

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 –

Специализация –

Информационная безопасность
телекоммуникационных систем
Разработка защищенных
телекоммуникационных систем

ДИПЛОМНЫЙ ПРОЕКТ

на тему

СИСТЕМА ЗАЩИТЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ДЛЯ
ПОДГОТОВКИ И ВЫДАЧИ СЕРТИФИКАТОВ ЭЛЕКТРОННОЙ ПОДПИСИ

Студент _____ Глазков Максим Алексеевич

Руководитель инженер 1-ой категории

ПФ ФГУП «НТЦ «Атлас» _____ Назаров А.В.

Нормоконтролёр _____ Иванов А.П.

Рецензент инженер 2-ой категории

ПФ ФГУП «НТЦ «Атлас» _____ Жамейц С.Ю.

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

Заведующий кафедрой _____ С.Л. Зефилов

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

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2018

Оглавление

Введение.....	5
1 Анализ состояния отрасли защиты конфиденциальной информации.....	8
2 Обзор и анализ нормативной документации и публикаций по защите конфиденциальной информации и персональных данных.....	10
2.1 Обзор и анализ нормативной документации по защите конфиденциальной информации.....	10
2.2 Обзор и анализ публикаций по защите конфиденциальной информации.....	13
3 Выбор средств защиты конфиденциальной информации и персональных данных для аттестуемой автоматизированной системы	17
3.1 Общие положения	17
3.2 Адаптация базового набора мер	17
3.3 Сравнение СЗИ для аттестуемой автоматизированной системы.....	19
3.4 Выполнение требований по защите от несанкционированного доступа.....	25
4 Настройка средств защиты информации	30
4.1 Общие положения	30
4.2 Настройка ПАК <i>Соболь</i>	30
4.3 Настройка СЗИ от НСД <i>Secret Net Studio</i>	33
4.4 Настройка <i>Kaspersky Endpoint Security 10</i>	43
5 Оформление и выдача техпаспорта на аттестованную автоматизированную систему.....	49
6 Оформление программы и методики аттестационных испытаний.....	50

7 Проведение аттестационных испытаний объекта информатизации в части технической защиты от несанкционированного доступа.....	51
8 Проведение аттестационных испытаний объекта информатизации в части технической защиты от утечки информации по техническим каналам.....	67
9 Оформление аттестационных материалов.....	72
10 Вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие	73
10.1 Общие положения	73
10.2 Вредные факторы, влияющие на органы зрения специалиста по защите информации.....	73
10.3 Методы и средства физической культуры, снижающие воздействие вредных психофизиологических факторов, влияющих на органы зрения.....	76
Заключение	78
Список используемых источников.....	80
Приложение А (обязательное) Технический паспорт.....	82
Приложение Б (обязательное) Программа и методика аттестационных испытаний	90
Приложение В (обязательное) Протокол испытаний комплексной системы защиты информации АС	105
Приложение Г (обязательное) Протокол оценки защищенности ОТСС из состава АС.....	121
Приложение Д (обязательное) Протокол оценки защищенности конфиденциальной информации от утечки за счет наводок на	

вспомогательные технические средства и системы и их коммуникации, имеющие выход за пределы контролируемой зоны	127
Приложение Е (обязательное) Предписание на эксплуатацию АС	134
Приложение Ж (обязательное) Заключение по результатам проведения аттестационных испытаний АС	138
Приложение И (обязательное) Аттестат соответствия требованиям безопасности информации	146
Приложение К (обязательное) Протокол проверки на оригинальность в системе «Антиплагиат.ВУЗ».....	149

Введение

Одной из важнейших составных частей национальной безопасности любой страны в настоящее время является ее информационная безопасность. Проблемы обеспечения информационной безопасности становятся все более сложными и концептуально значимыми в связи с массовым переходом информационных технологий в управлении на безбумажную автоматизированную основу.

Соблюдение режима конфиденциальности для информации такого рода является одной из приоритетных задач для организации, обладающей данными и документами такого вида, а также позволяет соблюдать действующие правила по защите конфиденциальной информации и охранять таким образом собственные документы и информацию, принадлежащую этой организации и важную для нее.

Для соблюдения режима конфиденциальности необходимо, чтобы используемые средства информатизации и автоматизированные системы отвечали предъявляемым к ним требованиям, что может быть подтверждено в ходе прохождения аттестации по требованиям безопасности. А для этого автоматизированная система должна быть оборудована системой защиты. Для каждого объекта информатизации, требующего аттестации, в зависимости от информации, которая на нем обрабатывается, проводятся определенные аттестационные испытания. Данные испытания позволяют подтвердить заявленные характеристики безопасности объекта информатизации или автоматизированной системы и проводятся организацией, имеющей на это право (обладающей лицензией и/или аттестатом аккредитации). Аттестация объекта является необходимым условием при работе с конфиденциальной информацией. Объект, прошедший аттестацию, будет допущен к эксплуатации федеральными органами исполнительной власти и не вызовет проблем при

эксплуатации у владельца данного объекта. Аттестованный объект показывает компетентность владельца объекта информатизации и не повлечет санкций за обработку конфиденциальной информации на неаттестованном объекте.

Как сказано в книге «Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации» [1] под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» – подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Федеральной службой по техническому и экспортному контролю (ФСТЭК) России.

Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленными в «Аттестате соответствия» [1].

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации [1].

Целью работы является создание системы защиты автоматизированной системы для подготовки и выдачи квалифицированного сертификата ключа проверки электронной подписи по требованиям защиты конфиденциальной информации и персональных данных.

Задачами выпускной квалификационной работы (ВКР) являются:

- выбор средств защиты для оснащения автоматизированной системы, их установка и настройка;
- разработка внутренней объектовой документации на автоматизированную систему в части защиты информации;
- проведение аттестационных испытаний автоматизированной системы.

1 Анализ состояния отрасли защиты конфиденциальной информации

На современном этапе развития нашего общества многие традиционные ресурсы человеческого прогресса постепенно утрачивают свое первоначальное значение. На смену им приходит новый ресурс, единственный продукт не убывающий, а растущий со временем, называемый информацией. Информация становится сегодня главным ресурсом научно-технического и социально-экономического развития мирового сообщества..

В современном мире информационная безопасность становится жизненно необходимым условием обеспечения интересов человека, общества и государства и важнейшим, стержневым, звеном всей системы национальной безопасности страны.

Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Конфиденциальной информацией может быть любая информация с ограниченным доступом, не отнесённая действующим законодательством к государственной тайне, так как информация с ограниченным доступом - это прежде сведения, данные и знания, известные определенному кругу лиц, имеющих для них особую ценность. Ограничение доступа к информации устанавливается в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Основу для законодательного закрепления отдельных видов конфиденциальной информации в Российском законодательстве составляет Конституция Российской Федерации, в ней закреплено право граждан, организаций и государства на тайну. На основе этих положений Конституции

Российской Федерации отраслевым законодательством выделяются соответствующие виды информации с ограниченным доступом.

Не менее важной проблемой защиты конфиденциальной информации, является состояние информационной безопасности в России, которое характеризуется высоким уровнем технологической зависимости. Это касается как технических средств, так и программного обеспечения, в первую очередь, системного. Такая зависимость в некоторых секторах государственного управления может создать угрозу национальной безопасности.

В России на данный момент по защите конфиденциальной информации как техническими мерами существуют необходимые документы, так и организационными. Часть документации выпущена в этом десятилетии, другая часть в начале прошлого, но она актуальна и является действующей на момент написания данной работы.

Вопрос защиты конфиденциальной информации всегда был важен и актуален, так как невыполнение определенных правил и порядков по ее защите приводит к ответственности со стороны федеральных органов исполнительной власти, а также к потере репутации и доверия со стороны клиентов и других организаций. Таким образом, данный вопрос защиты конфиденциальной информации и персональных данных был выбран для рассмотрения в рамках дипломного проекта.

2 Обзор и анализ нормативной документации и публикаций по защите конфиденциальной информации и персональных данных

2.1 Обзор и анализ нормативной документации по защите конфиденциальной информации

2.1.1 Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) содержат следующие положения:

- термины и определения, которые будут использоваться в данном документе. Это позволяет лучше понимать данный документ и проще ориентироваться в нем;
- общие сведения о защите конфиденциальной информации и способах, мерах и средствах защиты;
- регламентацию порядка защиты конфиденциальной информации на предприятии;
- состав и содержание документационного аналитического обеспечения, необходимого для организации работ по защите конфиденциальной информации на предприятии;
- требования и рекомендации по защите речевой конфиденциальной информации;
- общие требования и рекомендации для защиты конфиденциальной информации, распространяемой в автоматизированных системах;
- требования по защите конфиденциальной информации при использовании съемных накопителей, в локальных вычислительных сетях, при межсетевом взаимодействии и при работе с системами управления с базами данными;

- рекомендации по защите конфиденциальной информации, содержащейся в негосударственных информационных ресурсах;

Таким образом, данный документ в полной мере содержит необходимые сведения, требования, данные и формы для работы специалиста по информационной безопасности в данной отрасли.

2.1.2 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам содержат следующие положения:

- методику оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и вибро-акустическому каналам;

- методику оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах;

- методику оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации;

- временную методику оценки защищенности конфиденциальной информации, обрабатываемой основными средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации.

Таким образом, данный документ содержит все необходимые методики оценки защищенности конфиденциальной информации от утечки по техническим каналам, раскрывает все аспекты данных методик, предоставляет все необходимые данные для работы с этими методиками, а также содержит и формы отчетов для работы специалиста по информационной безопасности и стандартизации в данной отрасли.

2.1.3 ГОСТ РО 0043-003-2012 содержит следующие положения:

- термины и определения, которые используются в данном документе. Это позволяет лучше понимать данный документ и проще ориентироваться в нем;
- основные понятия и тезисы, которые будут раскрываться в дальнейшем. Например, что является целью аттестации, какие виды аттестации бывают, когда проводится аттестация;
- регламентацию процедуры аттестации со стороны всех органов, участвующих в ней;
- порядок аттестации со стороны органа по аттестации, а также действия заявителя;
- условия ввода объекта в эксплуатацию;
- контроль за порядком аттестации и за эксплуатацией аттестованных объектов информатизации.

Таким образом, данный документ в полной мере содержит необходимые сведения, требования, данные и формы для работы органа по аттестации объектов информатизации, а также сведения для заявителей и владельцев объектов информатизации.

2.1.4 ГОСТ РО 0043-004-2013 содержит следующие положения:

- термины и определения, которые будут использоваться в данном документе. Это позволяет лучше понимать данный документ и проще ориентироваться в нем;
- основные виды объектов информатизации, также основные понятия и тезисы, которые будут раскрываться в дальнейшем.
- правила и порядок разработки методик;
- требования к содержанию программы аттестационных испытаний;
- требования к содержанию методик аттестационных испытаний;

Таким образом, данный документ в полной мере содержит необходимые сведения, требования, данные и формы, программы и методики аттестационных испытаний для работы органа по аттестации объектов информатизации.

2.2 Обзор и анализ публикаций по защите конфиденциальной информации

2.2.1 Первым для рассмотрения была взята публикация под названием «Разработка системы защиты конфиденциальной информации» [2]. Данная статья начинается с общих положений и определений, относящихся к защите конфиденциальной информации. Далее в статье описываются требования, выполнение которых необходимо для получения лицензии на право осуществления деятельности по технической защите конфиденциальной информации. Также статья содержит требования к составу устава организации, то есть к наличию пунктов, относящихся к защите конфиденциальной информации. Далее в документе указаны действия руководства при переводе сотрудника в установленном порядке на другую работу, связанную с конфиденциальной информацией, а также при увольнении. Затем приведен возможный список организационных мероприятий, исключающих или уменьшающих возможность возникновения опасности конфиденциальной информации. Следующим пунктом данной статьи идет состав службы безопасности. Далее указаны правила по отнесению информации к конфиденциальной, а также перечень законов, приказов, указов и документов, которыми следует руководствоваться при разработке перечня конфиденциальной информации. После этого указаны правила доведения сформированного перечня до сотрудников организации и обращения сотрудников с ним. Таким образом, данная статья содержит необходимые данные и перечни документов для организации технической и организационной защиты конфиденциальной информации в организации.

2.2.2 Статья «Инструкция по защите конфиденциальной информации в информационной системе предприятия» [3] состоит из восьми разделов:

- 1) Общие положения
- 2) Допуск к использованию ресурсов.
- 3) Доступ к использованию ресурсов. Регистрация пользователей.
- 4) Хранение носителей конфиденциальной информации в информационной системе (ИС).
- 5) Защита ресурсов ИС.
- 6) Инструкция по защите конфиденциальной информации пользователям ресурсов.
- 7) Ответственность за нарушение правил обращения конфиденциальной информации в ИС.
- 8) Контроль.

Первый раздел «Общие положения» содержит цели данной статьи и определения, используемые в ней.

Второй раздел «Допуск к использованию ресурсов» описывает условия, при которых работник организации может быть допущен к конфиденциальной информации.

Следующий раздел «Доступ к использованию ресурсов. Регистрация пользователей» содержит информацию о понятии привилегий системного администратора, лицах, кто имеет право получать такие полномочия. Также данный раздел содержит информацию по обращению с лицензионным и авторским программным обеспечением (ПО), а также с сетевыми службами.

Четвертый раздел «Хранение носителей конфиденциальной информации в ИС» описывает правила хранения магнитных носителей, а также правила обращения с сейфами и правила хранения носителей в архиве.

Пятый раздел «Защита ресурсов ИС» делится на четыре подраздела: физическая защита ресурсов, аппаратная защита ресурсов, программная защита

ресурсов и техническая защита ресурсов. Каждый из этих подпунктов описывает, каким образом можно защитить конфиденциальную информацию с одного из аспектов.

Следующий пункт «Инструкция по защите конфиденциальной информации пользователям ресурсов» содержит перечень действий, запрещенных пользователю, а также правила, которые он должен соблюдать при работе с конфиденциальной информацией.

Седьмой пункт «Ответственность за нарушение правил обращения конфиденциальной информации в ИС» описывает порядок действий со стороны организации над сотрудником, нарушившим правила обращения с конфиденциальной информацией.

Последний пункт «Контроль» содержит информацию о том, кто контролирует выполнение правил персоналом и кто проводит общий контроль.

2.2.3 Статья «Коммерческая ценность информации. Методы ее защиты» поделена на два раздела:

1) Понятие «коммерческая тайна» и «режим коммерческой тайны». Основные положения Федерального закона РФ «О коммерческой тайне» [4].

2) Каналы утечки конфиденциальной информации. Методы защиты конфиденциальной информации: активные и пассивные [5].

Первый раздел содержит понятия коммерческой тайны, режима коммерческой тайны и основные положения федерального закона РФ «О коммерческой тайне». Также данный раздел объясняет понятие «ноу-хау» с точки зрения коммерческой тайны, а также соотношение этих двух понятий. Кроме того описывается понятие коммерческой ценности информации. Далее описывается отсутствие доступа к информации на законном основании. Также в данной части статьи указан перечень мер, необходимых для создания «режима коммерческой тайны» в организации.

Второй раздел описывает проблему утечки конфиденциальной информации, дается понятие этого определения, содержится список возможных каналов утечки и некоторые способы утечки. Также в данном разделе содержатся активные и пассивные методы защиты телефонного аппарата от утечки информации по электроакустическому каналу и от перехвата электронными устройствами.

2.2.4 Таким образом, большинство рассмотренных статей содержат технические решения защиты конфиденциальной информации, методики, различные перечни и списки, которые достаточно легко воспринимаются и впоследствии применяются и используются на практике.

Также были найдены и другие публикации, но большинство из них являются рекламными статьями различных организаций, занимающихся информационной безопасностью, в частности защитой конфиденциальной информации. Данные статьи не подлежат к рассмотрению, так как не несут в себе полезной для данной работы информации.

3 Выбор средств защиты конфиденциальной информации и персональных данных для аттестуемой автоматизированной системы

3.1 Общие положения

Далее в данной работе предстоит выбор средств защиты конфиденциальной информации и персональных данных для аттестуемой автоматизированной системы. Для того, чтобы выбрать средства защиты необходимо учесть меры по обеспечению безопасности как для персональных данных, так и для конфиденциальной информации, так как в защищаемой автоматизированной системе хранятся данные обеих категорий. Для персональных данных уровень защищенности определен как третий. Для конфиденциальных данных класс защищенности определен как 1Г, так как данная АС является многопользовательской и в ней хранится информация разных уровней конфиденциальности.

3.2 Адаптация базового набора мер

Такие меры по обеспечению безопасности, как ИАФ 5, 6, УПД 3, 13-16, АНЗ 1, полный блок мер ЗСВ, ЗИС 3, 20 не учитывались при сравнении СЗИ, так как они не используются в данной автоматизированной системе. ИАФ.5 «Защита обратной связи при вводе аутентификационной информации» [6] не учитывается, так как автоматизированная система находится в отдельном помещении, доступ к которому имеет ограниченный круг лиц, уполномоченный работать с автоматизированной системой. ИАФ.6 «Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)» [6] не учитывается, так как работать с автоматизированной системой могут только работники оператора.

УПД.13 «Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети» [6] не нуждается в рассмотрении, потому что удаленный доступ в данной АС не используется. УПД.14 «Регламентация и контроль использования в информационной системе технологий беспроводного доступа» [6] также не рассматривается, так как беспроводной доступ к данной АС не предусмотрен. УПД.15 «Регламентация и контроль использования в информационной системе мобильных технических средств» [6] не рассматривалась, так как в защищаемой АС нет мобильных технических средств. УПД.16 «Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)» [6] не рассматривается, так как защищаемая АС не имеет взаимодействия с информационными системами сторонних организаций. Блок мер защиты информации «Защита среды виртуализации (ЗСВ)» [6] не рассматривался, так как в защищаемой АС не используется среда виртуализации. ЗИС.3 «Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи» [6] не используется, так как в рассматриваемой АС получаемые и обрабатываемые персональные данные не передаются за пределы контролируемой зоны, а также не используются беспроводные каналы связи. ЗИС.20 «Защита беспроводных соединений, применяемых в информационной системе» [6] не рассматривается, так как в защищаемой АС не применяются беспроводные соединения.

3.3 Сравнение СЗИ для аттестуемой автоматизированной системы

3.3.1 Для сравнения были выбраны одни из самых известных средств защиты персональных данных. Это СЗИ от НСД *Secret Net Studio*, СЗИ от НСД *Dallas Lock 8.0-K* и ПАК *Аккорд-Win64 K*. В таблице 1 приведено сравнение выбранных средств защиты информации по требованиям адаптированного набора мер уровня защищенности 3 приказа ФСТЭК №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [6].

Таблица 1 - Сравнение выбранных средств защиты информации по требованиям адаптированного набора мер уровня защищенности 3 приказа ФСТЭК №21

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Выполнение требований		
		Secret Net Studio	Dallas Lock 8.0-K	ПАК Аккорд-Win64 K
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)				
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Реализуется организационными мерами		
II. Управление доступом субъектов доступа к объектам доступа (УПД)				
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись,	+	+	+

Продолжение таблицы 1

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Выполнение требований		
		Secret Net Studio	Dallas Lock 8.0-K	ПАК Аккорд-Win64 K
	выполнение или иной тип) и правил разграничения доступа			
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Реализация средствами ОС Windows		
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Реализация средствами ОС Windows		
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	Реализация средствами ОС Windows		
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Реализация средствами ОС Windows		
IV. Защита машинных носителей персональных данных (ЗНИ)				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	Реализуется организационными мерами		
V. Регистрация событий безопасности (РСБ)				
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Реализуется организационными мерами		
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Реализуется организационными мерами		
РСБ.3	Сбор, запись и хранение информации о	+	+	+

Продолжение таблицы 1

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Выполнение требований		
		Secret Net Studio	Dallas Lock 8.0-K	ПАК Аккорд-Win64 K
	событиях безопасности в течение установленного времени хранения			
РСБ.7	Защита информации о событиях безопасности	Использование средств антивирусной защиты		
VI. Антивирусная защита (AB3)				
AB3.1	Реализация антивирусной защиты	Использование средств антивирусной защиты.		
AB3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Реализуется организационными мерами		
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)				
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Реализуется организационными мерами		
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Реализуется организационными мерами		
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Реализуется организационными мерами		
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Реализуется организационными мерами		
XII. Защита технических средств (ЗТС)				
ЗТС.3	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, в помещения и сооружения, в которых они установлены	Реализуется организационными и техническими мерами		
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Реализуется организационными и техническими мерами		
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)				

Продолжение таблицы 1

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Выполнение требований		
		Secret Net Studio	Dallas Lock 8.0-K	ПАК Аккорд-Win64 K
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных	Реализуется организационными мерами		
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	Реализуется организационными мерами		
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных	Реализуется организационными мерами		
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных	Реализуется организационными мерами		

3.3.2 Сравнение СЗИ для аттестуемой автоматизированной системы по требованиям руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г.

Далее в таблице 2 приведено сравнение выбранных средств защиты информации по требованиям руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г. [7] по классу защищенности 1Г.

Таблица 2 - Сравнение выбранных средств защиты информации по требованиям руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» по классу защищенности 1Г

№	Подсистемы и требования	Выполнение требований		
		Secret Net Studio	Dallas Lock 8.0-K	ПАК Аккорд-Win64 К
1. Подсистема управления доступом				
1.1	Идентификация, проверка подлинности и контроль доступа субъектов: - в систему - к терминалам ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ - к программам - к томам, каталогам, файлам, записям, полям записей	+ + + +	+ + + +	+ + + +
2. Подсистема регистрации и учета				
2.1.	Регистрация и учет: - входа (выхода) субъектов доступа в (из) систему - выдачи печатных (графических) выходных документов - запуска (завершения) программ и процессов (заданий, задач) - доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи - доступа программ субъектов доступа к терминалам ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	+ + + + - -	+ + + - - -	+ + + - - -
2.2.	Учет носителей информации	+	+	+
2.3.	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	+	+	-
3. Подсистема обеспечения целостности				
3.1.	Обеспечение целостности программных средств и обрабатываемой информации	+	+	+
3.2.	Физическая охрана средств вычислительной техники и носителей информации	реализуется организационными мерами		
3.4.	Периодическое тестирование СЗИ от НСД			
3.5.	Наличие средств восстановления СЗИ от НСД	+	+	-
4. Другое				
4.1	Наличие сертификата ФСТЭК	+	+	-

3.3.3 Выбор средств защиты для аттестуемой автоматизированной системы

По результатам проведенных сравнений было определено, что выбранные средства защиты информации по требованиям приказа ФСТЭК №21 практически равны. По требованиям руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» по классу защищенности 1Г имеет преимущества перед другими выбранными средствами защиты информации от несанкционированного доступа (СЗИ от НСД). Программно-аппаратный комплекс (ПАК) *Аккорд-Win64 К* не поддерживает функцию очистки (обнуления, обезличивания) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей, а также не обладает средствами восстановления. Также ПАК *Аккорд-Win64 К* не имеет сертификата ФСТЭК. На основании отсутствия данных функций данное СЗИ от НСД не было выбрано.

СЗИ от НСД *Dallas Lock 8.0-К* не имеет возможности регистрации доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи.

Таким образом, было принято решение выбрать СЗИ от НСД *Secret Net Studio*. Данная СЗИ удовлетворяет почти всем критериям, по которым производилось сравнение, также данное СЗИ обладает множеством дополнительных модулей и имеет сертификат ФСТЭК.

Также было принято решение оборудовать защищаемую автоматизированную систему ПАК *Соболь*. Данное средство предназначено для обеспечения повышенного контроля целостности и использования идентификаторов пользователя. Также ПАК *Соболь* содержит датчик случайных чисел, необходимый для функционирования рассматриваемой автоматизированной системы для подготовки и выдачи сертификатов

электронной подписи. Данное средство имеет сертификат ФСТЭК и может быть использовано в автоматизированных системах с установленным уровнем защищенности 3 и классом защищенности 1Г.

Для выполнения мер защиты информации РСБ.7, АВЗ.1 и АВЗ.2 на защищаемую автоматизированную систему было принято решение установить средство антивирусной защиты *Kaspersky Endpoint Security 10*. Данное средство имеет сертификат ФСТЭК и может быть использовано в автоматизированных системах с установленным уровнем защищенности 3 и классом защищенности 1Г.

3.4 Выполнение требований по защите от несанкционированного доступа

Требования и подходы защиты конфиденциальной информации и персональных данных имеют отличия, поэтому общий подход к защите информации в автоматизированной системе (АС) должен учитывать как требования по защите конфиденциальной информации, так и требования по защите персональных данных. Поэтому в данной работе необходимо рассмотреть оба направления параллельно.

Таким образом, в таблице 3 показано выполнение требований приказа ФСТЭК №21 [6] по защите от несанкционированного доступа по уровню защищенности 3, а в таблице 4 выполнение требований руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации по защите конфиденциальной информации от несанкционированного доступа» [7] по классу защищенности 1Г в защищаемой АС.

