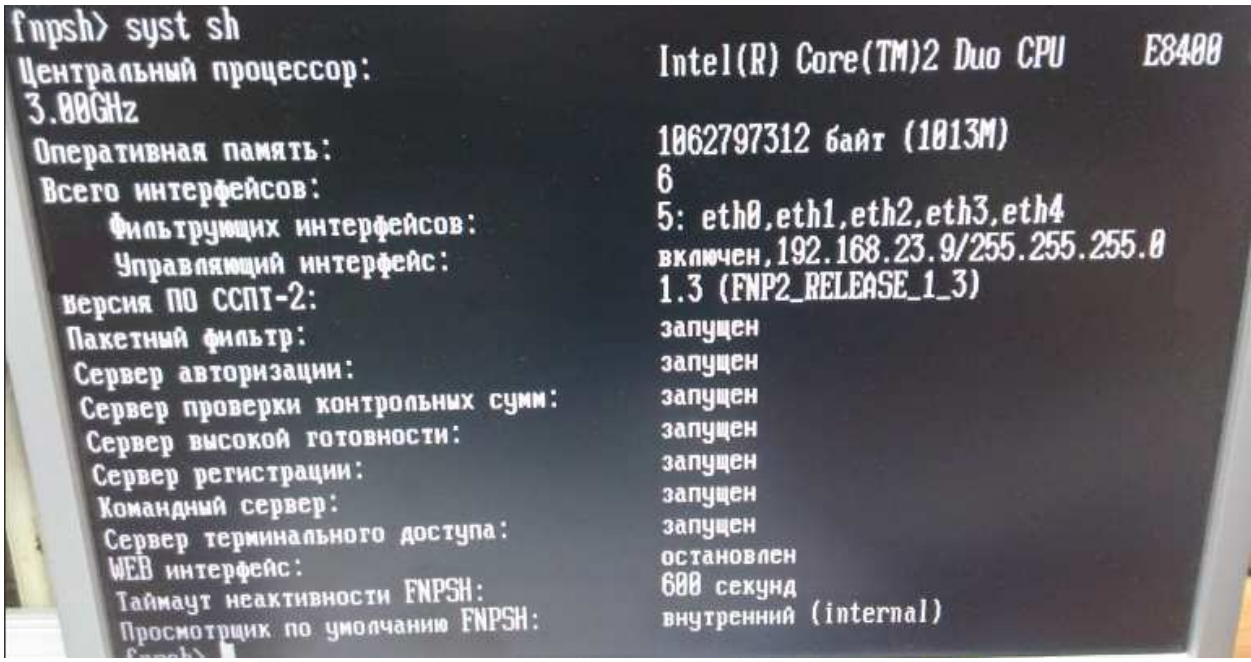

Рисунок Г.5 - Параметры

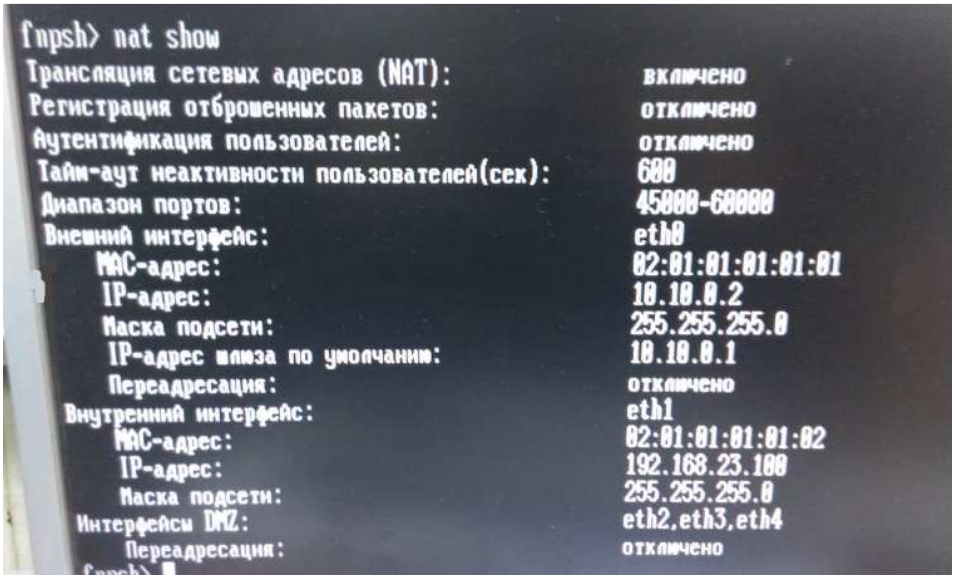

Рисунок Г.6 – Параметры NAT

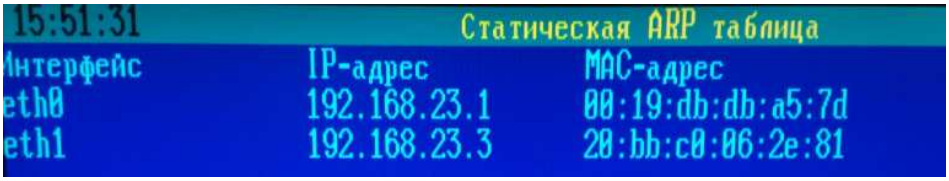

Рисунок Г.7 – Статическая ARP таблица

После всей настройки проверяем правильность настройки. результаты проверки представленны на рисунках далее.

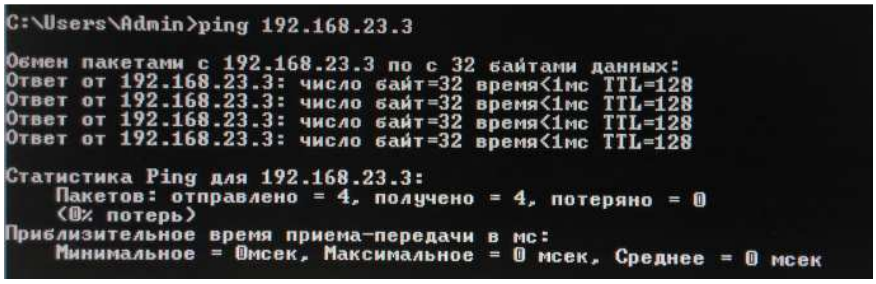

Рисунок Г.8 - Проверка работы

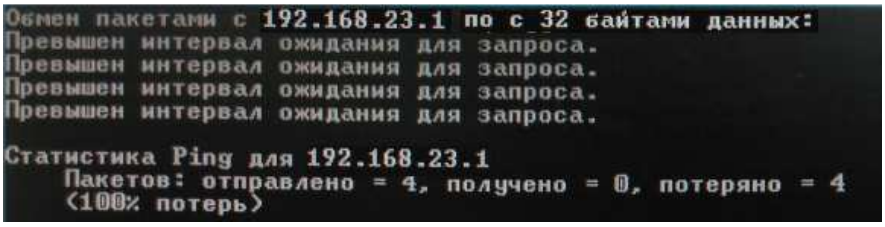

Рисунок Г.9 - Проверка работы

Горячее резервирование

С целью повышения надежности функционирования два ССПТ-2 могут объединяться в вычислительный кластер, работающих по схемам “активный/резервный” или “активный/активный”, реализуя таким образом систему горячего резерва.

ПРИЛОЖЕНИЕ Д

(обязательное)

Настройка средства обнаружения вторжения Форпост 2.0

Первичный запуск консоли администратора

1. Для запуска консоли администратора из меню ОС Windows необходимо выбрать пункт «Пуск → Программы → RNT → Форпост → Консоль администратора» («Start → Programs → RNT → Форпост→ Консоль администратора»).

При первом запуске консоли администратора приложению требуются права администратора. В связи с этим, первичный запуск консоли администратора необходимо осуществлять от имени администратора. В Windows 7/8/2012 для этого необходимо нажать правой кнопкой мыши по ярлыку «Консоль администратора» и в появившемся контекстном меню выбрать пункт «Запуск от имени администратора».

2. Сразу после установки по умолчанию консоль администратора в качестве параметров подключения использует IP-адрес 127.0.0.1, порт 10000. Данные параметры подходят (и подключение происходит успешно) только в случае, если консоль администратора установлена на том же узле, на котором установлен координационный центр.