Таблица 3 - Выполнение требований по защите персональных данных от несанкционированного доступа по уровню защищенности 3

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Способ реализации
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Использование возможностей Secret Net Studio, ПАК «Соболь» с персональными идентификаторами iButton; инструкция администратора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	
II. Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Реализация средствами ОС Windows, Secret Net Studio и ПАК «Соболь»
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Реализация средствами ОС Windows
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	Реализация средствами Secret Net Studio
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Реализация средствами ОС Windows
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Реализация средствами ОС Windows
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Реализация средствами ОС Windows, Secret Net Studio и ПАК «Соболь»

Продолжение таблицы 3

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Способ реализации
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	Реализация средствами ОС Windows
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Реализация средствами ОС Windows и ПАК «Соболь»
IV. Защита машинных носителей персональных данных (ЗНИ)		
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	Установленный инструкцией пользователя порядок уничтожения и обезличивания персональных данных средствами Secret Net Studio
V. Регистрация событий безопасности (РСБ)		
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Определено инструкцией администратора и политиками ИБ организации
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Определено инструкцией администратора
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Реализация средствами Secret Net Studio
РСБ.7	Защита информации о событиях безопасности	Использование средств антивирусной защиты
VI. Антивирусная защита (АВЗ)		
АВЗ.1	Реализация антивирусной защиты	Использование средств антивирусной защиты <i>Kaspersky Endpoint Security 10</i>
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Порядок обновления базы данных признаков вредоносных компьютерных программ установлен инструкцией администратора
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)		
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Определяется инструкцией администратора
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Порядок установки обновлений установлен инструкцией администратора
АНЗ.3	Контроль работоспособности,	Определяется инструкцией

Продолжение таблицы 3

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Способ реализации
	параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	администратора
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Определяется инструкцией администратора
XII. Защита технических средств (ЗТС)		
ЗТС.3	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, в помещения и сооружения, в которых они установлены	Установление пропускного режима на предприятии; замок на входе в комнату, где установлена АС, ключ от которого выдается только допущенным к работе с данной АС лицам
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Расположение дисплея монитора относительно окон, дверей, не позволяющее осуществить просмотр информации не допущенными к обработке ПДн сотрудниками
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)		
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных	Определено политиками ИБ организации
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	Установлено инструкцией администратора
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных	Определено политиками ИБ организации и инструкцией администратора и пользователя
УКФ.4	Документирование информации (данных)	Определено политиками

Продолжение таблицы 3

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Способ реализации
	об изменениях в конфигурации информационной системы и системы защиты персональных данных	ИБ организации

Таблица 4 - Выполнение требований по защите конфиденциальной информации от несанкционированного доступа по классу защищенности 1Г

№	Подсистемы и требования	Выполнение требований
1. Подсистема управления доступом		
1.1	Идентификация, проверка подлинности и контроль доступа субъектов: - в систему - к терминалам ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ - к программам - к томам, каталогам, файлам, записям, полям записей	 + + + +
2. Подсистема регистрации и учета		
2.1.	Регистрация и учет: - входа (выхода) субъектов доступа в (из) систему - выдачи печатных (графических) выходных документов - запуска (завершения) программ и процессов (заданий, задач) - доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи - доступа программ субъектов доступа к терминалам ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	 + + + + —
2.2.	Учет носителей информации	+
2.3.	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	+
3. Подсистема обеспечения целостности		
3.1.	Обеспечение целостности программных средств и обрабатываемой информации	+
3.2.	Физическая охрана средств вычислительной техники и носителей информации	реализуется организационными и техническими мерами
3.4.	Периодическое тестирование СЗИ от НСД	
3.5.	Наличие средств восстановления СЗИ от НСД	+
4. Другое		
4.1	Наличие сертификата ФСТЭК	+

4 Настройка средств защиты информации

4.1 Общие положения

В ходе выполнения дипломного проектирования была выполнена настройка средства защиты информации от несанкционированного доступа *Secret Net Studio*, ПАК *Соболь* и антивируса *Kaspersky Endpoint Security 10*.

4.2 Настройка ПАК *Соболь*

Программно-аппаратный комплекс *Соболь* настраивается до загрузки операционной системы. Для настройки был открыт раздел «Общие параметры». Параметр «Автономный режим работы» включен. «Число попыток тестирования ДСЧ» установлено равным трем. Включено «Тестирование ДСЧ» для пользователя. «Показ статистики пользователю» отключен. Максимальный срок действия пароля установлен равным 90 дням. Предельное число неудачных входов пользователя установлено равным 5. Поддержка USB идентификаторов отключена. Настройка общих параметров ПАК *Соболь* представлена на рисунке 1.

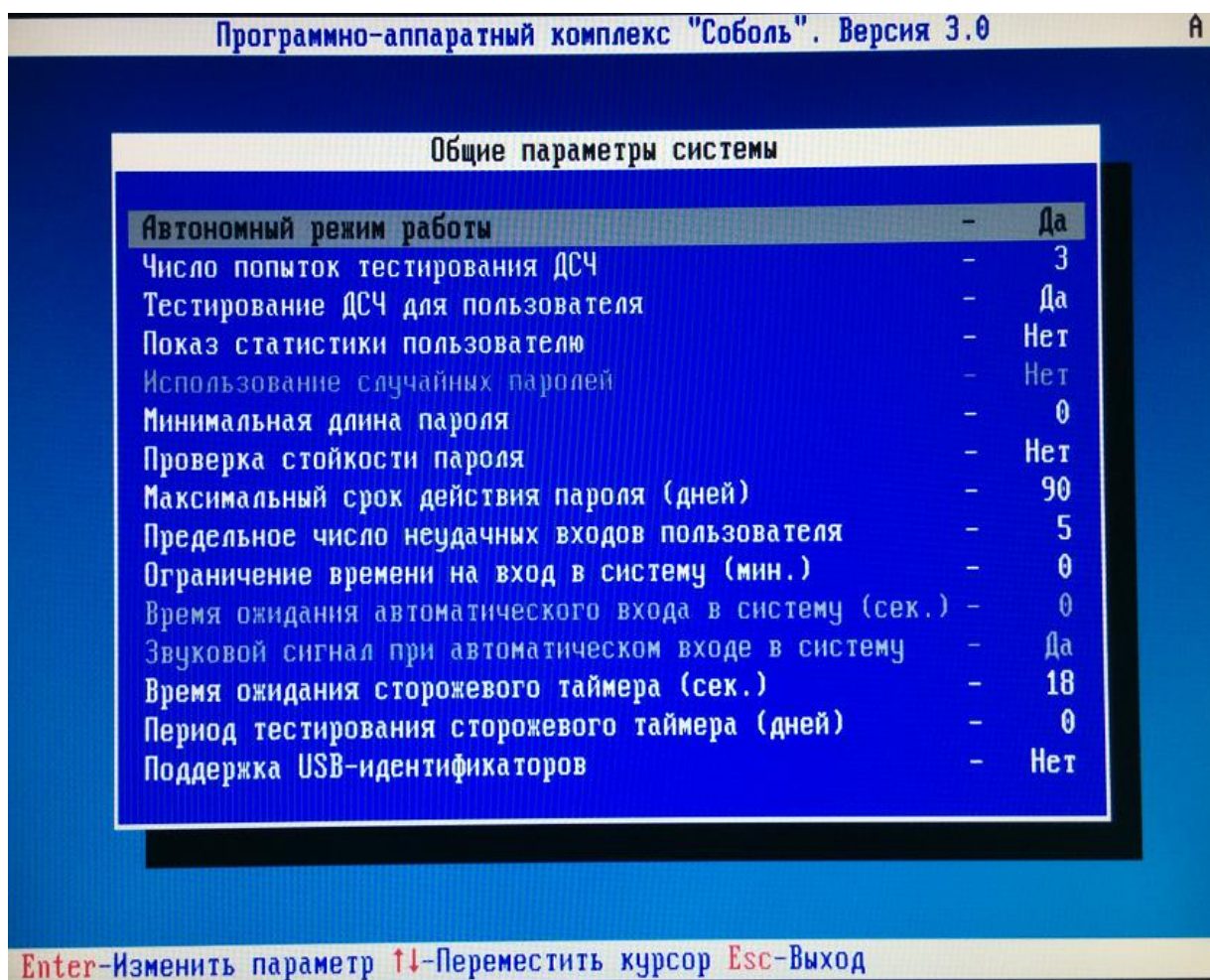


Рисунок 1 - Настройка ПАК «Соболь»

Далее была проведена настройка пользователей. Для этого был открыт раздел «Зарегистрированные пользователи». В данном разделе параметр «Режим контроля целостности» установлен как жесткий. Включен запрет загрузки с внешних носителей. Также включено ограничение срока действия пароля. Настройка для зарегистрированных пользователей представлена на рисунке 2. Также в этом разделе указывается номер идентификатора, время последнего входа, общее количество входов и количество неудачных попыток входа конкретного пользователя.

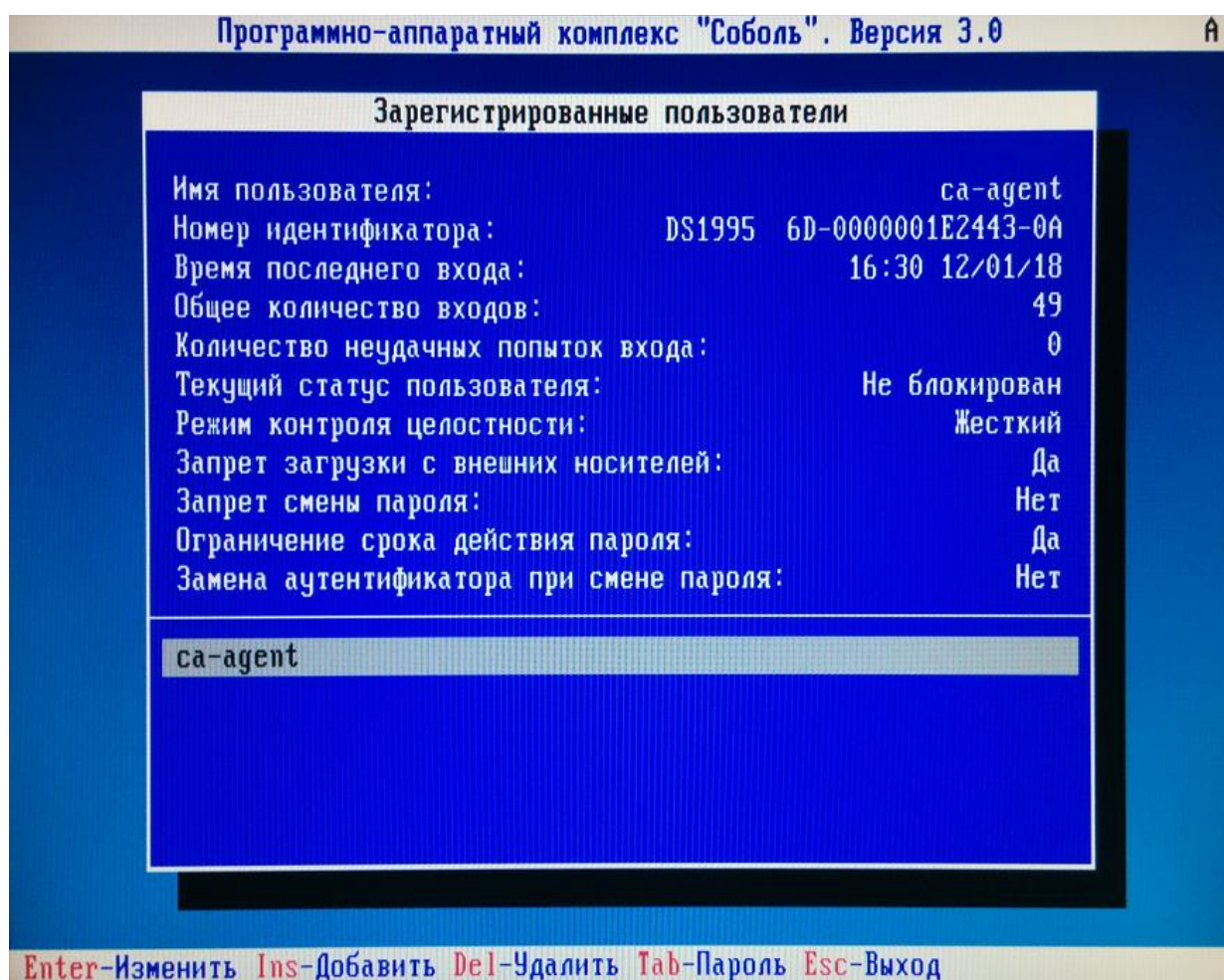


Рисунок 2 - Настройка для зарегистрированных пользователей

ПАК «Соболь» работает в паре с СЗИ от НСД Secret Net Studio. После выполнения настроек обоих средств, при запуске системы пользователю необходимо будет предъявить персональный идентификатор, о чем будет выдано информационное сообщение, представленное на рисунке 3. После этого необходимо будет ввести пароль в специальную форму, представленную на рисунке 4. Только после этого будет выполнена загрузка системы под контролем Secret Net Studio.



Рисунок 3 - Информационное сообщение

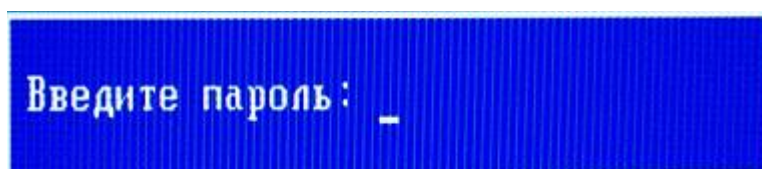


Рисунок 4 - Форма ввода пароля

Таким образом настройка ПАК *Соболь* выполнена в соответствии с требованиями по защите персональных данных от несанкционированного доступа по уровню защищенности 3 и требованиями по защите конфиденциальной информации от несанкционированного доступа по классу защищенности 1Г.

4.3 Настройка СЗИ от НСД *Secret Net Studio*

Настройка СЗИ от НСД *Secret Net Studio* выполняется в программе «Secret Net Studio – Центр управления». Для настройки необходимо запустить эту программу и открыть вкладку «Настройки». В правой стороне экрана находятся вкладки с основными разделами настроек: «Политики», «Регистрация событий», «Параметры». Данные разделы включают в себя подразделы, которые в свою очередь включают в себя вкладки.

Для того чтобы выполнить настройку входа в систему, был выбран раздел «Политики», подраздел «Базовая защита», вкладка «Вход в систему». Была выполнена настройка входа в систему. Максимальный период до блокировки экрана установлен в 20 минут, включен запрет вторичного входа в систему, количество неудачных попыток аутентификации установлено равным 5. Выполненная настройка представлена на рисунке 5.

Базовая защита

Вход в систему		Аудит...
Максимальный период неактивности до блокировки экрана	<input type="text" value="20"/> минут	
Запрет вторичного входа в систему	☒ Включить	
Реакция на изъятие идентификатора	<input type="text" value="Не блокировать"/>	
Количество неудачных попыток аутентификации	<input type="text" value="5"/> попыток	
Режим аутентификации пользователя	☒ Стандартная аутентификация ☐ Усиленная аутентификация по паролю ☐ Регистрировать неверные аутентификационные данные	
Режим идентификации пользователя	<input type="text" value="Смешанный"/>	

Рисунок 5 - Настройка входа в систему

Для настройки дискреционного управления доступом был выбран раздел «Политики», подраздел «Защита локальных ресурсов», вкладка «Дискреционное управление доступом». Настройка дискреционного управления доступом представлена на рисунке 6.

Защита локальных ресурсов

Дискреционное управление доступом		Аудит...
Учетные записи с привилегией управления правами доступа	<div>BUILTIN\Администраторы</div>	
<div> </div>		

Рисунок 6 - Настройка дискреционного управления доступом

Для настройки затирания данных доступом был выбран раздел «Политики», подраздел «Защита локальных ресурсов», вкладка «Затирание данных». Параметры «Количество циклов затирания на локальных дисках», «Количество циклов затирания на сменных носителях» и «Количество циклов затирания» установлены равным 1. Настройка затирания данных представлена на рисунке 7.

Защита локальных ресурсов

Затирание данных		
Количество циклов затирания на локальных дисках	<input type="text" value="1"/>	
Количество циклов затирания на сменных носителях	<input type="text" value="1"/>	
Количество циклов затирания оперативной памяти	<input type="text" value="1"/>	

Рисунок 7 - Настройка затирания данных

Для настройки полномочного управления доступом был выбран раздел «Политики», подраздел «Защита локальных ресурсов», вкладка «Полномочное управление доступом». Уровень конфиденциальности установлен как «Конфиденциально». Также включен контроль потоков. Настройка полномочного управления доступом представлена на рисунке 8.

Полномочное управление доступом		Аудит...
Названия уровней конфиденциальности	<div><div>Конфиденциально</div><div>Секретно</div><div>Совершенно секретно</div></div>	
	<div></div>	
Режим работы	<div><div>☐ Контроль потоков отключен</div><div>☒ Контроль потоков включен</div></div> <div><div>☒ Строгий контроль терминальных подключений</div><div>☒ Автоматический выбор максимального уровня сессии</div></div>	

Рисунок 8 - Настройка полномочного управления доступом

Для настройки замкнутой программной среды был выбран раздел «Политики», подраздел «Защита локальных ресурсов», вкладка «Замкнутая программная среда». Настройка замкнутой программной среды представлена на рисунке 9.

Защита локальных ресурсов

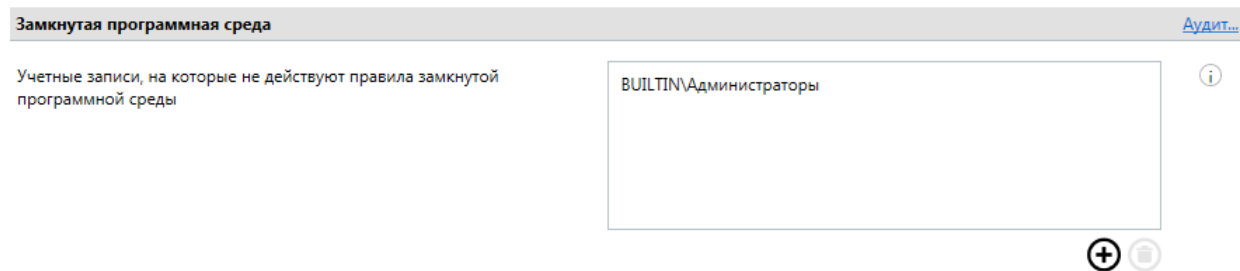


Рисунок 9 - Настройка замкнутой программной среды

Для настройки межсетевого экрана был выбран раздел «Защита сетевых подключений», подраздел «Межсетевой экран». Настройка межсетевого экрана представлена на рисунке 10.

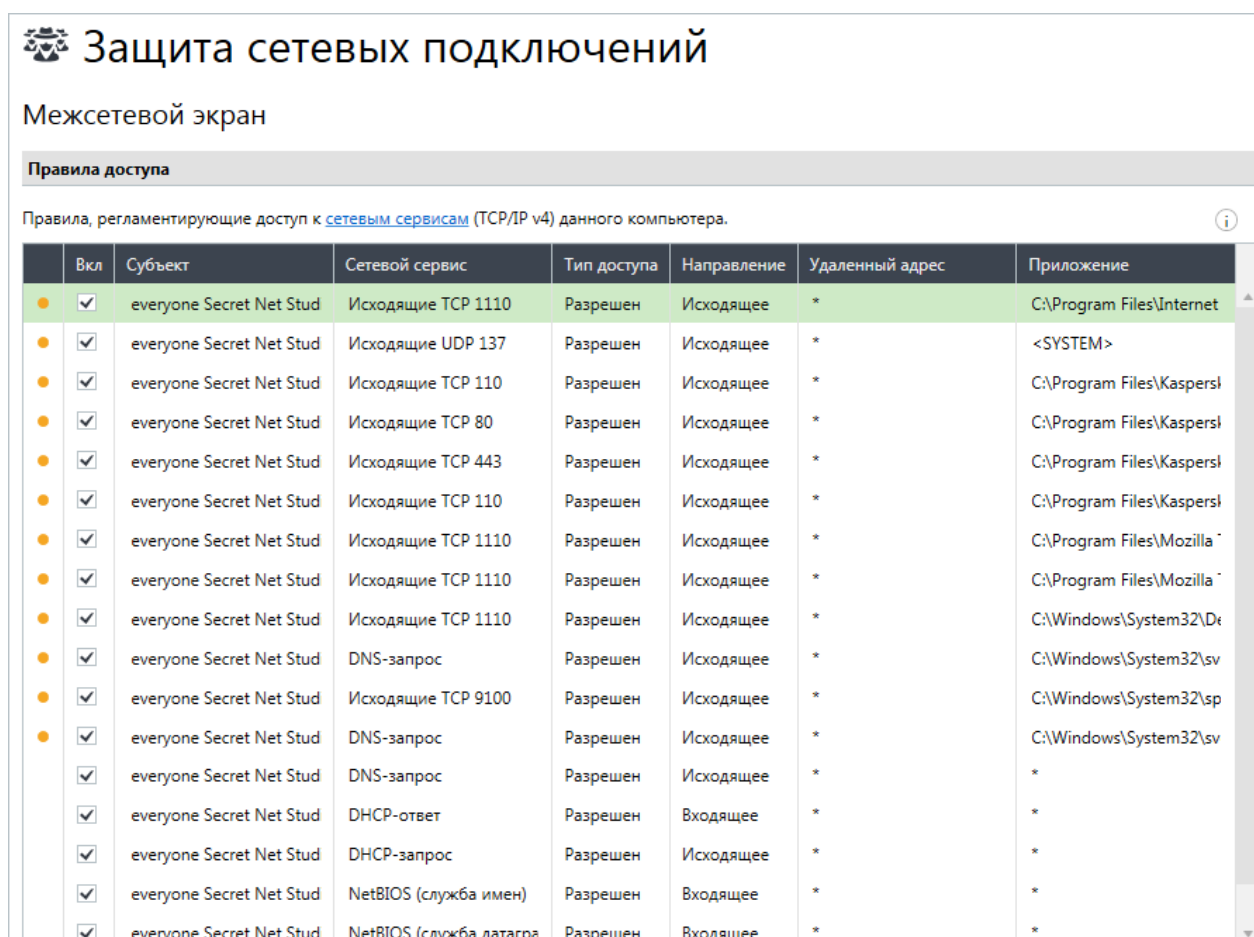


Рисунок 10 - Настройка межсетевого экрана

Для настройки контроля устройств был выбран раздел «Защита сетевых подключений», подраздел «Контроль устройств». Параметр «Теневое

копирование» установлен в положение «Определяется настройками устройства». Параметр «Перенаправление устройств в RDP-подключениях» для COM-портов, LPT-портов, дисков и устройств Plug and Play установлен в положение «Запрещено». Настройки для портов представлены на рисунке 11.

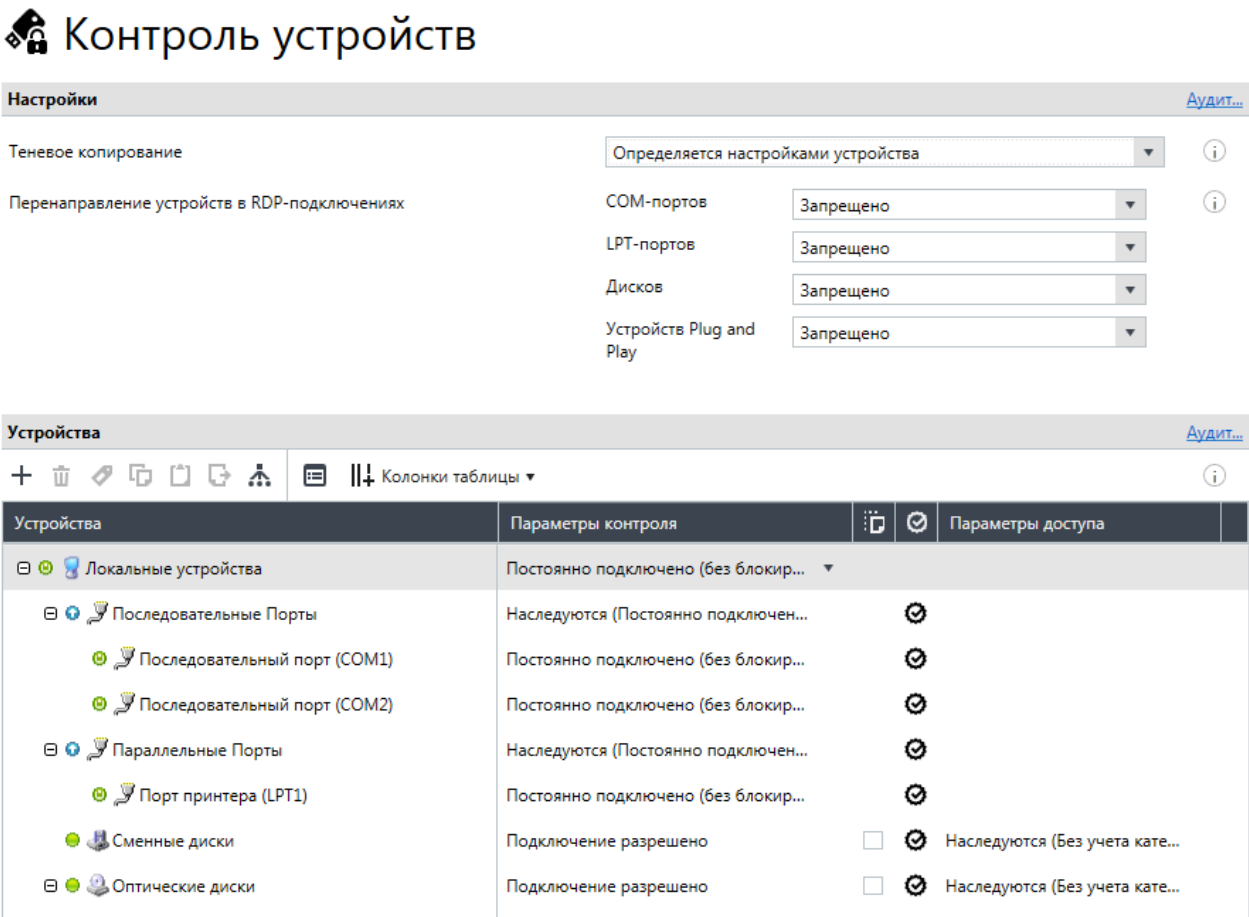


Рисунок 11 - Настройка контроля устройств

Настройки для устройств USB и устройств хранения представлены на рисунке 12. Настройки для электронных идентификаторов и считывателей представлены на рисунке 13.

Устройства	Параметры контроля	Параметры доступа
Системная плата	Наследуются (Постоянно подключен...	
Аппаратная поддержка	Постоянно подключено (с блокиров...	
ООО "Код Безопасности" ПАК "Соболь"	Постоянно подключено (с блокиров...	
Программно-реализованные диски	Подключение запрещено	☐ ☒ Наследуются (Без учета кате...
Устройства USB	Подключение разрешено	Без учета категории
Сетевые платы и модемы	Подключение запрещено	☐ Наследуются (Без учета кате...
Интерфейсные устройства (мышь, клавиату...	Подключение запрещено	☐ Наследуются (Без учета кате...
Aladdin R.D. JaCarta U2F (JC602) (VID_24D...	Подключение разрешено	Без учета категории
Сканеры и цифровые фотоаппараты	Подключение запрещено	☐ Наследуются (Без учета кате...
Принтеры	Подключение запрещено	☐ Наследуются (Без учета кате...
Устройства хранения	Подключение запрещено	☐ ☒ Наследуются (Без учета кате... ▾
Generic Mass Storage 2498446B	Подключение разрешено	☐ ☒ Без учета категории
Kingston DataTraveler 2.0 2008012500000...	Подключение разрешено	☐ ☒ Без учета категории
Kingston DT 101 II 5B8818000021	Подключение разрешено	☐ ☒ Без учета категории

Рисунок 12 - Настройки для устройств USB и устройств хранения

Электронные идентификаторы и считыватели	Не контролируется	Без учета категории
iKey 2032	Наследуются (Не контролируется) ▾	Наследуются (Без учета кате...
eToken Pro (CardOS 4)	Наследуются (Не контролируется)	Наследуются (Без учета кате...
eToken Pro (CardOS 4.01)	Наследуются (Не контролируется)	Наследуются (Без учета кате...
eToken Pro (CardOS 4.2)	Наследуются (Не контролируется)	Наследуются (Без учета кате...
eToken Pro (Java)	Наследуются (Не контролируется)	Наследуются (Без учета кате...
ESMART Token	Наследуются (Не контролируется)	Наследуются (Без учета кате...
RuToken	Наследуются (Не контролируется)	Наследуются (Без учета кате...
RuToken S	Наследуются (Не контролируется)	Наследуются (Без учета кате...
Aktiv Co. Rutoken S (VID_0A89 PID_00...	Не контролируется	Без учета категории
RuToken Lite	Наследуются (Не контролируется)	Наследуются (Без учета кате...
Aktiv Rutoken lite (VID_0A89 PID_0025)	Не контролируется	Без учета категории
RuToken ЭЦП	Наследуются (Не контролируется)	Наследуются (Без учета кате...
Athena ASEDrive V3	Наследуются (Не контролируется)	Наследуются (Без учета кате...
Athena ASEDrive IIIe	Наследуются (Не контролируется)	Наследуются (Без учета кате...

Рисунок 13 - Настройки для электронных идентификаторов и считывателей

Для настройки регистрации событий был выбран раздел «Регистрация событий». В данном разделе была включена регистрация всех событий во всех

подразделах. Пример настройки регистрации событий представлен на рисунке 14.

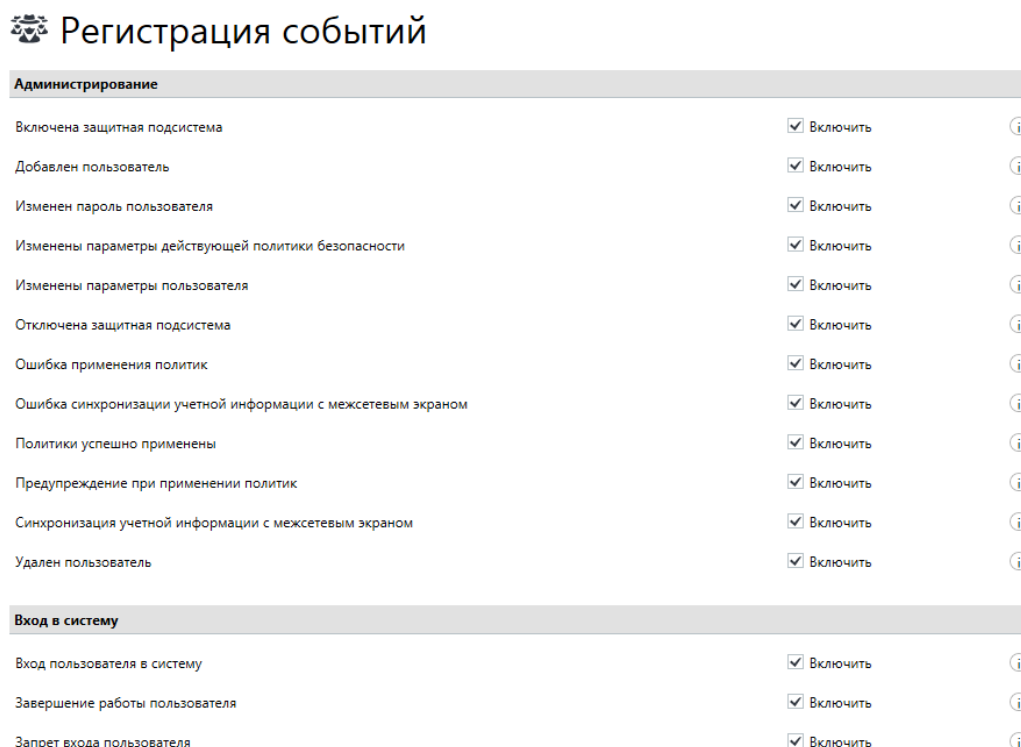


Рисунок 14 - Настройка регистрации событий

Для настройки пункта «Учетная информация» был выбран раздел «Параметры», подраздел «Учетная информация». Из этого подраздела была запущена программа «Управление параметрами безопасности пользователей». Была выбрана группа пользователей «Администраторы». В данную группу были добавлены пользователи «Admin» и «Администратор». Результат представлен на рисунке 15. Далее была выбрана группа пользователей «Пользователи». В данную группу был добавлен пользователь «sa-agent». Результат представлен на рисунке 16. Таким образом было настроено разделение полномочий в среде Secret Net Studio.

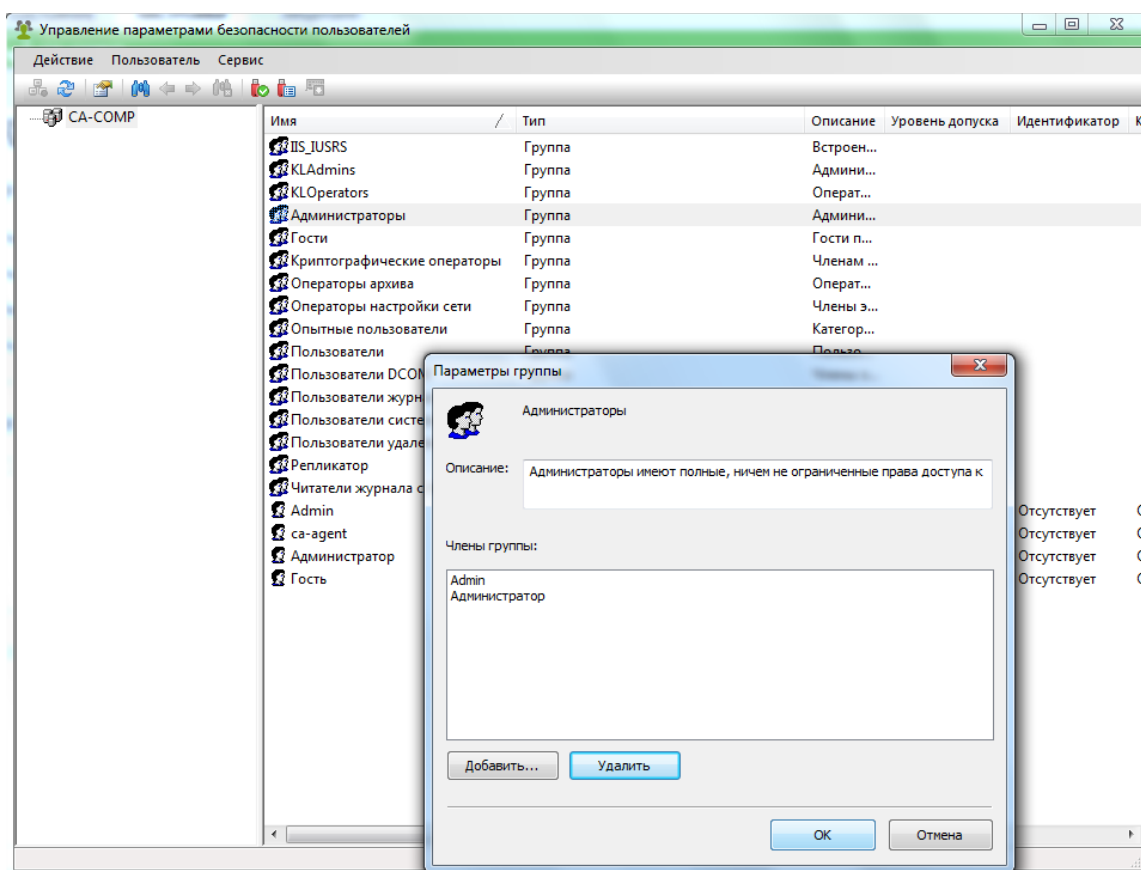


Рисунок 15 - Добавление администраторов

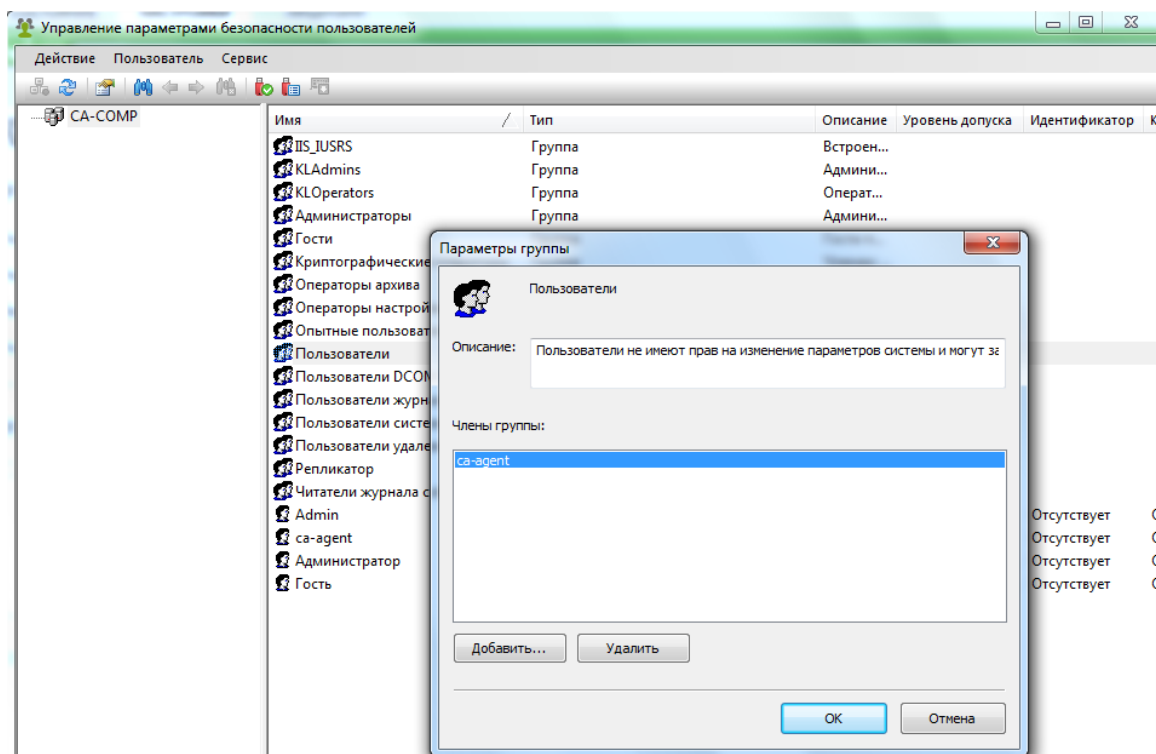


Рисунок 16 - Добавление пользователей

Для настройки субъектов управления была запущена программа «Контроль программ и данных». В разделе «Субъекты управления» настраивается замкнутая программная среда для групп пользователей путем добавления ранее созданных заданий в группу субъекта управления. В данном разделе была настроена замкнутая программная среда для группы «Пользователи», а также для всего компьютера. Настройка субъектов управления представлена на рисунке 17.

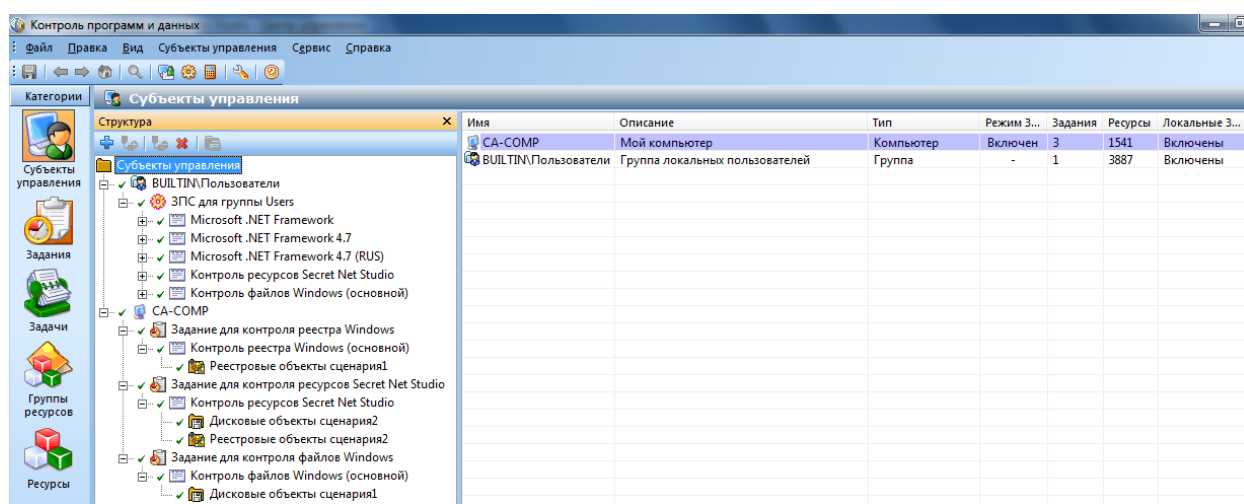


Рисунок 17 - Настройка субъектов управления

Для настройки групп ресурсов в программе «Контроль программ и данных» открыт раздел «Группы ресурсов». В этом разделе создаются списки файлов, подлежащие контролю и обладающие параметрами. Данные списки и являются группами ресурсов, которые затем добавляются в задания. В процессе выполнения настройки были созданы следующие группы ресурсов: Microsoft.NET Framework 4.7 (RUS) Реестр, Microsoft.NET Framework 4.7 (RUS) Файлы, Microsoft.NET Framework 4.7 Реестр, Microsoft.NET Framework 4.7 Файлы, Дисковые объекты сценария, Дисковые объекты сценария1, Дисковые объекты сценария2, Модули Assembly, Модули Microsoft.NET, Реестровые объекты сценария, Реестровые объекты сценария1, Реестровые объекты сценария2. Созданные группы ресурсов показаны на рисунке 18.

Группы ресурсов		Имя	Изменен	Путь/Описание	Тип	Эталоны	Контро...	Выполняем...	Группы
Структура									
Группы ресурсов									
Microsoft .NET Framework 4.7 (RUS) Реестр		netutils.dll	23.06.2017 10:47:32	C:\Windows\system32\	Файл	2	ДА	ДА	7
Microsoft .NET Framework 4.7 (RUS) Файлы		newdev.dll	23.06.2017 10:47:32	C:\Windows\system32\	Файл	2	ДА	ДА	7
Microsoft .NET Framework 4.7 Реестр		nlaapi.dll	23.06.2017 10:47:32	C:\Windows\system32\	Файл	2	ДА	ДА	7
Microsoft .NET Framework 4.7 Файлы		Normaliz.dll	23.06.2017 10:47:32	C:\Windows\SYSTEM32\	Файл	2	ДА	ДА	7
Дисковые объекты сценария		ntdll.dll	23.06.2017 10:47:32	C:\Windows\system32\	Файл	2	ДА	ДА	7
Дисковые объекты сценария2		NTDSAPI.dll	23.06.2017 10:47:32	C:\Windows\system32\	Файл	2	ДА	ДА	7
Модули Assembly		ntkrnlpa.exe	23.06.2017 10:47:33	C:\Windows\SYSTEM32\	Файл	2	ДА	ДА	2
Модули Microsoft.NET		ntoskrnl.exe	23.06.2017 10:47:33	C:\Windows\SYSTEM32\	Файл	2	ДА	ДА	7
Реестровые объекты сценария		HAL.dll	23.06.2017 10:47:33	C:\Windows\SYSTEM32\	Файл	2	ДА	ДА	7
Реестровые объекты сценария1		HID.DLL	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
Реестровые объекты сценария2		ieetwcollector.exe	23.06.2017 10:47:33	C:\Windows\SYSTEM32\	Файл	2	ДА	ДА	2
		iertutil.dll	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		imagehlp.dll	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		IMM32.dll	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		IPHLPAPI.DLL	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		ntshrui.dll	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		nvsvsc.exe	23.06.2017 10:47:33	C:\Windows\SYSTEM32\	Файл	2	ДА	ДА	2
		ODBC32.dll	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		ole32.dll	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		OLEACC.dll	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		OLEAUT32.dll	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		oledlg.dll	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		OSUNINST.dll	23.06.2017 10:47:33	C:\Windows\SYSTEM32\	Файл	2	ДА	ДА	7
		pcwum.dll	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		alg.exe	23.06.2017 10:47:33	C:\Windows\SYSTEM32\	Файл	2	ДА	ДА	2
		API-MS-Win-Core-Co...	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		API-MS-Win-Core-Dat...	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		API-MS-Win-Core-De...	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		API-MS-Win-Core-Del...	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		API-MS-Win-Core-Err...	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7
		API-MS-Win-Core-Fib...	23.06.2017 10:47:33	C:\Windows\system32\	Файл	2	ДА	ДА	7

Рисунок 18 - Созданные группы ресурсов

Для настройки заданий в программе «Контроль программ и данных» открыт раздел «Задания». В данном разделе были созданы задания по контролю реестра Windows и задание для контроля ресурсов Secret Net Studio. Также создается задание для контроля файлов Windows и задание замкнутой программной среды для группы Users. В созданные задания добавляются группы ресурсов, сформированные при выполнении предыдущего пункта настройки. Сформированные задания представлены на рисунке 19.

Таким образом, настройка СЗИ от НСД *Secret Net Studio* выполнена в соответствии с требованиями по защите персональных данных от несанкционированного доступа по уровню защищенности 3 и требованиями по защите конфиденциальной информации от несанкционированного доступа по классу защищенности 1Г.

Имя	Изменен	Путь/Описание	Тип	Эталоны	Контроль	Выполняется	Группы
Image File Execution ...	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Ключ	1	ДА	нет	1
clview.exe	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Ключ	1	ДА	нет	1
DisableExceptionChai...	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Перемен...	1	ДА	нет	1
DIINXOptions	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Ключ	1	ДА	нет	1
Apitrap.dll	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Перемен...	1	ДА	нет	1
ASSTE.dll	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Перемен...	1	ДА	нет	1
AVSTE.dll	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Перемен...	1	ДА	нет	1
Cleanup.dll	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Перемен...	1	ДА	нет	1
divx.dll	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Перемен...	1	ДА	нет	1
divxdec.ax	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Перемен...	1	ДА	нет	1
NORMALIZ	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
MSVCRT	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
MSCTF	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
LPK	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
kernel32	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
IMM32	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
IMAGEHLP	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
IERTUTIL	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
gdi32	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
DIIDirectory	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
DirxApi	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
COMDLG32	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
clbcatq	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
advapi32	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Перемен...	1	ДА	нет	1
KnownDlls	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\System\Curre...	Ключ	1	ДА	нет	1
Security Packages	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SYSTEM\Curr...	Перемен...	1	ДА	нет	1
Notification Packages	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SYSTEM\Curr...	Перемен...	1	ДА	нет	1
Authentication Packa...	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SYSTEM\Curr...	Перемен...	1	ДА	нет	1
VMApplet	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Перемен...	1	ДА	нет	1
Userinit	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Перемен...	1	ДА	нет	1
Shell	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Перемен...	1	ДА	нет	1
Dll Name	23.06.2017 10:47:54	HKEY_LOCAL_MACHINE\SOFTWARE\...	Перемен...	1	ДА	нет	1

Рисунок 19 - Сформированные задания

4.4 Настройка Kaspersky Endpoint Security 10

Для настройки обновлений вызвано окно «Обновление». Во вкладке «Источник» отмечены «Серверы обновлений «Лаборатории Касперского»» и «Kaspersky Security Center». Во вкладке «Режим запуска» выбран параметр «По расписанию». Параметр «периодичность» установлен в положение «Часы». Параметр «Выполнять каждые» установлен равным 6 часам. Настройка обновлений Kaspersky Endpoint Security 10 представлена на рисунке 20 и 21.

Для настройки файлового антивируса в главном окне программы, представленном на рисунке 22, выбрана вкладка «Настройка». В данном разделе выбран пункт «Файловый антивирус». В открывшемся окне во вкладке «Общие» в пункте «Типы файлов» выбран параметр «Файлы, проверяемые по формату». В разделе область защиты были отмечены все доступные области памяти. Данные настройки представлены на рисунке 23. Далее были выполнены настройки во вкладке «Производительность». Был включен эвристический анализ, параметр «Проверять только новые и измененные

файлы» и в разделе «Проверка составных файлов» отмечены все значения. Настройки во вкладке «Производительность» показаны на рисунке 24.