3. Консоль администратора установлена на отдельном компьютере, после первой попытки запуска консоли администратора появится сообщение об ошибке подключения к КЦ. В этом случае в следующем окне необходимо указать параметры подключения к КЦ:

- в поле «Хост» группы «Параметры подключения по протоколу TCP» необходимо ввести имя или IP-адрес узла, на котором установлен основной координационный центр;

- в поле порт – номер TCP-порта, по которому координационный центр ожидает подключений (по умолчанию для протокола TCP – 10000).

4. В случае реализации схемы резервирования координационных центров подключаться следует к основному КЦ. Подключение к резервному КЦ следует производить только в случае, когда основной КЦ недоступен.

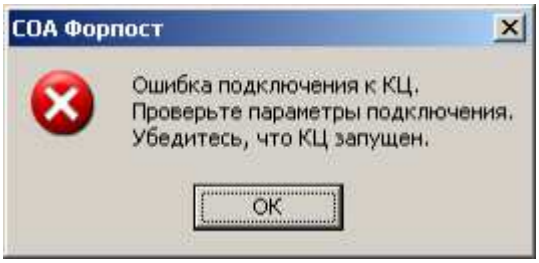

Рисунок Д.1 – Сообщение об ошибки подключения

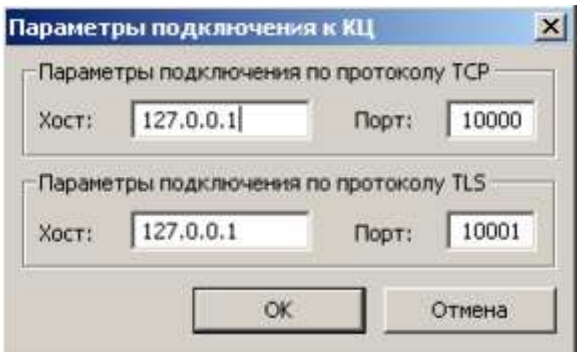

Рисунок Д.2 – Параметры подключения

Регистрация первого пользователя СОА «Форпост»

1. СОА «Форпост» не хранит непосредственно пароли пользователей, сохраняется только хэш пароля. По умолчанию для хэширования пароля используется алгоритм MD5, реализация которого уже встроена в операционную систему. В случае, если по условиям применения СОА необходимо использовать другую функцию хэширования, то до проведения регистрации первого пользователя СОА «Форпост» необходимо в настройках консоли администратора изменить алго- ритм хэширования пароля.

Для этого необходимо отредактировать файл ConsoleAdmin.cfg, находящийся в каталоге программы (например, «C:\Program Files\RNT\Forpost\ConsoleAdmin.cfg»). Необходимо отредактировать следующие строчки:

Forpost.Login.CryptoProviderName= <название_криптопровайдера>

Forpost.Login.HashAlgName= <название_алгоритма_хэширования>

Например, при использовании КриптоПро CSP:

Forpost.Login.CryptoProviderName=Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider

Forpost.Login.HashAlgName=GOST R 34.11-94

2. При первом запуске консоли администратора необходимо провести регистрацию первого пользователя СОА «Форпост». По умолчанию первому пользователю присваивается имя Administrator, пароль необходимо задать при первом запуске. Впоследствии только пользователь Administrator может добавлять/удалять других пользователей СОА.

3. Пароль должен удовлетворять следующим требованиям: длина пароля – не менее 6 символов, пароль должен содержать буквы и цифры.

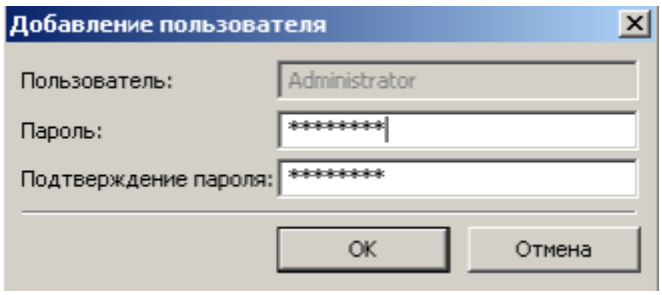

Рисунок Д.3 – Добавление нового пользователя

4. При последующих запусках консоли администратора для получения доступа в систему необходимо будет вводить имя пользователя и пароль.