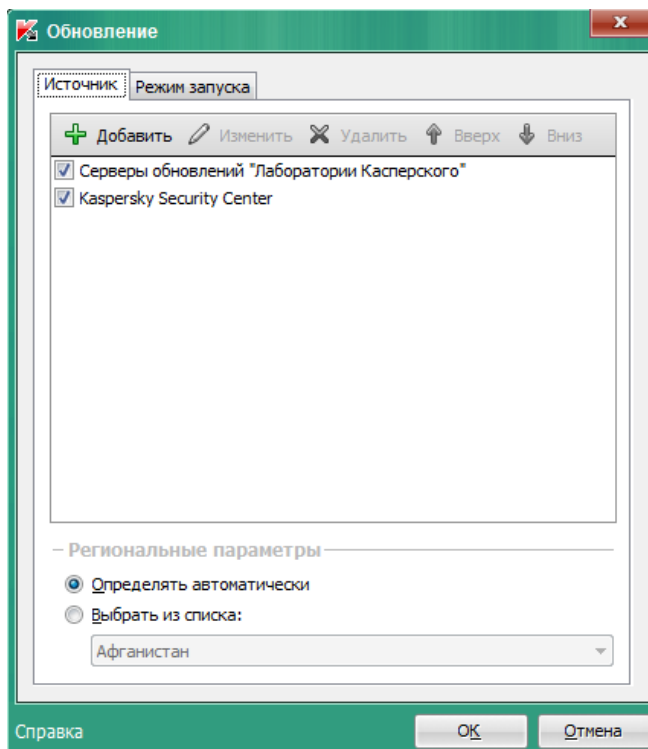


Рисунок 20 - Настройка источника обновлений

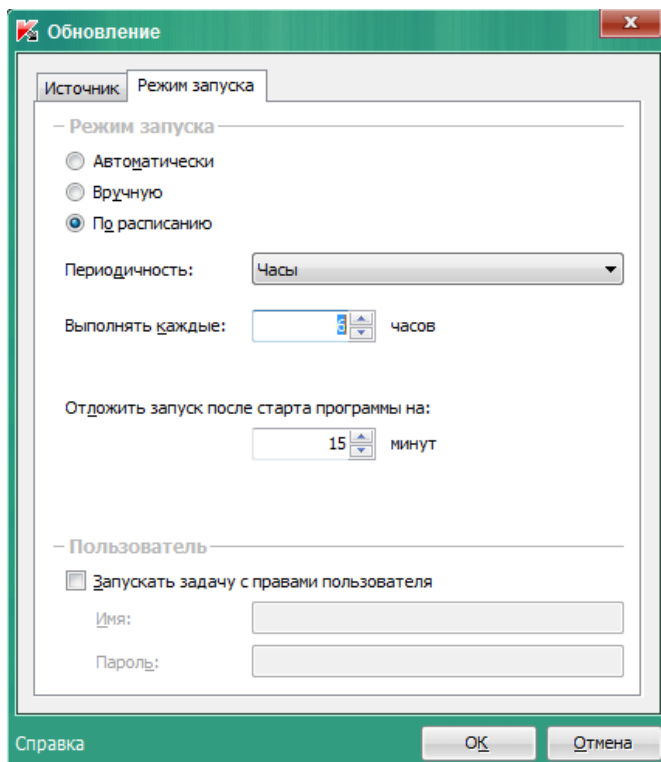


Рисунок 21 - Настройка обновлений

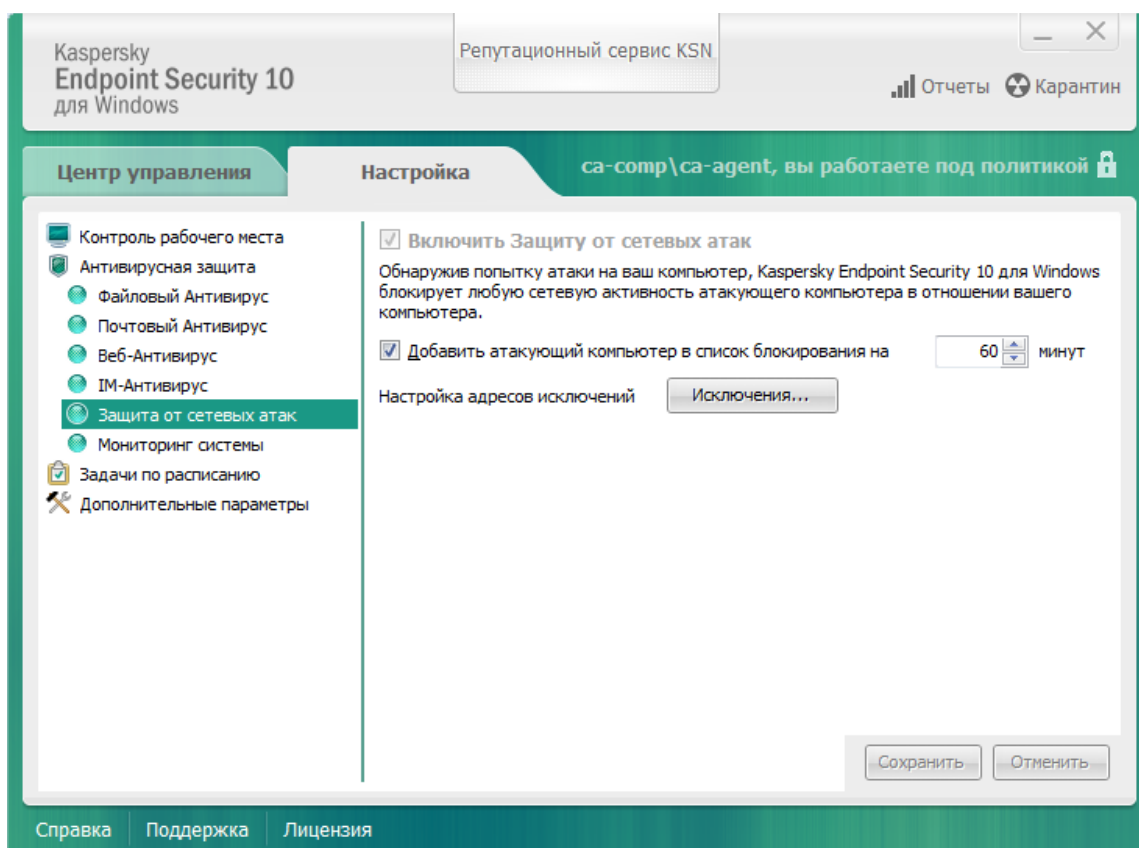


Рисунок 22 - Общий вид Kaspersky Endpoint Security 10

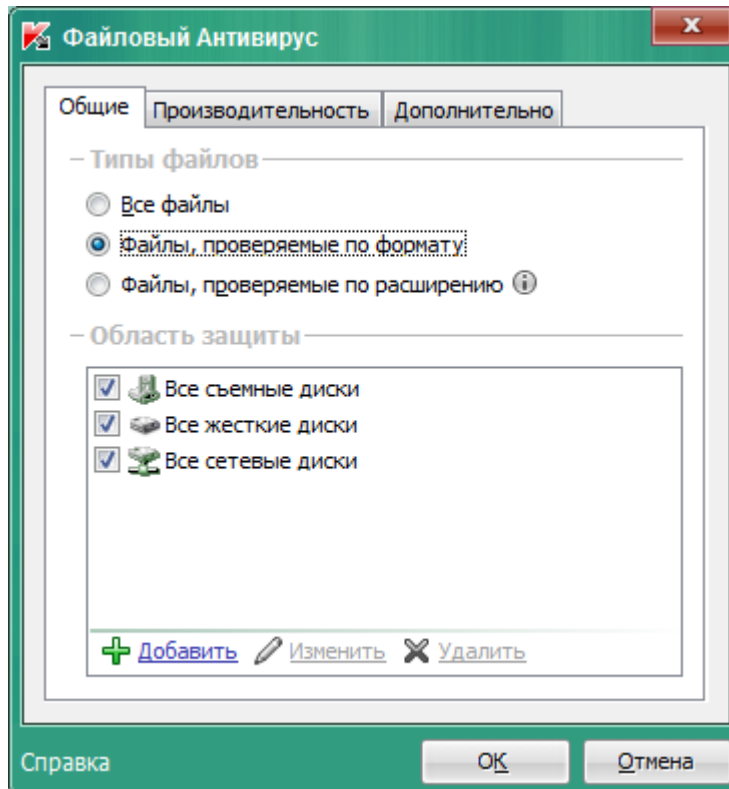


Рисунок 23 - Настройка вкладки «Общие»

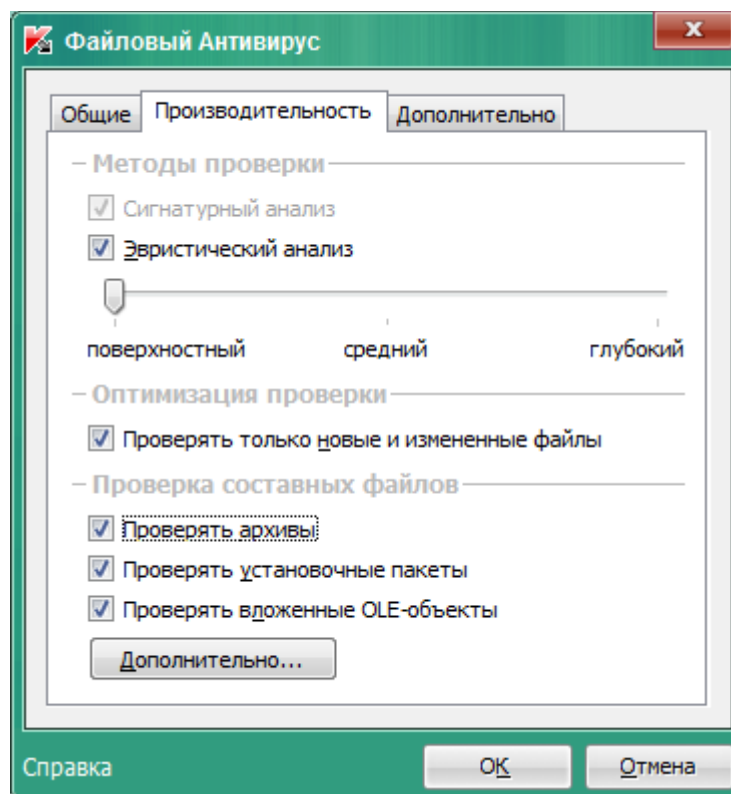


Рисунок 24 - Настройки вкладки «Производительность»

Для настройки почтового антивируса в главном окне программы выбрана вкладка «Настройка». В данном разделе выбран пункт «Почтовый антивирус». В открывшемся окне во вкладке «Общие» в пункте «Область защиты» выбран параметр «Входящие и исходящие сообщения». В пункте «Встраивание в систему» выбраны параметры «Трафик POP3 / SMTP / NNTP / IMAP» и «Дополнительно: плагин в Microsoft Office Outlook». Настройки вкладки «Общие» представлены на рисунке 25. Далее были выполнены настройки во вкладке «Дополнительно». Был включен эвристический анализ и его уровень выставлен как «Средний». Настройки во вкладке «Дополнительно» представлены на рисунке 26.

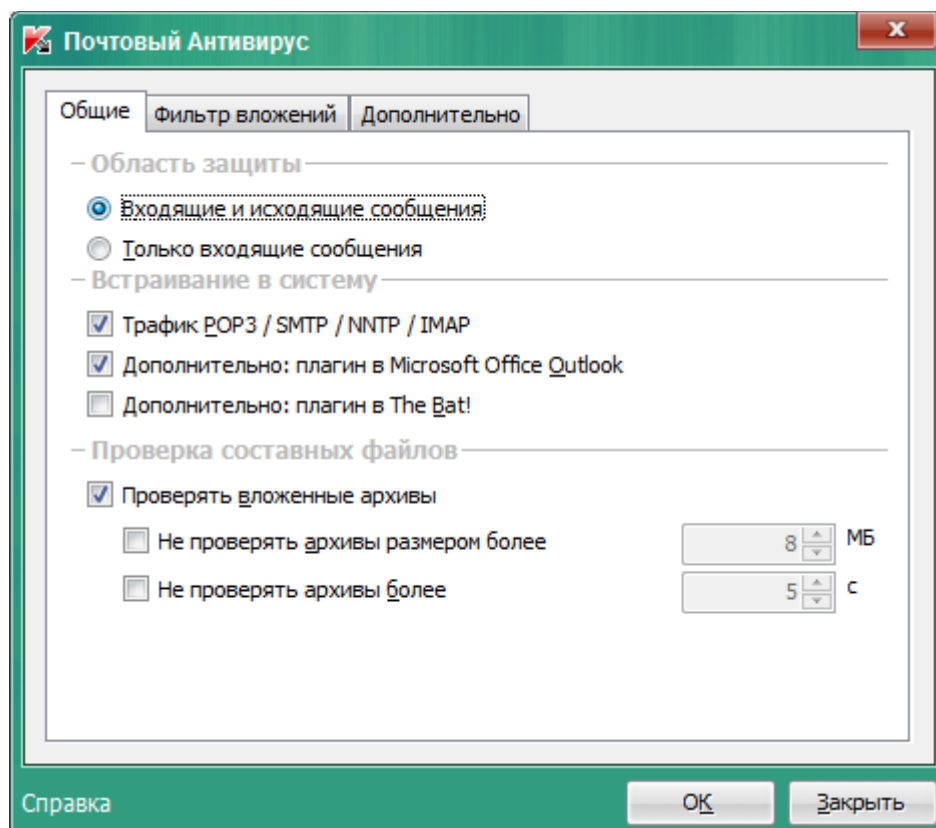


Рисунок 25 - Настройки вкладки «Общие»

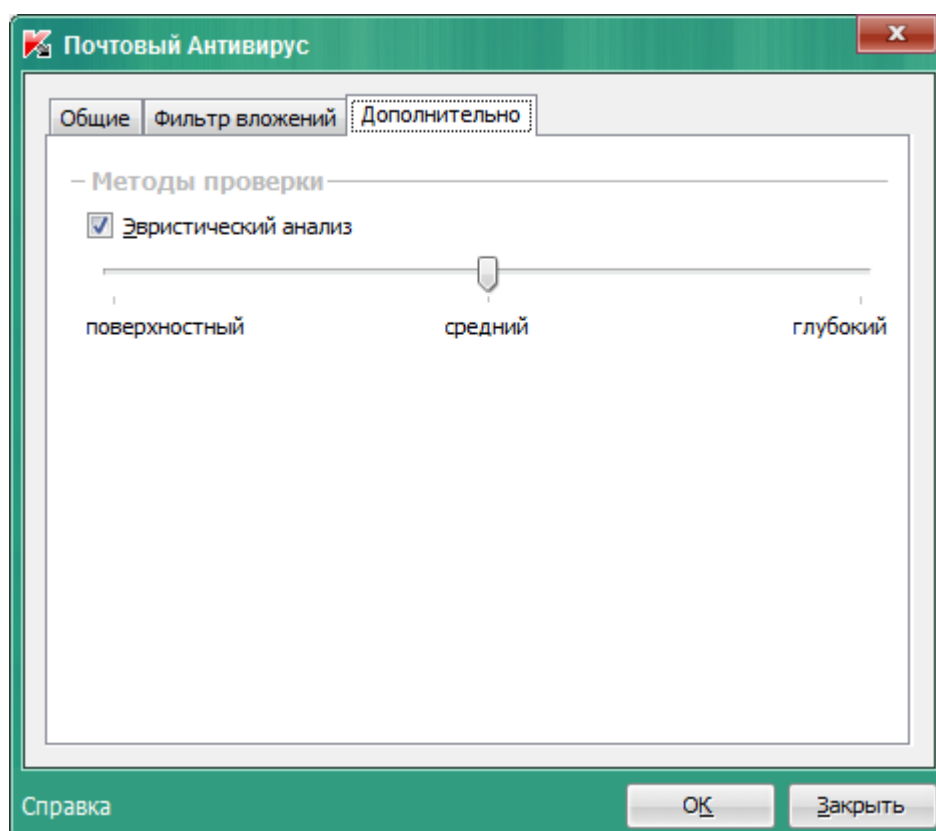


Рисунок 26 - Настройки вкладки «Дополнительно»

Для настройки веб-антивируса в главном окне программы выбрана вкладка «Настройка». В данном разделе выбран пункт «Веб-антивирус». В открывшемся окне во вкладке «Общие» в пункте «Методы проверки» выбраны параметры «Проверять ссылки по базе вредоносных веб-адресов» и «Эвристический анализ для обнаружения вирусов», уровень которого установлен как «Средний». В пункте «Параметры антифишинга» выбран параметр «Проверять ссылки по базе фишинговых веб-адресов» и «Эвристический анализ для обнаружения фишинговых ссылок», уровень которого установлен как «Средний». Также включен параметр «Ограничивать продолжительность кеширования веб-трафика». Настройки веб-антивируса представлены на рисунке 27.

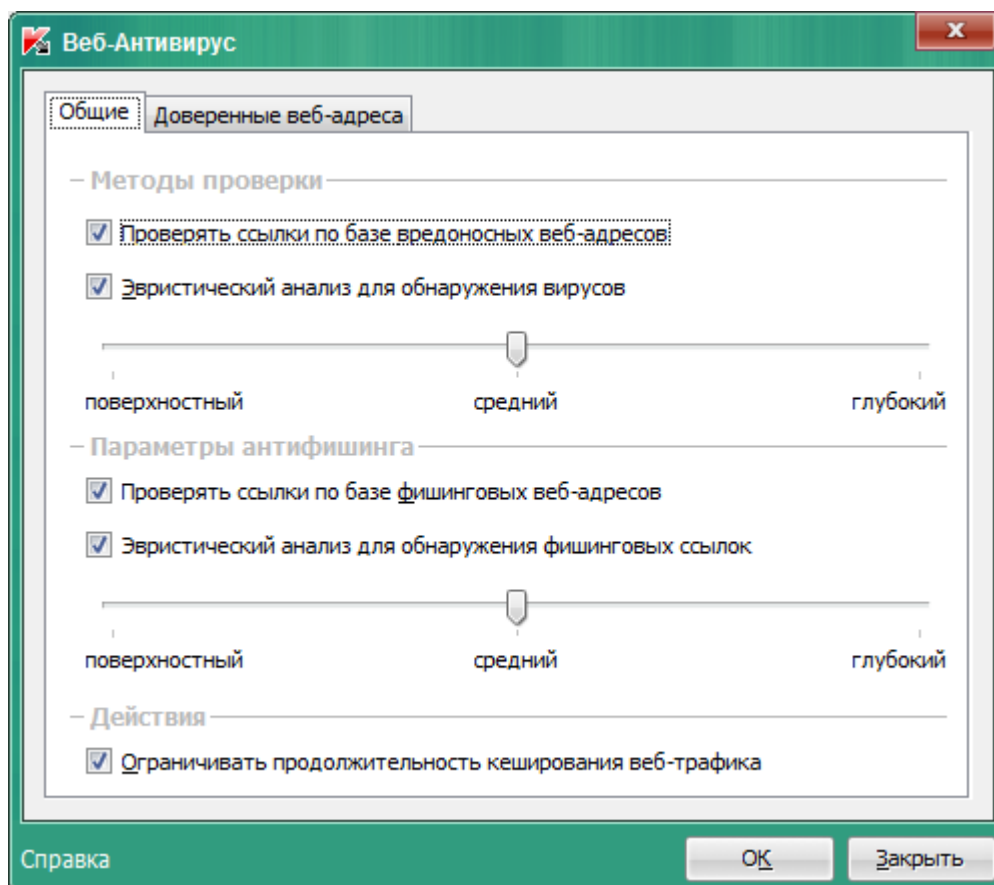


Рисунок 27 - Настройки веб-антивируса

Таким образом, настройка *Kaspersky Endpoint Security 10* выполнена для обеспечения безопасности защищаемой АС.

5 Оформление и выдача техпаспорта на аттестованную автоматизированную систему

Следующим этапом дипломного проектирования является оформление и выдача технического паспорта. Технический паспорт состоит из следующих пунктов:

- общие сведения об АС;
- состав оборудования АС;
- сведения о соответствии основных технических средств и систем (ОТСС) АС требованиям по безопасности информации;
- сведения об аттестации АС на соответствие требованиям по безопасности информации;
- учет проведения регламентных проверок;
- лист регистрации изменений;
- приложения.

Технический паспорт выполнен согласно требований нормативных документов и по стандартам предприятия, его выпускающего, и представлен в приложении А.

6 Оформление программы и методики аттестационных испытаний

Следующим этапом дипломного проектирования является оформление программы и методики аттестационных испытаний. Программа и методика аттестационных испытаний объединены в один документ, который состоит из следующих основных пунктов:

- цель аттестационных испытаний;
- условия и порядок проведения аттестационных испытаний АС;
- применяемая контрольно-измерительная аппаратура;
- проверка АС на соответствие организационно-техническим требованиям по защите информации;
- испытания АС на соответствие требованиям по защите информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН);
- испытания АС на соответствие требованиям по защите информации от НСД;
- оформление отчетной документации по результатам аттестации АС.

Программа и методика аттестационных испытаний выполнены по стандартам предприятия, его выпускающего, и представлен в приложении Б.

7 Проведение аттестационных испытаний объекта информатизации в части технической защиты от несанкционированного доступа

7.1 Для защиты автоматизированной системы необходимо ее оснащение специальными средствами защиты информации в соответствии с определенным классом защиты. Для рассматриваемой в данной работе автоматизированной системы выбран класс защищенности 1Г в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г., так как данная АС является многопользовательской, в которой одновременно обрабатывается и хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС.

7.2 Класс защищенности 1Г в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [7] предполагает требования к различным подсистемам, описанные ниже.

К подсистеме управления доступом предъявляются следующие требования:

- должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;
- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

К подсистеме регистрации и учета предъявляются следующие требования:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

- результат попытки входа: успешная или неуспешная - несанкционированная;

- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

- код или пароль, предъявленный при неуспешной попытке;

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);

- спецификация устройства выдачи (логическое имя (номер) внешнего устройства);

- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

- идентификатор субъекта доступа, запросившего документ;

- должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный - несанкционированный);
- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;
- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей.

В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта (логическое имя (номер));
- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.

Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

В подсистеме обеспечения целостности должна быть обеспечена целостность программных средств СЗИ от НСД, а также неизменность программной среды.

При этом:

- целостность СЗИ от НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;

- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

- должна осуществляться физическая охрана средств вычислительной техники (СВТ) (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

7.3 Аттестация автоматизированной системы проводится в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г. Тогда, когда создавался и принимался данный документ не было программных средств для проведения проверок. На данный момент такие программные средства существуют, и именно с помощью них решается большинство задач при аттестации автоматизированных систем в наше время. Это ускоряет процесс, увеличивает точность проверок и упрощает проведение проверки для органа по аттестации. В данной работе для проведения аттестации использованы наиболее популярные программные средства, решающие поставленную задачу. Данными программами являются:

- *Ревизор 1XP*;
- *Ревизор 2XP*;
- *ФИКС 2.0.2*;
- *Terrier 3.0*;
- *Агент инвентаризации*.

Каждая программа предназначена для выполнения своей задачи. *Ревизор 1XP* предназначен для создания модели доступа пользователей и администратора. Общий вид программы представлен на рисунке 28. *Ревизор 2XP* служит для тестирования созданной модели и сравнения заданных прав доступа с реальными. Общий вид программы представлен на рисунке 29. *Terrier 3.0* служит для проверки качества затирания удаляемой информации. Общий вид программы представлен на рисунке 30. *ФИКС 2.0.2* предназначен для снятия контрольных сумм приложений для дальнейшего их сравнения с эталонным значением или значением, полученным при предыдущей проверке. Общий вид программы представлен на рисунке 31. *Агент инвентаризации* является инструментом проверки состава комплектующих проверяемого

компьютера, а также состава установленного ПО. Общий вид программы представлен на рисунке 32.

СЗИ от НСД *Secret Net Studio* также помогает решать некоторые вопросы при проведении аттестации, так как помимо средств защиты, также обладает средствами контроля.

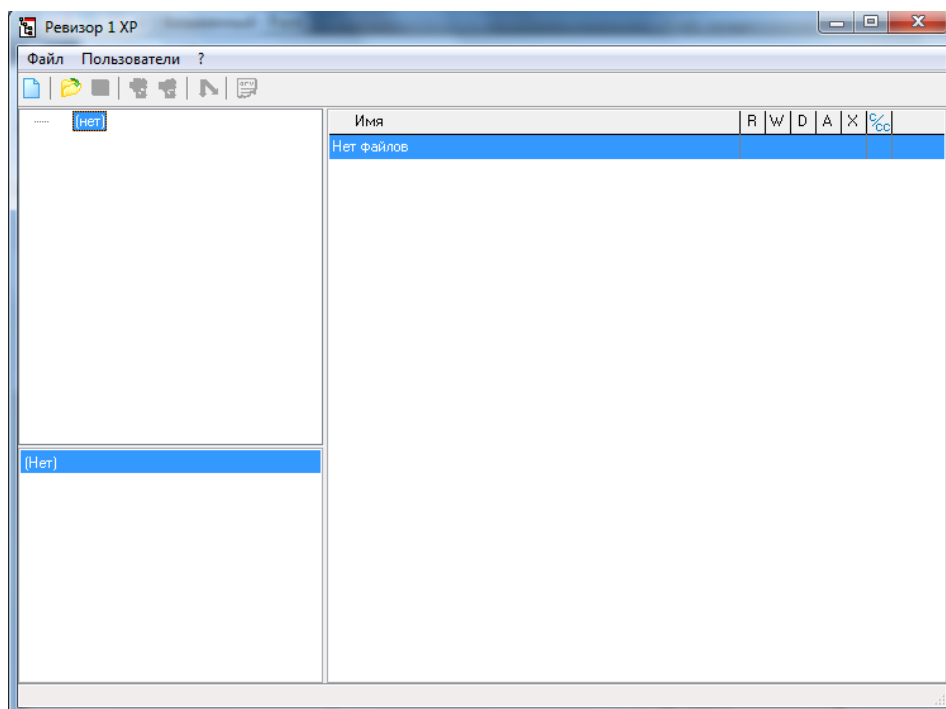


Рисунок 28 - Общий вид программы *Ревизор 1XP*

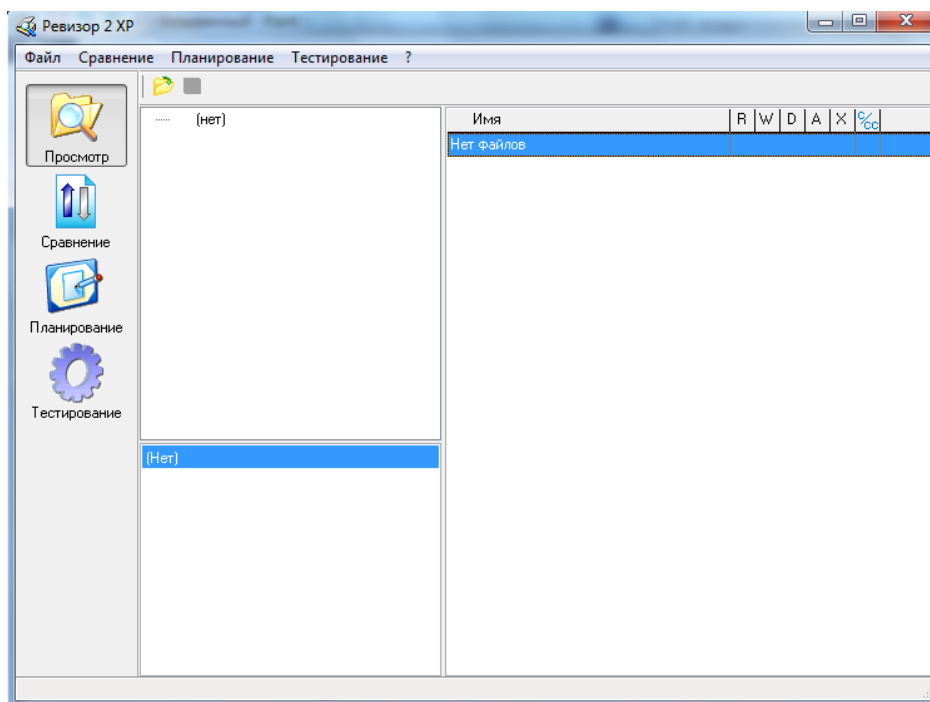


Рисунок 29 - Общий вид программы *Ревизор 2XP*

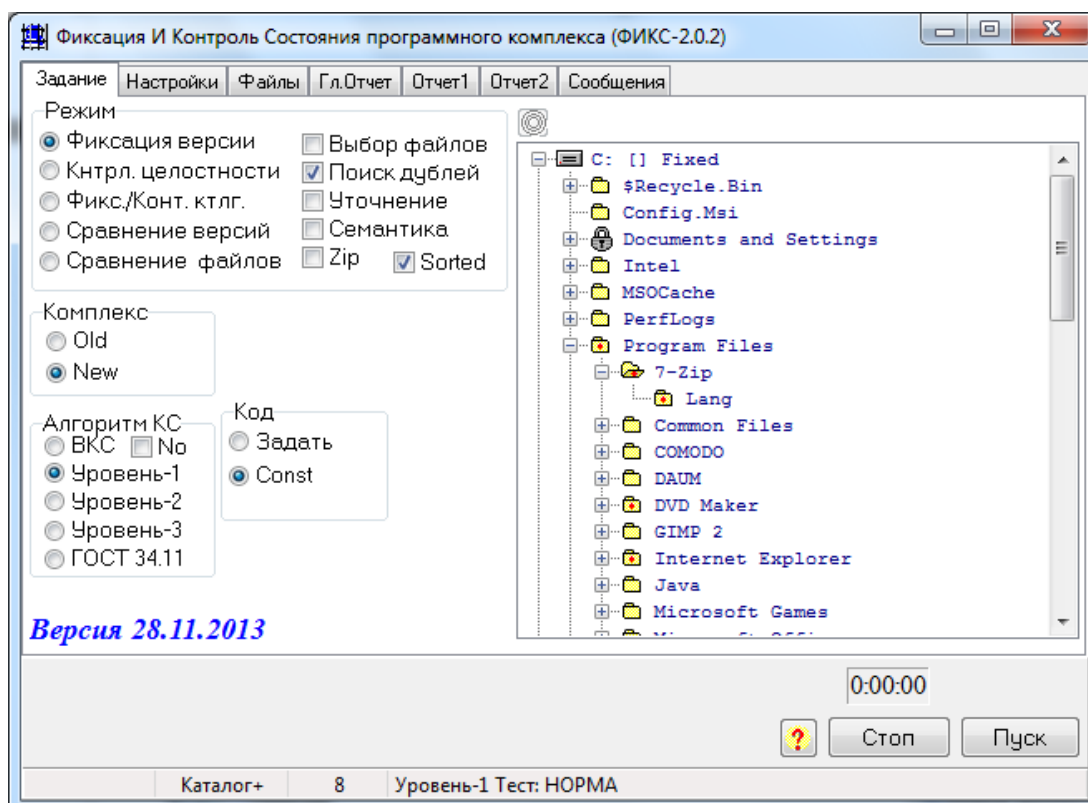


Рисунок 30 - Общий вид программы *ФИКС 2.0.2*

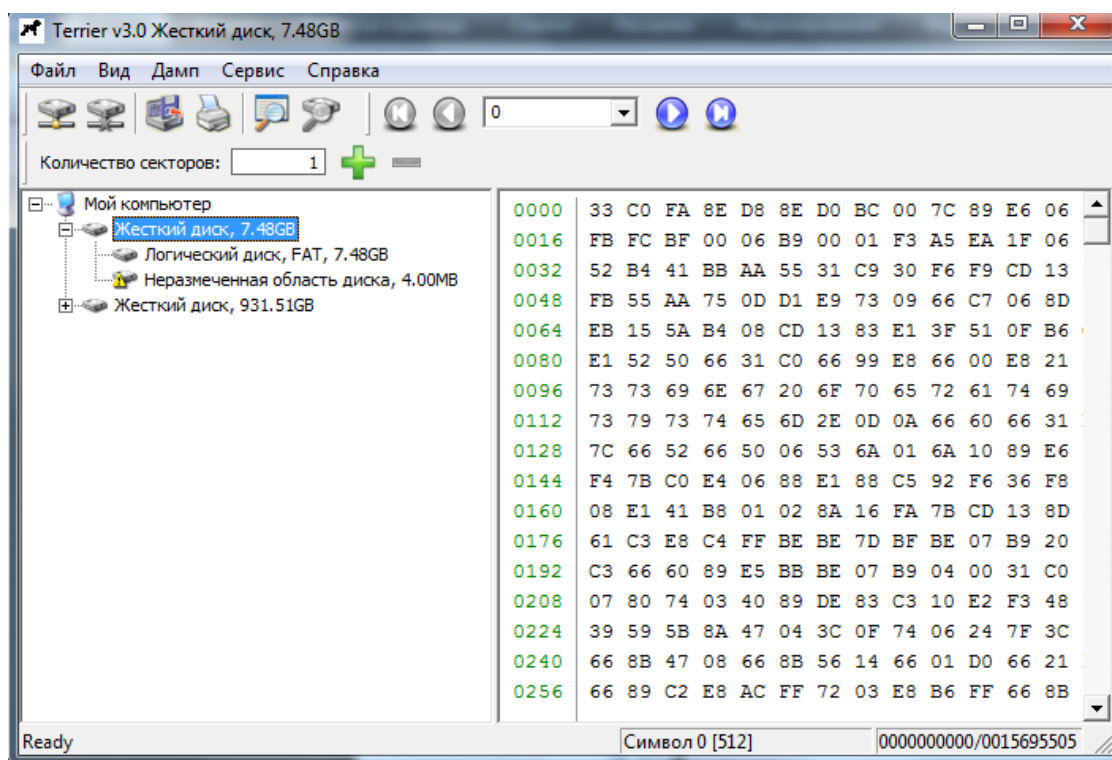


Рисунок 31 - Общий вид программы *Terrier 3.0*

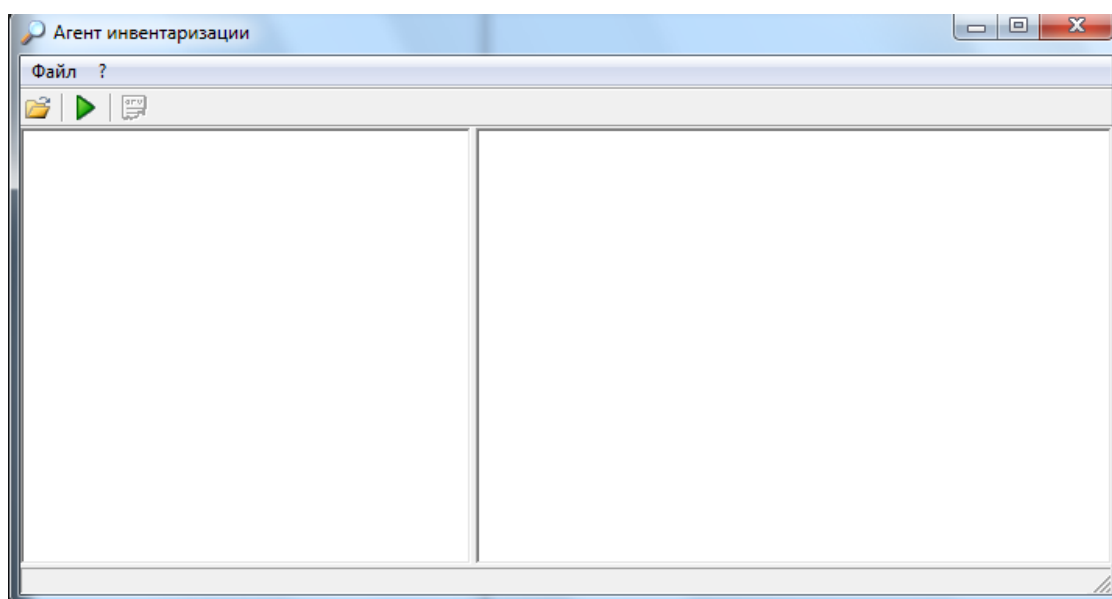


Рисунок 32 - Общий вид программы *Агент инвентаризации*

7.4 Для подсистемы управления доступом была проведена проверка идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов. Данная проверка была

проведена путем сравнения настроек СЗИ от НСД *Secret Net* с искомыми настройками. В программе «Локальная политика безопасности» была проверена минимальная длина пароля, а также просмотрены журналы доступа в систему. Сторонних пользователей в журналах доступа не обнаружено. При обращении проводится проверка принадлежности предъявленного идентификатора множеству всех зарегистрированных в АС идентификаторов. Если субъект доступа предъявляет идентификатор, не известный подсистеме идентификации, то средства управления прекращают процесс предоставления доступа.

7.5 После этого была проведена проверка доступа к ЭВМ, каналам связи, внешним устройствам ЭВМ. Для этого была использована программа *Агент инвентаризации*. Для начала анализа системы была нажата клавиша «Собрать информацию». В открывшемся диалоговом окне выбрано имя и местонахождение файла, отмечены параметры «Добавлять описание для идентификаторов классов и свойств» и «Подавлять вывод сообщений об ошибках». После сбора информации был составлен полный отчет о системе и отчет, включающий данные о ОС и ПО. Таким образом, было проверен состав автоматизированной системы на наличие неизвестных объектов доступа. Таких объектов не обнаружено.

7.6 Далее проведена проверка доступа пользователей к программам, каталогам и файлам. Данная проверка проводилась с помощью программ *Ревизор 1XP* и *Ревизор 2XP*. Для корректной работы программы *Ревизор 1XP* нужно, чтобы в программе «Локальная политика безопасности» во вкладке «Параметры Secret Net» в пункте «Полномочное управление доступом: режим работы» был выбран параметр «Контроль потоков включен». Но тогда для папок, в которых хранятся документы, представляющие собой конфиденциальную информацию, должна быть установлена метка «НС-ДСП», что означает «несекретно – для служебного пользования». Для установки

данной метки необходимо зайти в систему под администратором, выбрать определенную папку, вызвать контекстное меню, в нем выбрать раздел «Свойства» и во вкладке «Secret Net» установить категорию «НС-ДСП». Далее для того, чтобы программа *Ревизор IXP* заработала, ее нужно добавить в замкнутую программную среду, созданную средствами *Secret Net*. Для этого нужно запустить программу «Контроль программ и данных», в разделе «Структура» выбрать пункт «BUILTIN\Пользователи», далее пункт «Группа по журналу», в контекстном меню выбрать пункт «Добавить ресурсы», далее выбрать пункт одиночный и затем выбрать исполняемый файл программы *Ревизор 2XP* в список замкнутой программной среды. Далее нужно рассчитать эталоны по выбранному файлу. Для этого его нужно выбрать в списке, вызвать контекстное меню, в нем выбрать пункт «Расчет эталонов».

После подготовительного этапа настройки переходим к тестированию системы. В предполагаемые для проверки папки помещаются тестовые файлы *test.doc* и *test.exe*. Файл *test.doc* представляет собой тестовый файл, содержащий слово «test». Файл *test.exe* при запуске выдает информационное окно, что это тестовый исполняемый файл. Затем была запущена программа *Ревизор IXP*. Для начала работы была нажата клавиша «Создать проект». В открывшемся окне были выбраны логические диски, доступные пользователям, и сетевые ресурсы, а также пункты «Получить список пользователей» и «Считывать права доступа NTFS». После этого программа производит сканирование выбранных областей памяти. После этого в программе *Ревизор IXP* для выбранных пользователей необходимо установить права на чтение, запись, удаление, добавление и исполнение нужных папок или файлов. Данная программа может сама считать данные права, если они установлены средствами ОС, но если данные права установлены дискреционным доступом *Secret Net*, то в программе *Ревизор IXP* их следует установить вручную.

После этого была запущена программа *Ревизор 2XP*. После этого необходимо открыть в программе файл модели доступа, созданный программой *Ревизор 1XP*. Затем для выбранного пользователя был составлен план проверки. Для этого в программе был выбран раздел «Планирование». В открывшемся окне был отключен параметр случайной выборки. Это позволит создать план проверки доступа для выбранного пользователя вручную. Для этого необходимо вызвать окно выбора файлов и папок. Для тестирования доступа к программам достаточно выбрать исполняемый файл и какой-либо файл с расширением *dll*, находящийся в папке с предполагаемой к доступу программой. Также не нужно отмечать каждый файл по отдельности. Достаточно отметить папку, в которой хранятся файлы для определенного пользователя, так как работает принцип наследования. Для этого нужно вызвать контекстное меню на папке и отметить пункт «Выделить содержимое». После того, как план создан, он был сохранен в отдельный файл. Далее было проведено непосредственно тестирование. Для этого был выбран раздел «Тестирование». Перед началом тестирования необходимо выбрать имя и местоположение файла протокола тестирования, а также каталог для резервного копирования файлов. Также для корректной работы тестирования нужно отметить параметры «Сохранять права доступа NTFS» и «Выполнять автоматический вход в систему». После этого для начала тестирования необходимо ввести имя и пароль пользователя, для которого проводится тестирование, а также необходимо отметить параметр «С использованием службы вторичного входа в систему». Перед этим необходимо убедиться в том, что:

1) отключен запрет на вторичный вход в систему в настройках *Secret Net*. Для этого необходимо запустить программу «Локальная политика безопасности», выбрать пункт «Параметры Secret Net», в нем пункт «Настройки

подсистем» и далее параметр «Вход в систему: Запрет вторичного входа в систему» должен быть отключен;

2) отключен запрет на вторичный вход в систему в настройках Windows. Для этого необходимо запустить программу «Управление компьютером», выбрать пункт «Службы и приложения», в нем пункт «Службы» и далее открыть параметр «Вторичный вход в систему». В открывшемся окне необходимо установить параметр «Тип запуска» в положение «Вручную».

После ввода имени пользователя и пароля начнется тестирование. После проведения тестирования будут показаны результаты. Красным цветом будут выделены строки, где были найдены не совпадения в требуемых и фактических правах пользователя. После этого был сохранен отчет о проведении тестирования прав пользователя.

7.7 Для подсистемы регистрации и учета была проведена проверка входа (выхода) субъектов доступа в (из) системы. Проверка осуществлялась средствами СЗИ от НСД *Secret Net* и штатными средствами ОС. Для проверки использовались журналы *Secret Net* и журналы ОС Windows. Журналы ОС Windows регистрируют вход (выход) субъектов доступа в систему (из систем), а в журналах *Secret Net* также можно посмотреть дату и время загрузки (останова) системы, результат попытки входа, идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке.

7.8 Далее проведена проверка регистрации выдачи печатных (графических) документов на "твердую" копию. Данная проверка осуществлялась путем анализа соответствующего журнала *Secret Net*.

7.9 После этого проведена проверка запуска (завершения) программ и процессов (заданий, задач). Данная проверка осуществлялась путем анализа соответствующего журнала *Secret Net*.

7.10 Далее была проведена проверка доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи. Данная проверка осуществлялась путем анализа соответствующего журнала *Secret Net*.

7.11 Далее была проведена проверка доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам. Данная проверка не была пройдена из-за отсутствия средств регистрации данных событий.

7.12 После этого была проведена проверка учета носителей информации. Для этого был произведен визуальный осмотр всех защищаемых носителей информации и сверка нанесенной на них маркировкой с данными, внесенными в журнал учета. Также был осмотрен журнал учета на наличие записей регистрации выдачи (приема) носителей информации.

7.13 Далее была проведена проверка очистки (обнуления, обезличивания) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Для этого была запущена программа *Terrier 3.0*. Для проверки удаления информации был создан текстовый файл, содержащий информацию, которой не будет на проверяемом диске. После запуска программы нужно выбрать сканируемую область диска, где находится файл с известным контекстом. После этого в панели программы необходимо выбрать пункт «Сервис», в нем пункт «Поиск ключевых слов». В открывшемся окне в части «Активный список» была введена часть информации из созданного файла и запущен поиск. После того, как заданная информация будет найдена, файл с тестовой информацией был удален штатными средствами Windows. После этого в программе *Terrier 3.0* необходимо убедиться, что в секторе, в котором был найден известный контекст, последний больше не содержится, т.е. сектор или его часть были затерты случайной последовательностью. После этого необходимо убедиться, что искомая информация не была системно перемещена

в какой-либо сектор памяти на выбранном диске. Для этого был произведен повторный поиск на выбранном диске информации, которая была в поиске перед этим. Искомая информация не была найдена ни в найденном секторе, ни на всем диске, соответственно данный механизм работает корректно, и проверка затирания информации пройдена успешно.

7.14 Для подсистемы обеспечения целостности была проведена проверка обеспечения целостности программных средств и обрабатываемой информации. Данная проверка проводится каждый раз при загрузке СЗИ от НСД *Secret Net*. Также для проверки использовалась программа *ФИКС-2.0.2*. С использованием данной программы была снята контрольная сумма с папки *Secret Net*. Для этого вкладке «Задание» в области «Контролируемые файлы» была выбрана данная папка, алгоритмом снятия контрольной суммы был выбран «Уровень 1», так как данным алгоритмом снимается контрольная сумма с данного ПО фирмой-производителем. Затем во вкладке «Настройки» было выбрано имя и местоположение файла для сохранения контрольных сумм.

7.15 Далее была проведена проверка физической охраны средств вычислительной техники и носителей информации. Помещение размещения АС оборудовано техническими средствами охраны. Также в здании существует служба охраны и пропускной режим.

7.16 В организации назначен администратор безопасности, который в своей практической работе должен руководствоваться соответствующими нормативными документами. Администратором безопасности проводится периодическое обслуживание и тестирование функций СЗИ *Secret Net*. Порядок и периодичность проведения администратором технологических операций по обслуживанию и тестированию СЗИ и системы в целом определены в инструкциях для администратора безопасности.

7.17 Далее была проведена проверка наличия средств восстановления СЗИ НСД. В ходе проверки установлено наличие дистрибутивов используемого общего ПО и сертифицированного ПО СЗИ *Secret Net*.

7.18 Таким образом, была выполнена аттестация объекта информатизации по классу защищенности 1Г.

7.19 Обобщенный перечень требований РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [5] по классу защищенности 1Г представлены в таблице 5.

Таблица 5 - Требования РД и выполнение их в АС

№	Подсистемы и требования	Выполнение требований	
		ПЭВМ	РД (1Г)
1	2	3	4
1. Подсистема управления доступом			
1.1	Идентификация, проверка подлинности и контроль доступа субъектов: - в систему - к терминалам ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ - к программам - к томам, каталогам, файлам, записям, полям записей	 + + + +	 + + + +
2. Подсистема регистрации и учета			
2.1.	Регистрация и учет: - входа (выхода) субъектов доступа в (из) систему - выдачи печатных (графических) выходных документов - запуска (завершения) программ и процессов (заданий, задач) - доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи - доступа программ субъектов доступа к терминалам ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей - изменение полномочий субъектов доступа - создаваемых защищаемых объектов доступа	 + +— + + — + — —	 + + + + + — —
2.2.	Учет носителей информации	+—	+
2.3.	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	+	+
2.4.	Сигнализация попыток нарушения защиты	+	—
3. Подсистема обеспечения целостности			
3.1.	Обеспечение целостности программных средств и обрабатываемой информации	+	+
3.2.	Физическая охрана средств вычислительной техники и носителей информации	+	+

Продолжение таблицы 5

№	Подсистемы и требования	Выполнение требований	
		ПЭВМ	РД (1Г)
3.3.	Наличие администратора (службы) защиты информации в АС	+	—
3.4.	Периодическое тестирование СЗИ от НСД	+	+
3.5.	Наличие средств восстановления СЗИ от НСД	+	+
3.6.	Использование сертифицированных средств защиты	+	—

В графе 3 ставится:

«+», если требование выполняется;

«+—», если требование выполняется при помощи организационных мер;

«—», если требование не выполняется.

В графе 4 ставится:

«+», если требование должно выполняться;

«—», если требование не должно выполняться.

7.20 Таким образом, были проведены аттестационные испытания автоматизированной системы в части проверки требований безопасности информации.

8 Проведение аттестационных испытаний объекта информатизации в части технической защиты от утечки информации по техническим каналам

8.1 Как сказано в книге «Защита от утечки информации по техническим каналам: Учебное пособие» под техническим каналом утечки информации понимают совокупность источника информации, линии связи (физической среды), по которой распространяется информационный сигнал, шумов, препятствующих передаче сигнала в линии связи, и технических средств перехвата информации [8].

Сигналы являются материальными носителями информации. По своей природе сигналы могут быть электрическими, электромагнитными, акустическими и др. Сигналами, как правило, являются электрические, электромагнитные, акустические и другие виды колебаний (волн), причем информация содержится в изменениях их параметров [8].

К техническим средствам приема информации (ТСПИ), а также ее обработки, хранения и передачи относят технические средства, непосредственно обрабатывающие конфиденциальную информацию. В их число входят электронно-вычислительная техника, АТС для ведения секретных переговоров, системы оперативно командной и громкоговорящей связи, системы звукоусиления, звукового сопровождения и звукозаписи и т.д. [8].

Контролируемая зона – территория (либо здание, группа помещений, помещение), на которой исключено неконтролируемое пребывание лиц и транспортных средств, не имеющих постоянного или разового допуска. В контролируемой зоне посредством проведения технических и режимных мероприятий должны быть созданы условия, предотвращающие возможность утечки из нее конфиденциальной информации. Контролируемая зона определяется руководством организации, исходя из конкретной обстановки в

месте расположения объекта и возможностей использования технических средств перехвата [8].

8.2 Цель проведения работ по оценке защищенности заключалась в определении возможных расстояний распространения информативных сигналов от ОТСС и установления требуемого радиуса контролируемой зоны (КЗ) R2.

8.3 Измерению уровней побочных электромагнитных излучений подвергалась персональная электронно-вычислительная машина (ПЭВМ) в комплектации, приведенной в таблице 6.

Таблица 6 - Измерение уровней побочных электромагнитных излучений

№ п/п	Наименование ОТСС	Тип, модель	Серийный (заводской) номер
1.	Системный блок ПЭВМ в составе:	InWin	16119497356016
	- НЖМД	Seagate ST3120026A	3FN65PTF
	- DVD-ROM	Toshiba Samsung SD-M1912	68MA433632
2.	Монитор	Samsung 730BF	WM55XXXXX857629B
3.	Клавиатура	Mitsumi KFK-EA4XT	90LMFAO5CX5GMC8150*9291
4.	Манипулятор «мышь»	Logitech M-SBF90	XDB1285738
5.	Сканер	Epson J241A	FPGA979787

8.4 При проведении оценки защищенности ОТСС использовались действующие национальные стандарты по аттестации объектов информатизации.

Измерения уровней побочных электромагнитных излучений от вышеперечисленных ОТСС проводились по электрической (канал «Е») и магнитной (канал «Н») составляющим электромагнитного поля с применением следующих средств измерений:

- анализатор спектра;
- генераторы сигналов;
- осциллограф (с многофункциональным пробником);

- антенны измерительные

Все используемые средства вовремя проходят проверки и калибруются.

Оценка защищенности проводилась в следующих диапазонах частот: 9 кГц – 30 МГц (канал «Н»), 9 кГц – 1,0 ГГц (канал «Е»). Измерения составляющих электромагнитного поля проводились в дБ относительно 1 мкВ/м в полосе частот 9 кГц для диапазона 0,15 – 30 МГц и 120 кГц – для диапазона частот свыше 30 МГц. Измерительные антенны размещались на расстояниях (d) не менее двух геометрических размеров антенн от источника излучения опасного сигнала (ОС) до центра соответствующей антенны, а измерения проводились в местах обнаружения максимального сигнала с наибольшим соотношением сигнал/помеха.

В качестве тестов использовались сигналы, создаваемые специализированной программой, удовлетворяющие требованиям ГОСТ 29339-92.

8.5 Перечень ОС приведен в таблице 7.

Таблица 7 - Перечень ОС

№	Вид ОС
1.	ОС1 – сигналы видеомонитора
2.	ОС2 – сигналы записи/считывания НЖМД
3.	ОС3 – сигналы считывания DVD-ROM
4.	ОС4 – сигналы клавиатуры
5.	ОС5 – сигналы сканера
6.	ОС6 – сигналы USB-интерфейса

Возможными каналами утечки являются:

- электроакустический;
- акустический.

8.6 Результаты измерений и расчетов по оценке защищенности информации приведены в таблицах №№ 8 - 10. Сводные данные по каждому виду ОС приведены в таблице 11.

Сигналы монитора (ОС1):

1) $F_T = 54$ МГц.

2) Разрешение – 1280x1024, 60 Гц.

3) Тип кодирования – последовательное.

4) Сигнал – импульсный.

Таблица 8 - Расстояние до измерительной антенны – 1 м, канал «Е»

№	F, МГц	Uc+п, дБ	Up, дБ	Kпер, дБ	Esc, мкВ/м	Eшп, мкВ/м	R2, м
1	270	10,00	8,00	36,70	131,38	171,79	1,13
2	378	12,00	10,00	31,50	90,89	118,85	1,13
3	486	11,00	10,00	31,50	60,48	118,85	0,95
4	594	11,00	10,00	32,40	67,08	131,83	0,95
						Итог:	1,13

Сигналы НЖМД (ОС2):

1) $F_T = 25$ МГц.

2) Тип кодирования – последовательное.

3) Сигнал – импульсный.

Таблица 9 - Расстояние до измерительной антенны – 1 м, канал «Е»

№	F, МГц	Uc+п, дБ	Up, дБ	Kпер, дБ	Esc, мкВ/м	Eшп, мкВ/м	R2, м
1	125,00	12,00	8,00	18,30	25,40	20,65	0,98
						Итог:	0,98

Сигналы USB-интерфейса (ОС6):

1) $F_T = 240$ МГц.

2) Тип кодирования – последовательное.

3) Сигнал – импульсный.

Таблица 10 - Расстояние до измерительной антенны – 1 м, канал «Е»

№	F, МГц	Uc+п, дБ	Up, дБ	Kпер, дБ	Esc, мкВ/м	Eшп, мкВ/м	R2, м
1	240,00	9,00	8,00	36,70	87,42	171,79	0,73
2	720,00	12,00	8,00	28,40	81,24	66,07	0,98
						Итог:	0,98

Таблица 11 - Сводные данные по каждому виду ОС

Вид ОС	$F_{т}$, МГц	E_{0i} , дБ	pH_{0i} , дБ	$E_{шi}$, дБ	$pH_{шi}$, дБ	E_{Ci} , мкВ/м	pH_{Ci} , мкВ/м	R_i , м
ОС1	44,55	10	-	8	-	131,38	-	1,13
ОС2	25	12	-	8	-	25,4	-	0,98
ОС6	240	12	-	8	-	81,24	-	0,98

Согласно таблице 11, максимальный радиус требуемой контролируемой зоны (КЗ) для ОТСС определяется сигналами вида ОС1 и составляет 1,13 метра.

Сигналов вида ОС3 – ОС5 на фоне собственных шумов КИА и объектовой помехи не обнаружено. Минимальное расстояние от места установки ОТСС до границы КЗ составляет 12 метров.

8.7 Защищенность ОТСС от утечки конфиденциальной информации по каналу ПЭМИ обеспечивается, так как рассчитанный требуемый радиус КЗ не превышает минимального расстояния от ОТСС до границы КЗ.

Дополнительных мер по защите информации не требуется.

9 Оформление аттестационных материалов

Следующим этапом дипломного проектирования является оформление аттестационных материалов. В процессе выполнения данного этапа были оформлены следующие документы:

- Протокол испытаний комплексной системы защиты информации АС;
- Протокол оценки защищенности ОТСС из состава АС;
- Протокол оценки защищенности конфиденциальной информации от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации, имеющие выход за пределы контролируемой зоны;
- Предписание на эксплуатацию АС;
- Заключение по результатам проведения аттестационных испытаний АС;
- Аттестат соответствия требованиям безопасности информации.