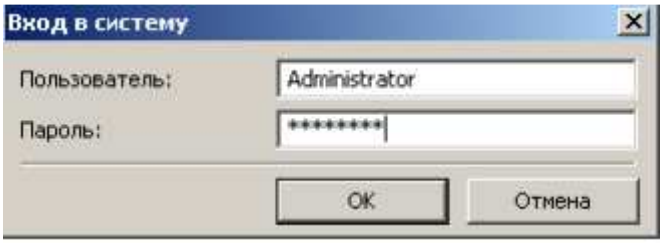

Рисунок Д.4 – Вход в систему

5. В случае, если потребуется смена алгоритма хэширования паролей пользователей в процессе эксплуатации СОА, это можно сделать выполнив следующие шаги:

1) Необходимо изменить настройки в части используемого алгоритма хэширования паролей всех установленных консолей администратора СОА по инструкции, приведенной выше.

2) Сбросить базу пользователей СОА. Для этого необходимо удалить из таблицы USERS базы данных IDS все записи. Сделать это можно на сервере информационного фонда, выполнив из среды Microsoft SQL Server Management Studio следующий запрос:

DELETE FROM [IDS].[dbo].[USERS]

3) После сброса базы пользователей СОА при запуске консоли администратора появится возможность ввести пароль для пользователя Administrator. Пароль будет захэширован с использованием нового алгоритма хэширования. Далее необходимо с использованием средств консоли администратора СОА завести заново всех остальных пользователей.

Настройка ограничений на сетевые адреса, с которых возможно подключение к серверным компонентам СОА «Форпост»

1. СОА «Форпост» позволяет накладывать ограничения на сетевые адреса, между которыми осуществляется взаимодействие компонентов. В частности, ограничения затрагивают адреса, с которых может выполняться удаленное администрирование системы, с которых могут по- ступать данные от датчиков через агенты СОА, с которых может быть получен доступ к информационному фонду СОА.

2. Для организации ограничения сетевых адресов используется файл whitelist.txt. Данный файл располагается в каталоге с установленным координационным центром СОА «Форпост» и компонентом «Агент БД».

3. Рекомендуется ограничить подключения к компоненту «Агент БД» серверами координационных центров СОА «Форпост»; подключения к координационным центрам – подсетями, из которых осуществляется

администрирование СОА «Форпост» и подсетями, в которых установлены агенты СОА.

4. Настройка списка разрешенных адресов для подключения к КЦ осуществляется редактированием файла whitelist.txt, например, из оснастки «Управление компонентами Форпост», находящейся в области уведомлений на узлах координационных центров и информационного фонда. В появившемся меню необходимо выбрать пункт «Агент БД Форпост» (или «Координационный центр») -> «Настройки» рисунок Д.54. В появившемся окне рисунок Д.55. выбрать параметр «Список разрешенных адресов подключения» и нажать на кнопку «…» в правой части строки.

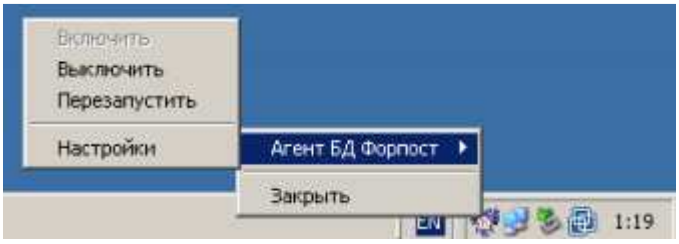

Рисунок Д.5 – Запуск «Агент БД Форпост»