Данные документы выполнены согласно нормативных документов и по стандартам предприятия, его выпускающего, и представлены в приложениях В – И.

10 Вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

10.1 Общие положения

Работа специалиста по защите информации напрямую связана с работой на компьютере. Продолжительная работа за компьютером вредит в первую очередь зрению. Эта проблема будет рассмотрена в данном разделе дипломного проекта.

10.2 Вредные факторы, влияющие на органы зрения специалиста по защите информации

Вредным производственным фактором называется такой производственный фактор, воздействие которого на работающего в определенных условиях приводит к заболеванию или снижению трудоспособности. Заболевания, возникающие под действием вредных производственных факторов, называются профессиональными [9].

К вредным производственным факторам, влияющим на органы зрения специалиста по защите информации можно отнести:

- отсутствие или недостаток естественного света;
- недостаточная искусственная освещенность рабочей зоны;
- повышенная яркость света;
- повышенная контрастность;
- прямая и отраженная блескость;
- зрительное напряжение.

Работа на компьютере сопровождается постоянным и значительным напряжением функций зрительного анализатора. Одной из основных особенностей является иной принцип чтения информации, чем при обычном чтении. При обычном чтении текст на бумаге, расположенный горизонтально на столе, считывается работником с наклоненной головой при падении светового потока на текст. При работе на ПК специалист по ИБ считывает текст, почти не наклоняя голову, глаза смотрят прямо или почти прямо вперед, текст формируется по другую сторону экрана, поэтому пользователь не считывает отраженный текст, а смотрит непосредственно на источник света, что вынуждает глаза и орган зрения в целом работать в несвойственном ему стрессовом режиме длительное время [10].

Расстройство органов зрения резко увеличивается при работе более четырех часов в день. Всемирная организация здравоохранения (ВОЗ) ввела понятие «компьютерный зрительный синдром» (КЗС), типовыми симптомами которого являются жжение в глазах, покраснение век и конъюнктивы, чувство инородного тела или песка под веками, боли в области глазниц и лба, затуманивание зрения, замедленная перефокусировка с ближних объектов на дальние [10].

Факторами, наиболее сильно влияющими на зрение, являются [11]:

1) несовершенство способов создания изображения на экране монитора. Эта группа факторов включает в себя:

- неоптимальные параметры схем развертки мониторов;
- несовместимость параметров монитора и графического адаптера;
- недостаточно высокое разрешение монитора, расфокусировка, несведение лучей и низкий уровень других его технических характеристик;
- избыточная или недостаточная яркость изображения;

2) непродуманная организация рабочего места, которая является причиной:

- наличия бликов на лицевой панели экрана;
- отсутствия необходимого уровня освещенности рабочих мест;
- несоблюдения расстояния от глаз до экрана.

Блики относятся к факторам, которые очень сильно мешают воспринимать информацию с экрана монитора. Они заставляют неосознанно напрягать зрение, чтобы прочесть нужную информацию на экране. При этом глаза испытывают дополнительное напряжение, что приводит к быстрой утомляемости органа зрения [11].

Блики создает любой пучок света, отраженный экраном дисплея и попавший на оболочку глаза. Их источниками могут быть расположенные напротив монитора яркие поверхности, светлое оборудование, осветительные приборы, незашторенные окна. Блики тем заметнее и тем сильнее снижают контрастность изображения, чем выше коэффициент зеркального отражения экрана. В ряде случаев текст может стать фактически нечитаемым [11].

В процессе работы с персональным компьютером приходится работать с изображениями на экране монитора. Считывание текста, таблиц, графиков с экрана отличается от чтения той же информации с листа бумага по нескольким причинам [11]:

- экран, являясь источником света, считается прибором активного контраста, в то время как при чтении с листа бумаги имеет дело отраженный текст, то есть с пассивным контрастом, который в малой степени зависит от интенсивности освещения и угла падения светового потока на бумагу;
- текст на бумаге является неизменным, а текст на экране периодически обновляется в процессе сканирования электронного луча по поверхности

экрана. Достаточно низкая частота обновления вызывает мерцание изображений;

- специалист по ИБ зачастую проводит весь рабочий день, работая за компьютером, что является причиной длительной неподвижности глазных и внутриглазных мышц, в то время как они нуждаются в динамическом режиме работы. Это приводит к их ослаблению;

- длительная работа с персональным компьютером требует повышенной сосредоточенности, что приводит к большим нагрузкам на зрительную систему пользователя. Развивается зрительное утомление (астенопия), которое способствует возникновению близорукости, головной боли, раздражительности, нервного напряжения и стресса.

Приведенные выше особенности изображений на экране дисплея, а также характера работы специалиста по защите информации в значительной мере влияют на степень утомляемости зрительного аппарата.

10.3 Методы и средства физической культуры, снижающие воздействие вредных психофизиологических факторов, влияющих на органы зрения

Для сохранения зрения и снижения воздействия вредных психофизиологических факторов специалисту по ИБ необходимы перерывы для снятия напряжения, в противном случае возможно развитие серьезных заболеваний. Специальная гимнастика для глаз поможет сохранить зрение.

Необходимо закрыть глаза и напрячь глазные мышцы на 4 секунды. Затем открыть глаза и расслабиться. Затем нужно посмотреть в окно вдаль около 6 секунд. Данное упражнение нужно повторить 4-5 раз.

Далее нужно перевести взгляд на переносицу и смотреть на неё примерно 4 секунды. Затем перевести взгляд на пейзаж за окном и смотреть туда около 6 секунд. Данное упражнение нужно повторить 4-5 раз.

После этого нужно посмотреть влево, при этом не поворачивая голову, зафиксировав глаза в этом положении примерно на 4 секунды. Затем нужно сделать то же самое, только смотря влево, вниз и вверх. Данное упражнение нужно повторить 3-4 раза.

Далее нужно выполнить повороты глазами в следующих направлениях: налево, вниз, направо, вверх, затем прямо вдаль в окно. Потом направо, вниз, налево, вверх, а дальше прямо вдаль в окно. Данное упражнение нужно повторить 3-4 раза.

После этого нужно моргнуть максимально быстро, отсчитав до 10, и потом закрыть глаза на несколько секунд. Затем нужно поморгать в течение минуты. Затем закрыть глаза на 2-3 секунды. После открыть их и посмотреть вдаль в окно. Повторить упражнение 2-3 раза.

Затем нужно рассмотреть любой хорошо видимый объект в течение 30 секунд. Потом перевести взгляд на самый удаленный предмет. Необходимо смотреть на него в течение 30 секунд. Потом вернуть взгляд на первый объект. Данное упражнение нужно повторить 6 раз.

После зарядки нужно дать глазам расслабиться, закрыв их. При этом не опускать голову вперед.

Выполнение подобных упражнений для глаз при работе за компьютером способствует их расслаблению и тренировке и снижает воздействие вредных психофизиологических факторов.

Заключение

В ходе выполнения выпускной квалификационной работы был произведен анализ состояния отрасли защиты конфиденциальной информации, обзор анализ и нормативной документации и публикаций по защите конфиденциальной информации и персональных данных. Далее был произведен выбор средств защиты информации путем их сравнения по требованиям приказа ФСТЭК №21 и руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г. Для сравнения СЗИ по требованиям приказа ФСТЭК №21 уровня защищенности 3 базовый набор мер был адаптирован. Затем была выполнена настройка выбранных СЗИ в соответствии с вышеуказанными требованиями. После этого были проведены аттестационные испытания автоматизированной системы в части технической защиты от несанкционированного доступа и от утечки информации по техническим каналам. Также в ходе выполнения выпускной квалификационной работы были разработаны следующие документы:

- технический паспорт АС;
- программа аттестации;
- протокол испытаний комплексной системы защиты информации АС;
- протокол оценки защищенности ОТСС из состава АС;
- протокол оценки защищенности конфиденциальной информации от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации, имеющие выход за пределы контролируемой зоны;
- предписание на эксплуатацию АС;
- аттестат соответствия требованиям безопасности информации;

– заключение по результатам проведения аттестационных испытаний АС.

Также был рассмотрен вопрос о вредных психофизиологических факторах, влияющих на органы зрения специалиста по защите информации.

Таким образом, задание на выпускную квалификационную работу выполнено в полном объеме.

Список используемых источников

1. Горбатов В. С. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации [Текст] / В. С. Горбатов, С. В. Дворянкин, А. П. Дураковский и др.; Под редакцией Ю. Н. Лаврухина. – М.: Национальный исследовательский ядерный университет «МИФИ», 2014. – 559 с.

2. Разработка системы защиты конфиденциальной информации : Организационные вопросы ЗИ : Статьи : Безопасность для всех. URL: <http://sec4all.net/modules/myarticles/article.php?storyid=188/> (дата обращения: 31.10.2017).

3. Глава 9 ПРАВОВЫЕ ОСОБЕННОСТИ ОБРАЩЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА - Тайна предприятия_ что и как защищать. URL: http://www.e-reading.club/chapter.php/64356/43/Chumarin_-_Taiina_predpriyatiya__cto_i_kak_zashchishchat%27.html/ (дата обращения: 31.10.2017).

4. Коммерческая ценность информации. URL: <https://lektsii.org/6-79482.html> (дата обращения: 31.10.2017).

5. Меры по охране конфиденциальности информации. URL: <https://lektsii.org/6-79483.html/> (дата обращения: 31.10.2017).

6. Приказ ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 №21 // ФСТЭК России. с изм. и допол. в ред. от 23.03.2017.

7. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация

автоматизированных систем и требования по защите информации. Утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. // Федеральная служба по техническому и экспертному контролю. – 30.03.1992. - Ст. 15.

8. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебное пособие [Текст] / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев – М.: Горячая линия – Телеком, 2005. – 416 с.

9. Опасные и вредные производственные факторы, общие понятия. URL: <http://storage.mstuca.ru/bitstream/123456789/1523/1/Лекции%20по%20дисциплине.pdf/> (дата обращения: 17.01.2018).

10. Вредные и опасные факторы при работе с компьютером. URL: <http://www.grandars.ru/shkola/bezopasnost-zhiznedeyatelnosti/vrednye-factory-pri-rabote-na-pk.html/> (дата обращения: 17.01.2018).

Приложение А

(обязательное)

Технический паспорт

Экз. № 1

УТВЕРЖДАЮ

Генеральный директор

11 ноября 2017 г.

ТЕХНИЧЕСКИЙ ПАСПОРТ

на автоматизированную систему на базе автономной ПЭВМ
(сер. №), расположенную в помещении № 3

Разработал:

2017

83

1. ОБЩИЕ СВЕДЕНИЯ ОБ АС

1.1. АС на базе автономной ПЭВМ (сер. №).

1.2. Расположение объекта: г. Пенза.

1.3. Режим входа в здание – охраняемый.

1.4. Класс защищенности 1Г для АС.

1.5. Акт ввода объекта в эксплуатацию №....

2. СОСТАВ ОБОРУДОВАНИЯ АС

2.1. Состав основных технических средств и систем (ОТСС) АС:

№ п/п	Наименование ОТСС	Тип, модель	Серийный (заводской) номер
1.	Системный блок ПЭВМ в составе:	InWin	16119497356016
	- НЖМД	Seagate ST3120026A	3FN65PTF
	- DVD-ROM	Toshiba Samsung SD-M1912	68MA433632
2.	Монитор	Samsung 730BF	WM55XXXXX857629B
3.	Клавиатура	Mitsumi KFK-EA4XT	90LMFAO5CX5GMC8150*9291
4.	Манипулятор «мышь»	Logitech M-SBF90	XDB1285738
5.	Сканер	Epson J241A	FPDA979787

2.2. Состав вспомогательных технических средств и систем (ВТСС) АС:

№ п/п	Наименование ВТСС	Тип, модель	Серийный (заводской) номер
1.	Телефонный аппарат	Atlinks FS29169GE2-C	29911734
2.	Датчик пожарной сигнализации (2 шт.)	-	б/н

2.3. Размещение ОТСС относительно границ контролируемой зоны (КЗ) АС:

- минимальный размер КЗ составляет 12 метров;

2.4. План размещения ОТСС, ВТСС, а также схема прокладки линий и инженерных коммуникаций приведен в Приложении 1.

2.5. План размещения АС относительно границ КЗ приведен в Приложении 2.

2.6. Инженерные коммуникации, к которым относится система теплоснабжения здания, в том числе помещение размещения АС, имеют выход за пределы КЗ.

2.7. Электропитание ОТСС АС осуществляется от понижающей трансформаторной подстанции, расположенной за пределами КЗ.

2.8. Заземление ОТСС АС осуществляется на контур заземления, расположенный в пределах КЗ.

2.9. Телефонная линия, заведенная в помещение № 39, имеет выход за пределы КЗ.

2.10. Линия пожарной сигнализации не имеет выход за пределы КЗ.

2.11. Аттестуемая АС подключена к учрежденческой ЛВС через межсетевой экран к серверному и коммутационному оборудованию и далее к каналу связи Internet, при этом магистраль канала связи с Internet выполнена оптоволоконным кабелем.

2.12. Перечень средств защиты информации:

№ п/п	Наименование СЗИ	Заводской номер	Номер знака соответствия	Сведения о сертификате	Место и дата установки
1.	Secret Net Studio 8.0	KLTRCP7	М 673056	сертификат ФСТЭК России № 3675 от 12.12.2016 г., действителен до 12.12.2019 г.	ПЭВМ, сер. № 11458720921807, 01.11.2017
2.	Kaspersky Endpoint Security 10 для Windows	СМП8877-2387	Л 729365	сертификат ФСТЭК России № 3025 от 25.11.2013 г., действителен до 25.11.2019 г.	ПЭВМ, сер. № 23678912459490, 01.11.2017

2.13. Состав программного обеспечения:

№ п/п	Наименование ПО
1.	ОС Microsoft Windows 7 Профессиональная SP1 x32, лиц. №
2.	Пакет офисных приложений Microsoft Office 2010, лиц. № в составе: Word, Excel
3.	Почтовая программа Mozilla Thunderbird 52.2.0, свободно-распространяемое ПО
4.	Программа чтения файлов в формате pdf Foxit Reader 7.3.6.321, свободно-распространяемое ПО
5.	Программа работы со сканером Epson Scan, свободно-распространяемое ПО
6.	СКЗИ КриптоПро CSP 3.9, лиц. №
7.	Антивирусная программа Касперского 10 (Kaspersky Endpoint Security 10 для Windows), лицензия
8.	СЗИ от НСД «Secret Net Studio 8.0» (редакция: Постоянная защита), лиц. №

**3. СВЕДЕНИЯ О СООТВЕТСТВИИ ОТСС АС
ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

**4. СВЕДЕНИЯ ОБ АТТЕСТАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ НА
СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ:**

Номер и дата регистрации аттестата соответствия	Номер и дата регистрации заключения по результатам аттестационных испытаний	Номера и дата регистрации протоколов по результатам аттестационных испытаний

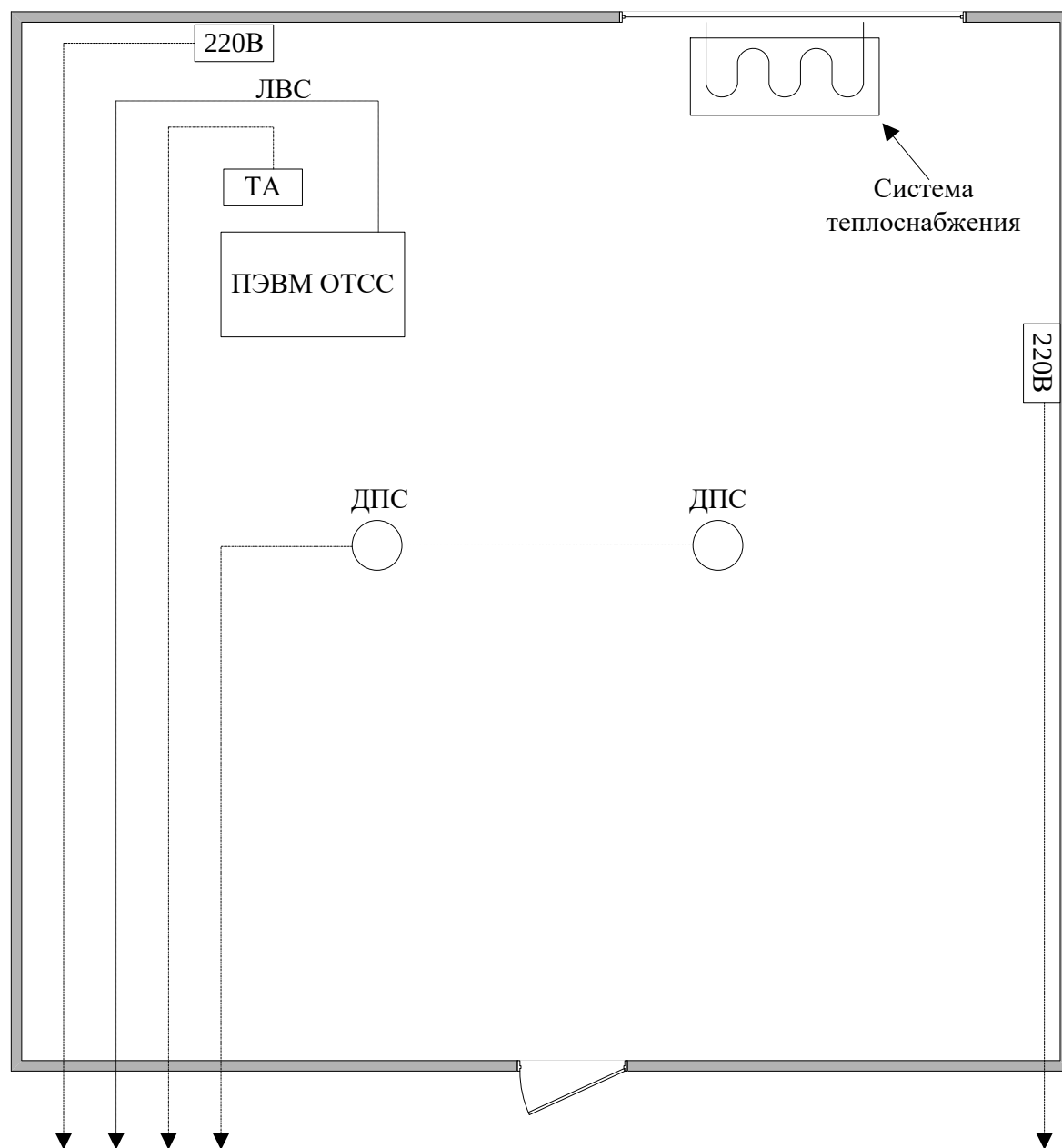
5. УЧЁТ ПРОВЕДЕНИЯ РЕГЛАМЕНТНЫХ ПРОВЕРОК

№ п/п	Наименование организации, проводившей проверку	Дата проведения проверки	Номер протокола	Примечание
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

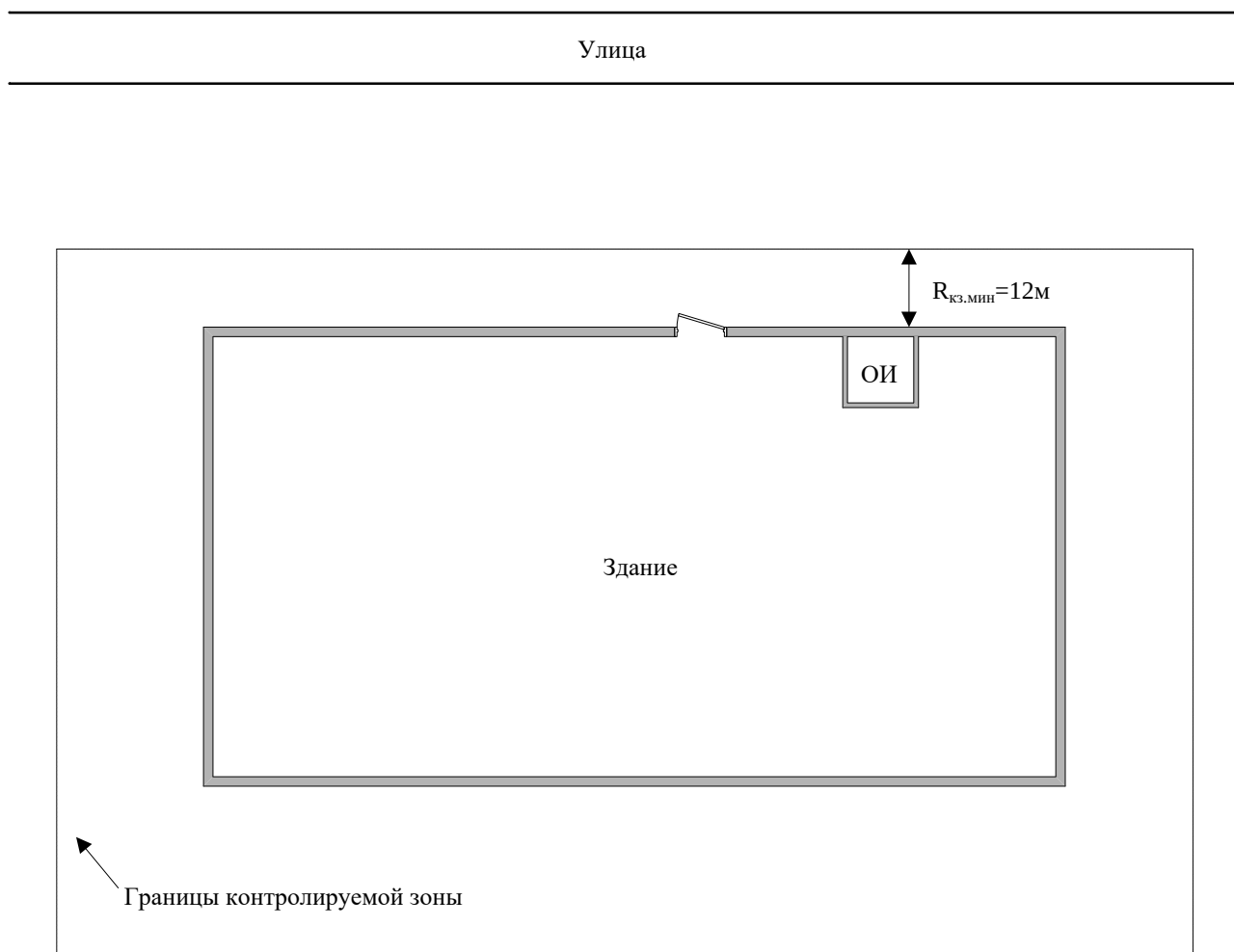
6. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Порядковый номер и дата введения изменений	Наименование документа, фиксирующего изменения	Номера заменённых (исправленных) листов документа	Подпись лица, внесшего изменения
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

ПЛАН размещения ОТСС, ВТСС и СЗИ в помещении № 3



ПЛАН
размещения АС относительно границ КЗ



Приложение Б

(обязательное)

Программа и методика аттестационных испытаний

ПРОГРАММА И МЕТОДИКИ

проведения аттестационных испытаний автоматизированной системы на базе автономной ПЭВМ, расположенной в помещении, на соответствие требованиям по безопасности информации

2017

Содержание

Принятые сокращения

1. Общие положения
2. Цель аттестационных испытаний АС
3. Основание для проведения аттестационных испытаний АС
4. Описание АС
5. Условия и порядок проведения аттестационных испытаний АС
6. Состав аттестационной комиссии
7. Применяемая контрольно-измерительная аппаратура (КИА)
8. Анализ технологического процесса автоматизированной обработки информации на АС
9. Проверка АС на соответствие организационно-техническим требованиям по защите информации
10. Испытания АС на соответствие требованиям по защите информации от утечки по каналам ПЭМИН
11. Испытания АС на соответствие требованиям по защите информации от НСД
12. Оформление отчетной документации по результатам аттестации АС
13. Приложение

Принятые сокращения

АС	– автоматизированная система
ОТСС	– основные технические средства и системы
ВТСС	– вспомогательные технические средства и системы
СИ	– специальные исследования
КЗ	– контролируемая зона
НСД	– несанкционированный доступ
ПЭМИН	– побочные электромагнитные излучения и наводки
РД	– руководящий документ
СВТ	– средства вычислительной техники
СЗИ	– средства (система) защиты информации

1. Общие положения

Настоящая программа определяет условия и порядок проведения аттестационных испытаний АС на базе автономной ПЭВМ (сер. № 16119497356016) на соответствие требованиям по безопасности конфиденциальной информации, а также информации, содержащей персональные данные.

Аттестационные испытания АС проводятся на основании требований следующих документов:

- Закон «О коммерческой тайне» № 98-ФЗ от 29.07.04 г.;
- Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27 июля 2006 г.

Объем аттестационных испытаний вышеуказанных АС определен следующим перечнем работ:

- анализ внутренней и распорядительной документации по защите информации на АС, технологического процесса обработки конфиденциальной информации (персональных данных) и анализ информационных потоков;
- проведение оценки защищенности АС и отдельных ее компонентов в условиях эксплуатации;
- проверка состояния организации работ и выполнения организационно-технических требований по защите информации, оценка правильности классификации АС;
- оценка полноты и уровня разработки организационно-распорядительной, проектной и эксплуатационной документации;
- оценка уровня подготовки кадров и распределения ответственности за выполнением требований по защите информации;
- испытания отдельных технических и программных средств АС, средств и систем защиты информации на соответствие требованиям защиты информации по утвержденным и согласованным с ФСТЭК (Гостехкомиссией) России методикам испытаний;
- комплексные испытания АС на соответствие требованиям по защите информации;
- подготовка отчетной документации - протоколов испытаний, заключения по результатам аттестационных испытаний АС и «Аттестата соответствия...».