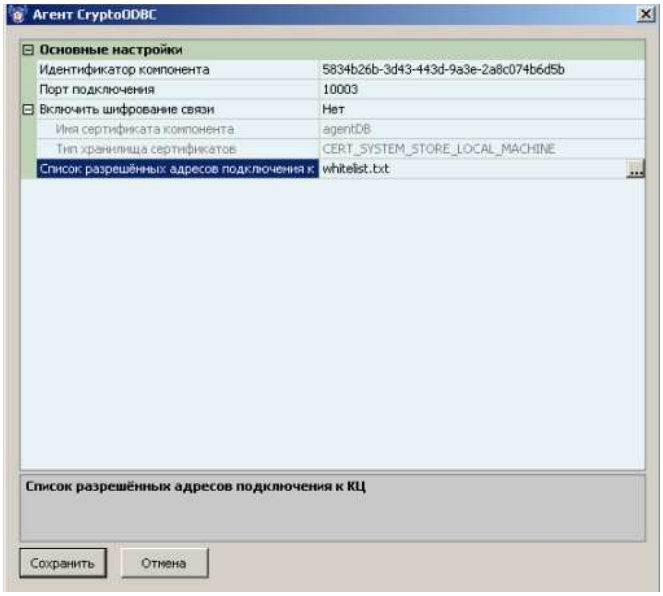

Рисунок Д.6 – «Агент БД Форпост»

5. Далее рисунок Д.7 производится редактирование файла, содержащего список разрешенных адресов. При необходимости можно выбрать другой файл,

нажав на кнопку «Выбрать другой файл». По окончанию редактирования необходимо нажать кнопку «Сохранить». Для применения настроек необходимо нажать кнопку «Сохранить» основного окна оснастки и перезагрузить сервис (координационный центр или компонент «Агент БД»). Сделать это можно выбрав пункт меню «Агент БД Форпост» (или «Координационный центр») -> «Перезапустить» в оснастке «Управление компонентами Форпост», находящейся в области уведомлений.

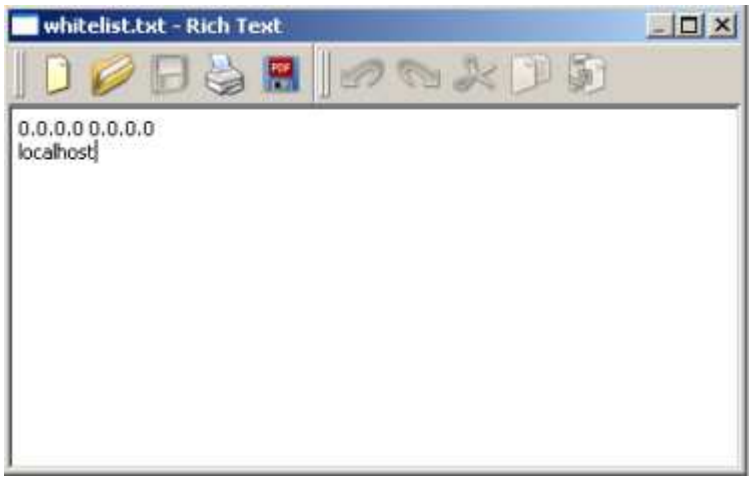

Рисунок Д.7 – Редактирование файла

6. Файл, содержащий список разрешенных адресов, редактируется в соответствии со следующими правилами.

6.1 По умолчанию в этом файле настроено разрешение подключения со всех IP- адресов и с localhost.

6.2 В этом файле с новой строчки должны быть перечислены IP-адреса с масками, или доменные имена узлов, с которых разрешено подключение к координационному центру.

6.3 IP-адреса записываются в виде четырех десятичных чисел (в диапазоне от 0 до 255), разделенных точкой.

6.4 Маска записывается аналогично IP-адресам. Наложение маски происходит сле- дующим образом: там, где маска имеет нулевой бит, бит в IP-

адресе игнорируется. Таким образом, можно записывать диапазоны IP-адресов. Например:

192.168.1.1 255.255.255.255 – доступ возможен с IP-адреса 192.168.1.1

192.168.10.136 255.255.255.248 - доступ возможен для диапазона IP-адресов 192.168.10.136-192.168.1.143

192.168.1.0 255.255.255.0 – доступ возможен для диапазона IP-адресов 192.168.1.0-192.168.1.255

192.168.96.0 255.255.224.0 - доступ возможен для диапазона IP-адресов 192.168.96.0-192.168.127.255

172.16.0.0 255.255.0.0 – доступ возможен для диапазона IP-адресов 172.16.0.0-172.16.255.255

0.0.0.0 0.0.0.0 - доступ возможен с любого IP-адреса

localhost - возможен локальный доступ с localhost

Маску 255.255.255.255 допускается не указывать.