2. Цель аттестационных испытаний АС

Целью аттестационных испытаний АС является оценка защищенности

конфиденциальной информации и персональных данных, обрабатываемых ОТСС данной системы, от ее утечки по техническим каналам в соответствии с действующими в стране нормативно-методическими документами.

3. Основание для проведения аттестационных испытаний АС

При проведении аттестационных испытаний АС необходимо руководствоваться требованиями национальных стандартов по аттестации объектов информатизации для обеспечения выполнения требований по классу защищенности 1Г для автоматизированных систем и уровню защищенности УЗЗ для информационных систем персональных данных.

4. Описание АС

Аттестуемая АС предназначена для обработки конфиденциальной информации и персональных данных, которые могут храниться на ЖМД и сменных МНИ и предназначены для работы в многопользовательском режиме. АС размещена в помещении.

Состав технических средств (ОТСС, ВТСС), установленных в помещении размещения АС приведен в приложении настоящей Программы.

5. Условия и порядок проведения аттестационных испытаний АС

5.1. Аттестационные испытания АС проводятся в эксплуатационных режимах работы ОТСС с использованием тестирующих технических и программных средств.

5.2. Для проведения испытаний АС аттестационной комиссии представляются следующие исходные данные и документация:

- технический паспорт на АС;
- акт классификации АС;
- перечень защищаемых на АС ресурсов;
- разрешительная система доступа персонала к защищаемым ресурсам АС;
- описание технологического процесса обработки информации на АС;
- инструкция пользователю АС;
- протоколы специальных исследований ОТСС из состава АС;
- предписания на эксплуатацию ОТСС из состава АС;
- план размещения АС относительно границ КЗ;
- паспорт (руководство по эксплуатации) СЗИ;
- сертификаты соответствия требованиям безопасности информации на используемые СЗИ;
- сведения по уровню подготовки кадров, обеспечивающих защиту информации на АС.

5.3. Объем аттестационных испытаний АС определяется следующим перечнем работ:

- анализ технологического процесса автоматизированной обработки информации на АС;
- проверка АС на соответствие организационно-техническим требованиям по защите информации;
- испытания АС на соответствие требованиям по защите информации от утечки по каналам ПЭМИН;
- испытания АС на соответствие требованиям по защите информации от НСД;
- оформление отчетных документов (протоколы испытаний, заключение по результатам испытаний и «Аттестат соответствия...»).

6. Состав аттестационной комиссии

Приказом № 33 от 10.01.2018г. назначена и действует аттестационная комиссия, состав которой представлен в таблице 1.

Таблица 1

№ п/п	ФИО	Должность	Выполняемые работы

7. Применяемая контрольно-измерительная аппаратура (КИА)

7.1. Перечень КИА и вспомогательного оборудования, используемых при проведении аттестационных испытаний, приведён в таблице 2.

Таблица 2

№ п/п	Наименование	Тип, модель	Серийный номер	Дата поверки
1.	Селективный микровольтметр			
2.	Селективный микровольтметр			
3.	Генератор сигналов			
4.	Генератор сигналов			
5.	Осциллограф (с многофункциональным пробником)			
6.	Антенна измерительная			
7.	Антенна измерительная			

8. Анализ технологического процесса автоматизированной обработки информации на АС

При изучении технологического процесса автоматизированной обработки и хранения информации анализу подвергаются такие компоненты АС как объекты и субъекты доступа, средства обработки и передачи информации:

- к объектам доступа относятся средства обработки и передачи информации, информационные носители на магнитной и бумажной основе, накопители и все виды памяти ПЭВМ, в которых может находиться информация, отдельные документы и их архивы, используемые в технологическом процессе автоматизированной обработки информации, файлы, записи и другие единицы информационных ресурсов, доступ к которым необходимо регламентировать;
- к субъектам доступа относятся персонал и все лица, которые имеют возможность доступа к средствам обработки информации, а также программные средства, посредством которых осуществляется доступ к объектам;
- к средствам обработки и передачи информации относятся технические и программные средства, средства и линии связи, предоставляющие возможности как для перемещения (копирования) информации между различными областями памяти и информационными носителями, различными средствами обработки, определенными для АС, так и по выводу информации из установленной для нее сферы обращения.

Используя исходные данные по технологии обработки информации и разрешительной

системы доступа персонала к защищаемым ресурсам, анализируется обобщенная технологическая схема АС с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой информации.

Проверяется соответствие описания технологического процесса обработки, хранения и передачи конфиденциальной информации реальной практике.

Проверяются паспортные (исходные) данные на АС и устанавливаются опасные факторы и угрозы, критические места, снижающие уровень защиты, комплектность и характеристики средств защиты.

Проверяется наличие оформленных разрешений на допуск персонала к конфиденциальной информации, метки на информационных носителях, соответствие технологических инструкций пользователей и администратора безопасности информации установленным требованиям.

По результатам изучения уточняется схема технологического процесса с привязкой к конкретным средствам обработки и передачи информации и штатному персоналу.

9. Проверка АС на соответствие организационно-техническим требованиям по защите информации

9.1. Проверка проводится в объеме, указанном в таблице 3.

Таблица 3

Наименование проверок и испытаний	Пункт методических рекомендаций
Проверка достаточности представленных документов на АС и соответствия их содержания требованиям по безопасности информации	9.2
Проверка соответствия состава и структуры программно-технических средств АС представленной документации	9.3
Проверка правильности классификации АС	9.4
Проверка уровня подготовки кадров и распределения ответственности персонала	9.5
Проверка наличия сертификатов соответствия на средства защиты информации	9.6
Проверка выполнения требований к помещениям, в которых производится обработка информации на ОТСС	9.7

9.2. Проводится проверка достаточности представленных документов и соответствия их содержания требованиям стандартов и РД по безопасности информации ФСТЭК (Гостехкомиссии) России и других органов государственного управления в пределах компетенции.

9.3. Состав и структура программно-технических средств, включенных в реальный технологический процесс обработки информации, сверяется с представленной документацией.

9.4. Проверка правильности классификации АС производится в соответствии с требованиями РД Гостехкомиссии России «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» и требованиями приказа ФСТЭК России №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» на основании следующих определяющих признаков:

- уровней полномочий по доступу к конфиденциальной информации различных пользователей;
- режимов обработки данных на АС - многопользовательский или однопользовательский.

Требуемый класс и уровень АС сравниваются с установленными на АС.

9.5. Проверка уровня подготовки кадров и распределения ответственности производится на основе следующих показателей:

- экспертной оценки знаний инструкций по безопасности информации пользователями и эксплуатационным персоналом;
- наличия разрешительной системы доступа персонала к защищаемым ресурсам, определяющей полномочия по доступу к конфиденциальной информации и процедуры их оформления, системы распределения ответственности персонала за выполнение требований по безопасности информации, оформленной приказами и распоряжениями руководителя предприятия;
- экспертной оценки проводимой технической учебы и повышения квалификации персонала и пользователей АС.

Путем опроса персонала проверяется доведение до конкретных исполнителей руководящих документов, технологических инструкций, предписаний, актов, заключений и уровень овладения персоналом технологией безопасной обработки информации, описанной в этих инструкциях.

9.6. Производится проверка наличия документов (сертификатов соответствия), подтверждающих возможность применения технических и программных средств защиты для обработки конфиденциальной информации.

9.7. Производится проверка выполнения требований руководящих документов по условиям размещения ОТСС в рабочих помещениях, которые исключали бы возможность несанкционированного просмотра информации с экранов мониторов, с распечаток принтеров и с других устройств ввода-вывода информации лицами, не имеющими права доступа к обрабатываемой информации.

9.8. По результатам проверки аттестационная комиссия должна сделать выводы о соответствии (или несоответствии) предъявленных документов и исходных данных установленным требованиям по безопасности информации.

10. Испытания АС на соответствие требованиям по защите информации от утечки по каналам ПЭМИН

10.1. Специальные исследования ОТСС из состава АС.

10.1.1. Проверка выполнения требований по защите информации, обрабатываемой ОТСС, от утечки за счет ПЭМИ в составе АС проводится в объеме, указанном в таблице 4.

Таблица 4

Наименование проверок и испытаний	Пункт методических рекомендаций
Проверка соответствия фактических размеров КЗ представленным документам.	10.1.2
Проверка соответствия размеров КЗ требованиям предписаний на эксплуатацию ОТСС и других документов, определяющих требования к размеру зоны R2.	10.1.3
Проверка работоспособности средств защиты информации и выполнения правил их эксплуатации.	10.1.4
Экспертная оценка результатов инструментальной оценки защищенности ОТСС.	10.1.5
Инструментальная оценка эффективности применяемой системы защиты информации от утечки по каналам ПЭМИ.	10.1.6

10.1.2. Проводится проверка соответствия размеров КЗ в представленных документах (планы размещения ОТСС, акты обследования и др.) фактическим размерам КЗ. Определяются минимальные значения расстояний от источников информативных сигналов до границы КЗ.

10.1.3. Сравниваются требуемые значения расстояний до границы КЗ, указанные в предписаниях на эксплуатацию ОТСС (радиусы зоны R2), с фактическими значениями этих расстояний. Значения R2 должны быть меньше расстояний от ОТСС до границ КЗ. В противном случае должны применяться дополнительные меры и средства защиты.

10.1.4. Проверка средств защиты информации производится по следующим показателям:

- соответствие применяемых средств защиты тем, что указаны в предписаниях на эксплуатацию ОТСС (средства активного зашумления, экранирующие конструкции, сетевые помехоподавляющие фильтры и т.д.);
- наличие сертификатов соответствия на применяемые средства защиты;
- наличие актов установки средств защиты информации и выполнение правил их эксплуатации.

10.1.5. Производится экспертная оценка эффективности применяемой защиты информации, обрабатываемой ОТСС, по следующим признакам:

- использованные методики контроля;
- использованные тестовые средства;
- применяемая контрольно-измерительная аппаратура;
- полнота проведенных измерений по объему и видам измерений (частотный спектр, режимы работы ОТСС, измеренные составляющие электромагнитного поля, направления распространения информативных сигналов в пространстве);
- достоверность результатов измерений.

10.1.6. Инструментальная оценка эффективности применяемой системы защиты информации от утечки по каналам ПЭМИ производится для ОТСС в соответствии с действующими нормами защиты информации по методикам специальных исследований, утвержденных (согласованных) ФСТЭК (Гостехкомиссией) России.

10.2. Проверка выполнения требований по защите информации от утечки за счет наводок по цепям электропитания и заземления ОТСС.

10.2.1. Проверка проводится в объеме, указанном в таблице 5.

Таблица 5

Наименование проверок и испытаний	Пункт методических рекомендаций
Проверка выполнения требований к схеме организации электропитания ОТСС, монтажу питающих кабелей, фильтрации опасных сигналов в цепях электропитания.	10.2.2
Проверка выполнения требований к системе заземления ОТСС.	10.2.3
Проверка работоспособности СЗИ, применяемых на объекте применения ОТСС, выполнения правил их эксплуатации.	10.2.4
Инструментальная оценка эффективности применяемой системы защиты информации от утечки по цепям заземления и электропитания ОТСС.	10.2.5

10.2.2. Проверка выполнения требований к схеме организации электропитания ОТСС проводится в части:

- размещения понижающей трансформаторной подстанции;
- монтажа фидерных линий, их экранированию и фильтрации.

10.2.3. Проверка выполнения требований к системе заземления ОТСС проводится в части:

- места размещения контура заземления относительно границ КЗ;
- величине сопротивления току растекания заземлителей при наличии

протокола измерения;

- отсутствию соединений системы заземления с металлоконструкциями, выходящими за пределы КЗ.

10.2.4. Проводится проверка работоспособности применяемых на объекте пассивных и активных средств защиты и правильности их эксплуатации.

10.2.5. Проводится инструментальная оценка защищенности информации, обрабатываемой ОТСС, от утечки по цепям заземления и электропитания в соответствии с методиками, утвержденными (согласованными) ФСТЭК (Гостехкомиссией) России.

10.3. Комплексные испытания АС на соответствие требованиям по защите информации от утечки за счет ПЭМИН.

Комплексные испытания АС проводятся в рабочих эксплуатационных режимах технических средств и средств защиты информации. При этом оценивается работоспособность средств защиты информации, включая средства их контроля и сигнализации, а также их электромагнитная совместимость со средствами обработки информации.

В процессе испытаний (по выбору комиссии) могут моделироваться нештатные ситуации, связанные с выходом из строя средств защиты и т.п.

10.4. Рекомендации по результатам аттестационных испытаний.

По результатам аттестационных испытаний должны быть сделаны выводы о соответствии (или несоответствии) АС требуемому уровню защиты информации от утечки за счет ПЭМИН.

Комиссия может рекомендовать следующие меры по устранению недостатков:

- применение дополнительных организационных и технических мер по защите информации;
- применение дополнительных сертифицированных средств защиты информации;
- исключение отдельных ОТСС из состава АС.

11. Испытания АС на соответствие требованиям по защите информации от НСД

Испытания АС на соответствие требованиям по защите информации от НСД проводятся в объеме, указанном в таблице 6.

Таблица 6

Наименование проверок и испытаний	Пункт методики испытаний
Анализ и оценка техпроцесса обработки информации АС	11.1
Выбор инструментальных средств и методики испытаний	11.2
Испытания подсистемы управления доступом	
Проверка механизма идентификации	
Проверка механизма аутентификации	
Проверка механизма контроля доступа	
Проверка механизмов управления потоками информации	
Испытания подсистемы обеспечения целостности	11.3
Испытания подсистемы регистрации и учета	11.4
Проверка механизма уничтожения информации	11.5
Проверка состава и работоспособности технических и программных средств	11.6
Контроль изменений в АС	11.7

Объем испытаний на соответствие требованиям по ЗИ от НСД может уточняться в зависимости от установленного класса АС.

11.1. Анализ и оценка технологического процесса обработки информации в части

НСД.

11.1.1. Комиссии представляется описание технологического процесса обработки информации аттестуемой АС, включающее в себя:

- перечень объектов доступа;
- перечень субъектов доступа;
- перечень штатных средств доступа к информации на АС;
- перечень средств защиты информации;
- описание реализованных правил разграничения доступа;
- описание информационных потоков.

11.1.2. В качестве объекта доступа принята АС на базе ПЭВМ в целом.

11.1.3. В качестве субъектов доступа рассматриваются лица и процессы (общесистемные и прикладные программы пользователей), имеющие возможность доступа к объектам штатными средствами указанной АС.

Субъекты доступа должны иметь официальное разрешение (допуск) к конфиденциальной информации и персональным данным.

11.1.4. Комиссия проверяет соответствие описания технологического процесса обработки и хранения конфиденциальной информации и персональных данных реальному процессу.

11.1.5. Проводится анализ разрешенных и запрещенных связей между субъектами и объектами доступа с привязкой к конкретной АС и штатному персоналу, оценка их соответствия разрешительной системе доступа персонала к защищаемым ресурсам на всех этапах обработки.

11.2. Выбор методики испытаний и инструментальных средств.

При аттестационных испытаниях использование инструментальных средств аттестуемой АС не является необходимым.

11.3. Испытания подсистемы обеспечения целостности.

11.3.1. Проверка подсистемы обеспечения целостности СЗИ от НСД проводится по перечню функций, определенных РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» для данного класса АС.

11.3.2. Надежность функций контроля целостности программных средств может быть проверена при помощи внесения изменений в отдельные программы или их подмены. При этом отслеживается при помощи программы «ФИКС 2.0.2» реакция системы защиты на произведенные нарушения, осуществляется расчет контрольных сумм файлов из состава системы защиты для их сравнения с эталонными контрольными суммами на момент аттестации и при дальнейших проверках.

11.3.3. При проверке обеспечения неизменности программной среды определяется наличие и работоспособность технологии внесения новых программных средств в операционную среду, предусматривающую процедуры экспертной оценки или верификации новых программных средств для выявления потенциально опасных для СЗИ программных функций, критерии санкционирования ввода программ в операционную среду и допуска определенных категорий пользователей к этим программам.

Проверяется наличие и работоспособность средств и мер предотвращения несанкционированного ввода программ в операционную среду.

11.3.4. По результатам анализа технологического процесса обработки и хранения информации в АС проверяется выполнение требований по физической охране средств и носителей информации АС, пропускному режиму и оборудованию помещений необходимыми защитными средствами.

Проверяется наличие в системе администратора системы защиты информации, оценивается его уровень подготовленности и степень оснащения его рабочего места необходимыми средствами оперативного контроля и сопровождения СЗИ.

11.3.5. Проверяется наличие и работоспособность средств периодического тестирования всех функций СЗИ от НСД, наличие графика проведения тестирования. Средства тестирования должны давать однозначную информацию о всех функциях СЗИ, предусмотренных требованиями к данному классу АС.

11.3.6. Проводится оценка защищенности информационных ресурсов АС от компьютерных вирусов.

11.3.7. Проверяется работоспособность технологии восстановления программных средств защиты информации в АС, ведение архива программных средств защиты, условия и периодичность их обновления и тестирования.

Автоматическое оперативное восстановление функций СЗИ от НСД при сбоях проверяется путем моделирования сбойных ситуаций и последующей проверки (тестирования) функций СЗИ от НСД.

11.3.8. Проверяется наличие сертификатов соответствия на СЗИ, а также установленные в них классы защищенности, уровни контроля и т.п.

11.4. Испытания подсистемы регистрации и учета.

11.4.1. Регистрация и учет событий, определенных требованиями по безопасности информации к установленному классу АС, должны производиться на всех этапах технологического процесса хранения и обработки конфиденциальной информации. Регистрация должна охватывать все события, определенные вышеуказанными Руководящими документами Гостехкомиссии России для АС установленного класса и Положением ФСТЭК России для АС установленного класса.

11.4.2. Для проверки необходимо при помощи стандартных средств АС просмотреть результаты регистрации всех действий, которые были проведены с защищаемыми ресурсами при проверках по п. 11.2 таблицы 6. Должны быть зарегистрированы все требуемые события с требуемыми параметрами регистрации.

11.4.3. Для проверки регистрации изменения полномочий субъектов доступа необходимо произвести эти изменения при помощи СЗИ и просмотреть результаты регистрации.

11.4.4. Для проверки процедуры автоматического учета создаваемых, иницируемых защищаемых информационных ресурсов необходимо смоделировать создание защищаемого носителя информации на тех этапах технологического процесса, где используются ОТСС.

При помощи СЗИ просматриваются результаты учета. Должны быть автоматически учтены все созданные защищаемые информационные ресурсы с требуемыми параметрами учета.

11.4.5. Проверяется ведение учета всех защищаемых носителей информации, осуществляемого вручную персоналом, путем проверки технологических инструкций, степени ознакомления с ними конкретных исполнителей, проверки правильности ведения карточек и журналов учета.

11.4.6. Проверка отработки средств сигнализации на попытки нарушения защиты осуществляется путем моделирования несанкционированных обращений к защищаемым объектам доступа и отслеживания появления определенных сигналов в местах интерфейса с администратором системы защиты и нарушителем.

11.4.7. Рекомендации по результатам испытаний АС.

Комиссия может рекомендовать следующие меры по устранению недостатков:

- применение дополнительных организационно-технических мероприятий по защите информации;

- доработка организационно-распорядительной документации;
- применение дополнительных сертифицированных СЗИ;
- исключение отдельных программных средств из состава АС.

11.5. Проверка механизма уничтожения информации.

Надежность функции уничтожения (стирания) или обезличивания может быть проверена при помощи программы *Terrier 3.0*. Для проверки удаления информации создается текстовый файл, содержащий информацию, которой заведомо нет на проверяемом диске. Затем выполняется поиск искомой информации средствами программы *Terrier 3.0*. После удаления искомого файла удаляется и выполняется повторный поиск информации. Проверка считается пройденной, если искомая информация не найдена.

11.6. Проверка состава и работоспособности технических и программных средств.

В процессе выполнения данной проверки выполняется контроль установки программно обеспечения, включая обновления программного обеспечения средств защиты информации путем просмотра версии ПО и сравнения ее с актуальной версией. Также в ходе данной проверки выполняется контроль состава технических средств, ПО и СЗИ. Данная проверка выполняется штатными средствами ОС Windows и с помощью программы *Агент Инвентаризации*.

11.7. Контроль изменений в АС.

В процессе проведения данной проверки выполняется анализ документации на наличие в ней информации о назначении лиц, ответственных за внесения изменений в конфигурацию АС и СЗ АС, а также выполняется опрос данных сотрудников.

12. Оформление отчетной документации по результатам аттестации АС

12.1. Результаты аттестационных испытаний АС по всем рассмотренным выше направлениям обеспечения безопасности информации оформляются протоколом испытаний, содержащими:

- состав комиссии, дату испытаний, наименование АС;
- цель испытаний;
- перечень нормативных документов и методик испытаний;
- результаты испытаний на момент их окончания.

12.2. На основании полученных результатов испытаний принимается заключение по аттестации АС, которое должно включать:

- оценку соответствия АС требованиям по безопасности информации;
- перечень выявленных недостатков и нарушений;
- рекомендации по устранению выявленных недостатков и нарушений;
- вывод о возможности выдачи «Аттестата соответствия».

12.3. Оценка соответствия АС требованиям по безопасности информации проводится на основании анализа общих результатов испытаний и выявленных в процессе испытаний конкретных недостатков и нарушений.

12.4. В случае несоответствия АС установленным требованиям по защите информации комиссия может рассмотреть предложения заявителя по оперативному устранению выявленных недостатков и нарушений. При этом могут рекомендоваться следующие меры:

- доработка организационно-распорядительной документации;
- снижение класса защищенности АС;

- исключение отдельных ОТСС из состава АС;
- применение дополнительных организационно-технических мер защиты;
- применение дополнительных сертифицированных СЗИ.

12.5. Если в процессе аттестационных испытаний выявлены недостатки, не приводящие к нарушению установленных требований и норм защищенности информации, то комиссия может рекомендовать следующие меры:

- оперативное устранение выявленных недостатков в процессе аттестационных испытаний;
- устранение установленных недостатков и нарушений в согласованные с комиссией сроки с представлением необходимых документов;
- проведение дополнительных частичных испытаний в согласованные сроки.

Аттестационная комиссия:

Руководитель аттестационной комиссии:

Члены аттестационной комиссии:

Таблица 1 – состав ОТСС

№ п/п	Наименование ОТСС	Тип, модель	Серийный (заводской) номер
1.	Системный блок ПЭВМ в составе:	InWin	16119497356016
	- НЖМД	Seagate ST3120026A	3FN65PTF
	- DVD-ROM	Toshiba Samsung SD-M1912	68MA433632
2.	Монитор	Samsung 730BF	WM55XXXXX857629B
3.	Клавиатура	Mitsumi KFK-EA4XT	90LMFAO5CX5GMC8150*9291
4.	Манипулятор «мышь»	Logitech M-SBF90	XDB1285738
5.	Сканер	Epson J241A	FPDA979787

Таблица 2 – состав ВТСС

№ п/п	Наименование ВТСС	Тип, модель	Серийный (заводской) номер
1.	Телефонный аппарат	Atlinks FS29169GE2-C	29911734
2.	Датчик пожарной сигнализации (2 шт.)	-	б/н

Таблица 3 – состав СЗИ

№ п/п	Наименование СЗИ	Заводской номер	Номер знака соответствия	Сведения о сертификате	Место и дата установки
1.	Secret Net Studio 8.0	KLTRCP7	М 673056	сертификат ФСТЭК России № 3675 от 12.12.2016 г., действителен до 12.12.2019 г.	ПЭВМ, сер. № 11458720921807, 01.11.2017
2.	Kaspersky Endpoint Security 10 для Windows	СМП8877-2387	Л 729365	сертификат ФСТЭК России № 3025 от 25.11.2013 г., действителен до 25.11.2019 г.	ПЭВМ, сер. № 23678912459490, 01.11.2017

Таблица 4 – состав ПО

№ п/п	Наименование ПО
1.	ОС Microsoft Windows 7 Профессиональная SP1 x32, лиц. №
2.	Пакет офисных приложений Microsoft Office 2010, лиц. № в составе: Word, Excel
3.	Почтовая программа Mozilla Thunderbird 52.2.0, свободно-распространяемое ПО
4.	Программа чтения файлов в формате pdf Foxit Reader 7.3.6.321, свободно-распространяемое ПО
5.	Программа работы со сканером Epson Scan, свободно-распространяемое ПО
6.	СКЗИ КриптоПро CSP 3.9, лиц. №
7.	Антивирусная программа Касперского 10 (Kaspersky Endpoint Security 10 для Windows), лицензия
8.	СЗИ от НСД «Secret Net Studio 8.0» (редакция: Постоянная защита), лиц. №

Приложение В

(обязательное)

Протокол испытаний комплексной системы защиты информации АС

Экз. № 1

УТВЕРЖДАЮ

Генеральный директор

11 ноября 2017 г.

ПРОТОКОЛ

испытаний комплексной системы защиты информации автоматизированной
системы
на базе ПЭВМ (сер. № 16119497356016), расположенной в помещении № 3, на
соответствие требованиям по
безопасности информации в части защиты от
НСД и компьютерных вирусов

2017

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

АС	автоматизированная система
ЖМД	жесткий магнитный диск
ЛВС	локальная вычислительная сеть
МНИ	машинный носитель информации
МЭ	межсетевой экран
НСД	несанкционированный доступ
ОС	операционная система
ПО	программное обеспечение
ПЭВМ	персональная электронно-вычислительная машина
РД	руководящий документ
СЗИ	система (средство) защиты информации
СЗИ НСД	система защиты информации от несанкционированного доступа
СКЗИ	система криптографической защиты информации
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЭЦП	электронно-цифровая подпись

1 СОСТАВ И КЛАССИФИКАЦИЯ АС

На аттестационные испытания была представлена АС на базе ПЭВМ, сер. № Данная ПЭВМ подключена к учрежденческой ЛВС с использованием средств межсетевого экранирования. IP-адрес ПЭВМ – 192.168.0.110, сетевое имя – СА-COMP.