Настройка координационного центра

1. Настройка параметров координационного центра может осуществляться с помощью оснастки «Управление компонентами Форпост». Для этого необходимо щелкнуть правой кнопкой по значку этой оснастки, находящейся в области уведомлений. В появившемся меню выбрать пункт «Координационный центр» -> «Настройки». Далее появится окно, в котором можно производить настройку. По окончании настройки необходимо нажать на кнопку сохранить, а что бы изменения вступили в силу необходимо перезапустить координационный центр. Сделать это можно выбрав пункт меню «Координационный центр» -> «Перезапустить» в оснастке «Управление компонентами Форпост», находящейся в области уведомлений.

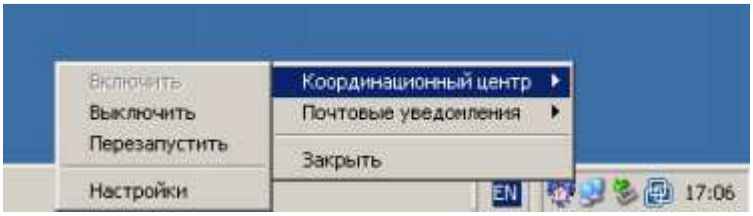

Рисунок Д.8 – Запуск настроек

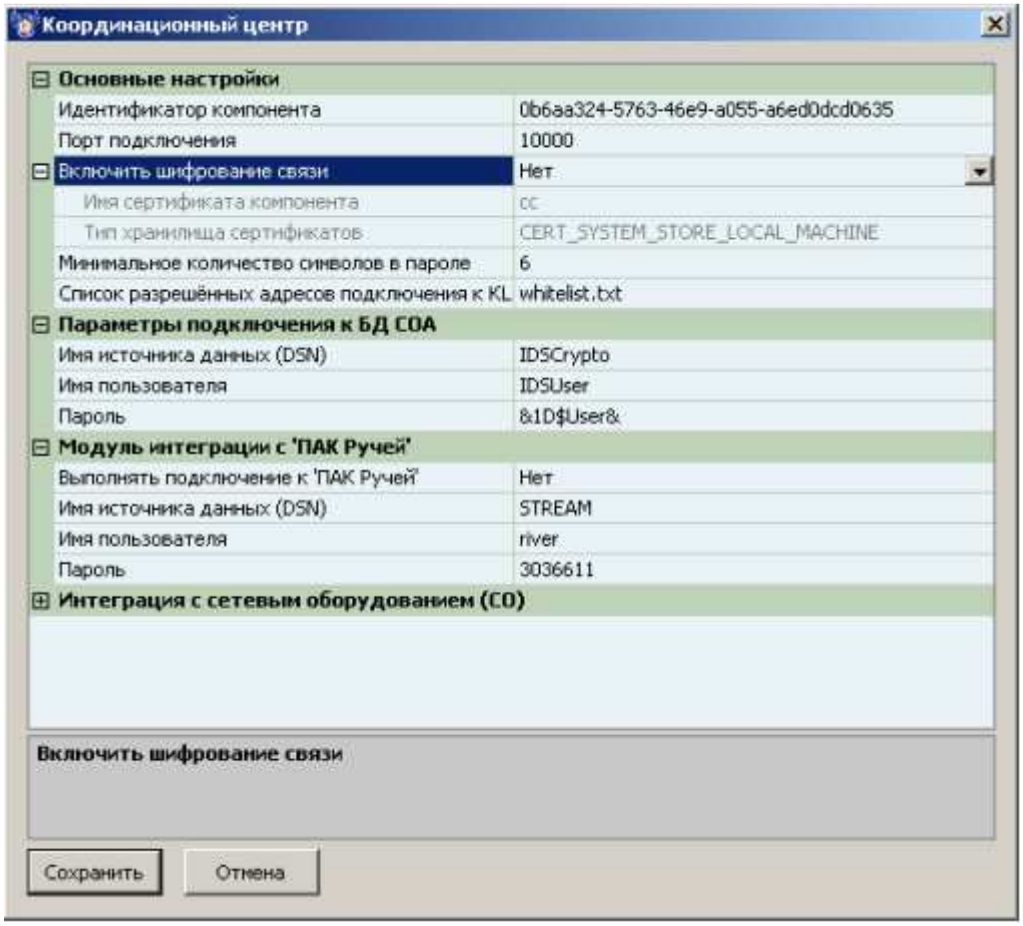

Рисунок Д.9 – Окно настройки

2. Настройки координационного центра с пояснениями представлены в таблице Д.1.

Настройка параметров данной группы позволяет просматривать журнал вирусной активности ПАК «Ручей-М» из консоли администратора СОА «Форпост

Таблица Д.1 – Настройки координационного центра СОА «Форпост»

Наименование параметра	Описание параметра
Группа «Основные настройки»	
Идентификатор компонента	Уникальный идентификатор компонента
Порт подключения	Номер порта, на котором координационный центр ожидает подключения агентов. По умолчанию – 10000 для открытого соединения и 10001 для криптографически защищенного
Включить шифрование связи	Включает шифрование информационного обмена между координационным центром и агентами
Имя сертификата компонента	Имя сертификата компонента (параметр требуется задавать, если включено шифрование информационного обмена между координационным центром и агентами)
Тип хранилища сертификатов	Тип хранилища сертификатов, в которое установлен сертификат для компонента (параметр требуется задавать, если включено шифрование информационного обмена между координационным центром и агентами). Допускаются следующие значения этого параметра: − CERT_SYSTEM_STORE_CURRENT_USER (хра нилище текущего пользователя); – CERT_SYSTEM_STORE_LOCAL_MACHINE (локальное хранилище узла);

Продолжение таблицы Д.1

Наименование параметра	Описание параметра
	– CERT_SYSTEM_STORE_CURRENT_SERVICE (хранилище конкретного сервиса); – CERT_SYSTEM_STORE_SERVICES (хранилище сервисов). По умолчанию поле имеет значение CERT_SYSTEM_STORE_LOCAL_MACHINE
Минимальное количество символов в пароле	Минимальное количество буквенно-цифровых символов в пароле (по умолчанию – 6)
Список разрешенных адресов подключения к КЦ	Имя файла, содержащего список разрешенных адресов для подключения к КЦ. По умолчанию список разрешенных адресов содержится в файле whitelist.txt, в котором изначально разрешено подключение к КЦ со всех адресов
Группа «Параметры подключения к БД СОА	
Имя источника данных (DSN)	Имя системного источника данных для подключения к базе данных (информационному фонду) СОА «Форпост». Если по условиям применения СОА «Форпост» в конкретной АИС предполагается использовать для связи координационных центров с СУБД информационного фонда ODBC-драйвера из состава СОА «Форпост», то поле должно иметь значение IDSCrypto. Если по условиям применения СОА

Продолжение таблицы Д.1

Наименование параметра	Описание параметра
	«Форпост» в конкретной АИС предполагается использовать для связи координационных центров с СУБД информационного фонда ODBC-драйвера из состава операционной системы или СУБД, то поле должно иметь значение IDS. Использование ODBC-драйвера из состава СОА «Форпост» вместо драйвера из комплекта поставки операционной системы или СУБД является обязательным, если предполагается шифрование информационного обмена между координационным центрами и информационным фондом с использованием отечественных криптоалгоритмов
Имя пользователя	Имя пользователя для подключения к базе данных
Пароль	Пароль для подключения к базе данных
Группа «Модуль интеграции с ПАК «Ручей-М»	
Выполнять подключение к ПАК «Ручей-М»	Установка этого параметра в значение «Да» дает возможность просматривать журнал вирусной активности ПАК «Ручей-М» из консоли администратора СОА «Форпост». По умолчанию параметр имеет значение «Нет»
Имя источника данных (DSN)	Имя системного источника данных для подключения к базе данных ПАК «Ручей-М»

Продолжение таблицы Д.1

Наименование параметра	Описание параметра
Имя пользователя	Имя пользователя для подключения к базе данных ПАК «Ручей-М»
Пароль	Пароль для подключения к базе данных ПАК «Ручей-М»

ПРИЛОЖЕНИЕ Е

(обязательное)

Протокол проверки ВКР на оригинальность