АС расположена в помещении № 3 по адресу: г. Пенза.

Комплектация аттестуемой ПЭВМ указана в таблице 1. Состав ПО, установленного на данной ПЭВМ, приведен в таблице 2. Носители информации с дистрибутивами лицензионного ПО на СЗИ находятся у администратора безопасности.

Таблица 1 – комплектация ПЭВМ

№ п/п	Наименование ОТСС	Тип, модель	Серийный (заводской) номер
1.	Системный блок ПЭВМ в составе:	InWin	16119497356016
	- НЖМД	Seagate ST3120026A	3FN65PTF
	- DVD-ROM	Toshiba Samsung SD-M1912	68MA433632
2.	Монитор	Samsung 730BF	WM55XXXX857629B
3.	Клавиатура	Mitsumi KFK-EA4XT	90LMFAO5CX5GMC8150*9291
4.	Манипулятор «мышь»	Logitech M-SBF90	XDB1285738
5.	Сканер	Epson J241A	FPDA979787

Таблица 2 – состав ПО, установленного на ПЭВМ

№ п/п	Наименование ПО
1.	ОС Microsoft Windows 7 Профессиональная SP1 x32, лиц. №
2.	Пакет офисных приложений Microsoft Office 2010, лиц. № в составе: Word, Excel
3.	Почтовая программа Mozilla Thunderbird 52.2.0, свободно-распространяемое ПО
4.	Программа чтения файлов в формате pdf Foxit Reader 7.3.6.321, свободно-распространяемое ПО
5.	Программа работы со сканером Epson Scan, свободно-распространяемое ПО
6.	СКЗИ КриптоПро CSP 3.9, лиц. №
7.	Антивирусная программа Касперского 10 (Kaspersky Endpoint Security 10 для Windows), лицензия
8.	СЗИ от НСД «Secret Net Studio 8.0» (редакция: Постоянная защита), лиц. №

Высший уровень конфиденциальности обрабатываемой информации – «коммерческая тайна». Режим работы пользователей – коллективный. Права доступа пользователей к информации – различные. На ПЭВМ установлен сертифицированный МЭ 3-го класса защищенности. Класс защищенности согласно РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» – 1Г для АС.

2 СОСТАВ СРЕДСТВ КОНТРОЛЯ ЗАЩИЩЕННОСТИ, ИСПОЛЬЗОВАННЫХ ПРИ АТТЕСТАЦИОННЫХ ИСПЫТАНИЯХ АС

Для контроля защищенности АС от НСД в ходе аттестационных испытаний использовались сертифицированные ФСТЭК России программные средства контроля эффективности применения СЗИ:

средство создания модели системы разграничения доступа «Ревизор 1 ХР», имеющая сертификат № 989 от 08.02.2005 г., выданный ФСТЭК России и лицензию на право использования.

программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 ХР», имеющая сертификат № 990 от 08.02.2005 г., выданный ФСТЭК России.

программа фиксации и контроля исходного состояния программного комплекса «ФИКС» версия 2.0.2, имеющая сертификат № 1548 от 15.01.2008 г., выданный ФСТЭК России и лицензию на право использования.

программа поиска и гарантированного уничтожения информации на дисках «Terrier 3.0», имеющая сертификат № 1193 от 16.05.2006 г., выданный ФСТЭК России и лицензию на право использования.

система анализа программного и аппаратного обеспечения TCP/IP сетей (сетевой сканер) «Ревизор Сети» версии 3.0, имеющая сертификат № 3413 от 02.06.2015 г., выданный ФСТЭК России и лицензию на право использования.

сетевой сканер «Nessus 3.0.3».

3 АНАЛИЗ И ОЦЕНКА ИСХОДНЫХ ДАННЫХ ПО АТТЕСТУЕМОЙ АС

Проверка состава технических средств, места их расположения, а также перечня установленных на ПЭВМ программных средств показала соответствие представленных исходных данных реальным условиям размещения и эксплуатации АС.

Аттестационной комиссии в ходе подготовки и проведения испытаний АС были представлены следующие документы:

приказ о назначении администратора безопасности;

акт классификации автоматизированной системы;

перечень сведений конфиденциального характера, подлежащих защите;

разрешительная система доступа к информационным ресурсам автоматизированной системы;

описание технологического процесса обработки информации в автоматизированной системе;

инструкция администратору безопасности АС;

инструкция по работе пользователей АС;

инструкция по проведению антивирусного контроля;

список лиц, имеющих право доступа в помещение № 3.

Проверка представленных документов показала их достаточность для проведения аттестационных испытаний заявленной АС.

4 ПРОВЕРКА ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ И ХРАНЕНИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

Проверка заключалась в анализе состояния реального технологического процесса обработки информации в АС и выработке заключения о его соответствии или несоответствии предоставленной эксплуатационной и организационно-распорядительной документации при аттестационных испытаниях.

В ходе проверки были определены:

- особенности технологического процесса обработки информации;
- перечень объектов доступа;
- перечень субъектов доступа;
- перечень штатных средств доступа к информации;
- перечень средств защиты информации;
- описание реализованных правил разграничения доступа;
- перечень угроз НСД.

4.1 Анализ техпроцесса обработки информации, реализованного в АС

Согласно описанию техпроцесса обработки информации, представленному в вышеуказанной документации, АС предназначена для генерации и записи закрытых ключей на съемные электронные носители информации (eToken, ruToken и др.), формирования сертификатов открытых ключей, отправки их в корневой удостоверяющий центр по каналам связи общего пользования закрытых ключей. Данные закрытые ключи, в соответствии с положениями, принятыми, являются информацией с уровнем конфиденциальности «КОНФИДЕНЦИАЛЬНО».

Данная АС предназначена для работы в многопользовательском режиме, доступ исполнителей к работе на ПЭВМ осуществляется по утвержденному списку, пользователи имеют различные права доступа к информации, обрабатываемой в АС.

Каждый пользователь имеет право постоянного хранения файлов с информацией, содержащей конфиденциальные сведения, в специально выделенных каталогах на ЖМД (в соответствии с «Разрешительной системой доступа...»). Однако, в соответствии с технологическим процессом генерации закрытых ключей данные ключи не хранятся на ЖМД, а после генерации сразу записываются на съемные МНИ, которые передаются владельцу ключа, для которого они генерируются.

В целях защиты информации от НСД локального, а также со стороны ЛВС и открытых каналов связи в АС используется СЗИ НСД «Secret Net Studio 8.0». Средствами СЗИ НСД на ПЭВМ организуются права доступа пользователей к ресурсам ПЭВМ. В состав СЗИ НСД входит ПАК «Соболь».

Настройка СЗИ НСД для конкретных пользователей и контроль ее работы осуществляется администратором безопасности. Функции, права, обязанности и порядок работы на ПЭВМ администратора и пользователей регламентируется вышеуказанными документами.

Доступ к работе на АС осуществляется по предъявлению электронного идентификатора и паролю конкретного пользователя (в ПАК «Соболь» при включении питания ПЭВМ) и по вводу логина (персонального идентификатора, имени пользователя) и паролю, после чего тот получает установленные администратором безопасности права доступа к устройствам, каталогам, файлам и программам ПЭВМ.

На ПЭВМ установлена операционная система Microsoft Windows 7.

Для генерации ключей установлена СКЗИ «КриптоПро CSP 3.9».

Для обеспечения рабочего технологического процесса используются также программы Mozilla Thunderbird (для отправки сертификатов по электронной почте в корневой удостоверяющий центр), Epson Scan (сканирования документов заявителей), Foxit Reader (для чтения документов pdf).

Антивирусная защита осуществляется с применением программного средства Антивирус Касперского 10 в соответствии с «Инструкцией по антивирусной защите...».

Помещение размещения АС находится под охраной постоянно. В здании действует пропускной режим входа, само здание охраняется круглосуточно. Дверь в помещение оборудована механическим замком, который закрыт все время, когда ПЭВМ не эксплуатируется. Пользователи, работающие на ПЭВМ, следят за отсутствием посторонних лиц в помещении во время работы на ПЭВМ.

4.2 Перечень объектов доступа

Объектами доступа являются:

ПЭВМ в целом;

устройство ввода-вывода на сменные МНИ;

ЖМД;

монитор с отображаемой на нем конфиденциальной информацией;

персональные сменные МНИ с расположенными на них ключами;

каталоги всех файлов, хранимых на магнитных носителях;

оперативная память ПЭВМ;

операционная система;

программы, предназначенные для генерации ключей.

4.3 Перечень субъектов доступа

Субъектами доступа к защищаемой информации на АС являются:

администратор безопасности;

пользователи, работающие на ПЭВМ;

процессы, выполняемые на ПЭВМ от имени администратора и пользователей при обработке информации и настройке АС;

пользователи, не допущенные до работы на ПЭВМ, но имеющие доступ к ЛВС;

субъекты, пользующиеся теми же каналами связи и открытыми сетями связи, что и пользователи АС.

4.4 Перечень штатных средств доступа к информации

Для пользователей в качестве штатных средств доступа в АС предусмотрены:

стандартные средства операционной системы Microsoft Windows 7;

СКЗИ «КриптоПро CSP 3.9»;

программы из списка установленного ПО, разрешенного для запуска пользователями;

средства настройки и контроля функций установленного на ПЭВМ СЗИ НСД «Secret Net Studio 8.0».

4.5 Перечень средств защиты информации

Общесистемное ПО не позволяет обеспечить защиту информации, поэтому на ПЭВМ используются следующие сертифицированные СЗИ:

СЗИ НСД «Secret Net Studio» в составе:

- ПО «Secret Net Studio 8.0»;
 - ПАК «Соболь» версии 3.0 со считывателем и идентификаторами;
- Антивирусная программа Касперского 10 (Kaspersky Endpoint Security 10 для Windows).

СЗИ НСД «Secret Net Studio» имеет сертификат № 3675 от 12.12.2016 г., действительный до 12.12.2019 г., выданный ФСТЭК России на соответствие требованиям руководящих документов по 2 уровню контроля отсутствия НДВ, 3 классу защищенности СВТ и 2 классу защищенности МЭ. Может применяться в АС до класса 1Б включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно.

Антивирусная программа «Kaspersky Endpoint Security 10 для Windows» имеет сертификат № 3025 от 25.11.2013 г., действительный до 25.11.2019 г., выданный ФСТЭК России на соответствие требованиям документов «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВЗ.В2.ПЗ» (ФСТЭК России, 2012) и «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ» (ФСТЭК России, 2012).

Лицензионные продукты были приобретены у производителя данного продукта. Средства защиты были установлены в соответствии с руководствами по установке и администрированию и функционируют в среде Microsoft Windows 7 в соответствии с руководствами по эксплуатации.

СЗИ НСД реализует следующие защитные механизмы:

- контроль входа пользователей в систему;
- защита от загрузки посторонней операционной системы;
- контроль устройств;
- контроль печати;
- замкнутая программная среда;
- дискреционное управление доступом к ресурсам файловой системы;
- затирание данных;
- защита информации на локальных дисках;
- межсетевое экранирование с фильтрацией по следующим параметрам:
 - фильтрация на сетевом уровне с независимым принятием решений по каждому пакету;
 - фильтрация пакетов служебных протоколов (ICMP, IGMP и т.д.), необходимых для диагностики и управления работой сетевых устройств;
 - фильтрация с учетом входного и выходного сетевого интерфейса для проверки подлинности сетевых адресов;
 - фильтрация на транспортном уровне запросов на установление виртуальных соединений (ТСР-сессий);
 - фильтрация на прикладном уровне запросов к прикладным сервисам (фильтрация по символьной последовательности в пакетах);
 - фильтрация с учетом полей сетевых пакетов;
 - фильтрация с учетом даты/времени суток

Антивирусная программа обеспечивает:

комплексную защиту компьютера от известных и новых угроз, сетевых и мошеннических атак;

обновление баз и модулей программы, используемых в работе программы;

мониторинг уязвимостей в режиме реального времени, проверяющий программы, запущенные на ПЭВМ, а также проверяет программы в момент их запуска;

мониторинг системы, собирающий данные о действиях программ на компьютере и предоставляющий эту информацию другим компонентам для более эффективной защиты ПЭВМ;

антивирусную защиту файлов, позволяющую избежать заражения файловой системы компьютера. (запускается при старте, постоянно находится в оперативной памяти ПЭВМ и проверяет все открываемые, сохраняемые и запускаемые файлы на ПЭВМ и на всех присоединенных дисках, перехватывает каждое обращение к файлу и проверяет этот файл на присутствие вирусов и других программ, представляющих угрозу);

антивирусную защиту почты (проверка входящих и исходящих почтовых сообщений на наличие в них вирусов и других программ, представляющих угрозу).

Реальные условия эксплуатации вышеперечисленных СЗИ обеспечивают условия эксплуатации, рекомендованные разработчиками данных СЗИ.

4.6 Описание реализованных правил разграничения доступа

С помощью применяемых в АС СЗИ субъектам доступа присвоены официальные полномочия для допуска к информации в соответствии с принятой разрешительной системой разграничения доступа.

В соответствии с представленной на АС документацией реализованы правила доступа, при которых каждый пользователь имеет право доступа:

к средствам ОС Microsoft Windows 7, обеспечивающим запуск и функционирование АС;

к средствам антивирусной защиты (Антивирус Касперского 10);

к программам из списка программ, разрешенных для выполнения;

к сменным МНИ, предназначенным для хранения ключевой информации;

к сменным МНИ, предназначенным для копирования с них на ПЭВМ открытой информации, необходимой для заполнения форм сертификата открытого ключа;

к каталогам на ЖМД;

к выделенным ПЭВМ ЛВС для получения и передачи необходимой информации (сервер обновления антивирусной программы).

Всем пользователям, кроме администратора безопасности, запрещен доступ к средствам настройки и изменения полномочий доступа СЗИ.

Операции доступа к объектам доступа документируются средствами регистрации и учета СЗИ.

4.7 Перечень угроз НСД в АС и реализованных мер по их устранению

Типовыми угрозами могут являться:

хищение, вывод из строя ПЭВМ в целом, либо носителей информации;

копирование защищаемых ресурсов на неучтенные МНИ;

доступ к ресурсам ПЭВМ за счет обхода СЗИ с использованием загрузки с МНИ, а также путем исключения загрузки модулей и драйверов СЗИ;
 нарушение целостности файлов операционной системы, СЗИ, в том числе компьютерными вирусами;
 разрушение защищаемой информации компьютерными вирусами;
 доступ во время отсутствия пользователя на рабочем месте при выполненном санкционированном входе в ОС, в том числе к загруженной ключевой информации;
 несанкционированное ознакомление с защищаемой информацией, отображаемой на мониторе;
 запуск пользователем вредоносной программы с МНИ или ЖМД;
 доступ к ПЭВМ со стороны ЛВС и открытых каналов связи;
 доступ к запрещенным ПЭВМ ЛВС.

Согласно представленной документации перечисленные угрозы устраняются применением в АС СЗИ НСД «Secret Net Studio», антивирусной программы и их специальной настройкой, а также реализацией ряда организационных мер.

Обобщенный перечень реализованных в АС средств, способов и мер защиты применительно к существующим угрозам НСД с учетом категорий возможных нарушителей и способов реализации угроз представлен в таблице 3.

Таблица 3 – Угрозы НСД, способы их реализации и устранения

№ п/п	Тип угрозы НСД	Кто может явиться нарушителем	Способ реализации угрозы	Как устранена угроза
1.	Хищение, вывод из строя ПЭВМ в целом, либо носителей информации	Лица, имеющие возможность доступа в помещение с ПЭВМ (пользователи, администратор безопасности, обслуживающий персонал и т.д.)	Вынос оборудования	Контроль доступа в помещение, физическая охрана, использование средств технической охраны
2.	Копирование защищаемых информационных ресурсов на неучтенные МНИ	– / / –	В процессе работы на ПЭВМ легальных пользователей, Несанкционированный доступ к ПЭВМ посторонних лиц	Регламентация прав и ответственности пользователей в соответствии с «Инструкцией пользователя...»
3.	Доступ к ресурсам АС за счет обхода СЗИ с использованием загрузки с МНИ, а также путем исключения загрузки модулей и драйверов СЗИ	– / / –	– / / –	Запрещение загрузки с внешних носителей средствами СЗИ НСД «Secret Net Studio»
4.	Нарушение целостности файлов операционной системы,	– / / –	– / / –	Контроль файлов СЗИ основных файлов ОС файлов средствами СЗИ

№ п/п	Тип угрозы НСД	Кто может явиться нарушителем	Способ реализации угрозы	Как устранена угроза
	СЗИ, в том числе компьютерными вирусами			НСД «Secret Net Studio» Контроль ПАК «Соболь» целостности своих файлов
5.	Разрушение защищаемой информации компьютерными вирусами	– // –	– // –	Наличие антивирусной программы и методических документов по антивирусной защите
6.	Доступ во время отсутствия пользователя на рабочем месте при выполненном санкционированном входе в ОС, в том числе к загруженной ключевой информации	– // –	Во время отсутствия на рабочем месте легального пользователя	Блокировка монитора и клавиатуры средствами СЗИ НСД «Secret Net Studio», Ограниченный вход в помещение
7.	Несанкционированное ознакомление с защищаемой информацией, отображаемой на мониторе	– // –	Просмотр информации на мониторе при работе легальных пользователей, при наличии разграничений по доступу к информации, как пользователями, так и посетителями организации	Ограниченное «Списком лиц, имеющих право доступа в помещение № 39» количество лиц, имеющих возможность визуального просмотра. Принятие пользователями во время работы мер по затруднению просмотра информации на мониторе. Жалюзи на окнах
8.	Запуск пользователем вредоносной программы с МНИ или ЖМД	– // –	В процессе работы на ПЭВМ легальных пользователей, Несанкционированный доступ к ПЭВМ посторонних лиц	Разрешение запуска только ограниченного набора программ в соответствии с внутренней документацией
9.	Доступ к ПЭВМ со стороны ЛВС и открытых каналов связи	Пользователи ЛВС организации, а также посторонние пользователи открытых каналов связи, к которым подключена АС	– // –	Разрешение только разрешенных соединений средствами установленного СЗИ «Secret Net Studio»
	Доступ к запрещенным ПЭВМ ЛВС	Лица, имеющие возможность доступа в помещение с ПЭВМ (пользователи, администратор безопасности,	– // –	Разрешение только разрешенных соединений средствами установленного СЗИ «Secret Net Studio» Ответственность пользователя за доступ к посторонним ПЭВМ

№ п/п	Тип угрозы НСД	Кто может явиться нарушителем	Способ реализации угрозы	Как устранена угроза
		обслуживающий персонал и т.д.)		

5 ИСПЫТАНИЯ АС НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО ЗИ ОТ НСД

В рамках испытаний АС на соответствие требованиям по ЗИ от НСД были проведены:

- проверка подсистемы управления доступом;
- проверка подсистемы регистрации и учета;
- проверка подсистемы обеспечения целостности.

5.1 Проверка подсистемы управления доступом

В рамках испытаний подсистемы управления доступом проверке был подвержен механизм идентификации и проверки подлинности субъектов доступа при входе в систему.

Идентификация и проверка подлинности субъектов доступа осуществляется средствами ПАК «Соболь» версии 3.0 при загрузке ПЭВМ по персональному электронному идентификатору и паролю условно-постоянного действия, состоящему не менее, чем из шести буквенно-цифровых символов. Кроме того средствами ПО «Secret Net Studio 8.0» осуществляется авторизация пользователя при входе в систему по логину и паролю условно-постоянного действия, состоящим не менее, чем из шести буквенно-цифровых символов.

Настройки СЗИ выполнены таким образом, что при задании или смене пароля невозможно ввести пароль длиной менее шести символов. Смена паролей осуществляется каждым пользователем самостоятельно, не реже одного раза в месяц.

Надежность аутентификации оценивалась возможностью подбора или несанкционированного получения пароля посторонним субъектом доступа в период действия этого пароля с учетом временной блокировки ПЭВМ после превышения заданного в СЗИ «Secret Net Studio» (в том в числе ПАК «Соболь») предела (пять раз) попыток неправильного ввода пароля или предъявления незарегистрированного электронного идентификатора. Данные события фиксируются в журнале СЗИ НСД «Secret Net Studio», а также в журнале ПАК «Соболь», находящемся в энергонезависимой памяти контроллера СЗИ НСД. Доступ к данным журналам разрешен только администратору безопасности.

При временном оставлении рабочего места пользователем принудительно (либо по истечении интервала неактивности) включается блокировка монитора и клавиатуры ПЭВМ. Снятие блокировки возможно только путем предъявления идентификатора и ввода пароля пользователя, инициировавшего блокировку, или администратора безопасности.

Средствами СЗИ «Secret Net Studio» разрешены только необходимые соединения (серверы удостоверяющих центров, сервер обновления антивирусной программы). Доступ к ПЭВМ со стороны открытых каналов связи разрешен только при инициализации соединения со стороны АС.

Пользователи не имеют доступа к органам настройки СЗИ. Таким образом, возможность изменения настроек доступна только для администратора безопасности.

Система фильтрации, реализованная на ПЭВМ средствами СЗИ «Secret Net Studio», была проверена с помощью системы анализа программного и аппаратного обеспечения TCP/IP сетей (сетевой сканер) «Ревизор Сети» версии 3.0, а также сетевого сканера «Nessus 3.0.3», сканировавших порты ПЭВМ из состава АС.

Анализ результатов работы программы «Ревизор Сети» версии 3.0 и программы «Nessus 3.0.3» показал, что АС недоступна к защищаемым ресурсам ПЭВМ со стороны ПЭВМ из состава ЛВС, сетевой доступ которых к АС не разрешен.

Система разграничения доступа, реализованная на объекте средствами СЗИ «Secret Net Studio» была испытана с помощью средства создания модели системы разграничения доступа «Ревизор 1 ХР» и программы контроля полномочий доступа к информационным ресурсам «Ревизор 2 ХР».

Анализ результатов работы программы «Ревизор 2 ХР», а также имитации несанкционированных действий показал, что реальные права пользователей по доступу к защищаемым ресурсам соответствуют установленной разрешительной системе доступа, а примененные способы и средства контроля защищенности не позволяют получить несанкционированный доступ к защищаемым ресурсам ПЭВМ.

Вывод: права доступа пользователей к информационным и техническим ресурсам АС реализованы в соответствии с принятой для данной АС разрешительной системой доступа. Подсистема управления доступом обеспечивается средствами используемых систем защиты информации: СЗИ НСД «Secret Net Studio» и удовлетворяет требованиям РД к заявленному классу защищенности 1Г.

5.2 Проверка подсистемы регистрации и учета

При проведении аттестационных испытаний проверялись:
регистрация и учет событий входа/выхода пользователей в/из системы средствами установленных СЗИ на всех этапах технологического процесса обработки и хранения информации, требуемых РД;
порядок регистрации и учета носителей конфиденциальной информации.

В ходе проверки моделировались стандартные процессы обработки информации, после чего просматривались результаты учета в журнале регистрации событий.

Проверка показала, что в журнале СЗИ НСД «Secret Net Studio» регистрируются все события, требуемые РД для класса защищенности 1Г. Параметры регистрации также соответствуют требованиям РД. При наличии попыток несанкционированного доступа либо нарушениях целостности системы происходит фиксация данных событий в журнале СЗИ.

МЭ из состава СЗИ «Secret Net Studio» осуществляет регистрацию события сетевой активности ПЭВМ и сети, а также пакеты, полученные и отправленные ПЭВМ. Факты несанкционированных соединений также отмечаются в журнале МЭ. В журнале регистрируются заблокированные пакеты, причины их блокировки.

Также система обнаружения атак, входящая в состав СЗИ «Secret Net Studio», регистрирует в журнале обнаруженные сетевые атаки.

Установленные на ПЭВМ СЗИ не осуществляют автоматическую регистрацию, учет и маркировку защищаемых носителей информации. Однако выполнение соответствующих требований РД обеспечивается организационными мерами. Все носители информации, на которые записываются ключи подписи, получают лица, для которых формируется ключ подписи.

Печать конфиденциальных документов в АС не осуществляется.

Очистка областей оперативной памяти осуществляется при окончании работы на ПЭВМ, путем перезагрузки ПЭВМ. Очистка памяти на машинных носителях информации

автоматически осуществляется программными средствами, встроенными в СЗИ. Эффективность очистки была проверена с помощью программы поиска и гарантированного уничтожения информации на дисках «Terrier 3.0». Проверка показала, что после удаления файла участок на машинном носителе, где располагался этот файл, заполнен случайной последовательностью. Кроме того, фрагменты данного файла не были найдены программой «Terrier 3.0» на всем носителе.

Вывод: регистрация и учет различных событий осуществляется средствами СЗИ «Secret Net Studio». Параметры регистрации и учета при реализации принятых организационно-режимных мер, соответствуют требованиям РД к заявленному классу защищенности 1Г.

5.3 Проверка подсистемы обеспечения целостности

В ходе аттестационных испытаний осуществлялись:

- проверка обеспечения целостности программных средств СЗИ, а также неизменности программной среды;
- проверка отсутствия на ПЭВМ средств разработки и отладки программного обеспечения;
- проверка наличия физической охраны ПЭВМ;
- проверка наличия администратора (службы), ответственного за ведение, нормальное функционирование и контроль работы СЗИ НСД;
- проверка проведения периодического тестирования СЗИ;
- проверка используемых программных средств на наличие вирусов;
- проверка наличия средств восстановления как используемой программной среды и приложений, так и СЗИ.

При загрузке системы средствами ПАК «Соболь» осуществляется автоматический контроль целостности CMOS ПЭВМ, главных загрузочных записей (MBR0...MBR2) ЖМД, файлов СЗИ от НСД, а также основных файлов загрузчика операционной системы. При обнаружении нарушений СЗИ НСД сигнализирует об этом администратору и не позволяет пользователю загрузить ОС.

Кроме того, ПО СЗИ НСД «Secret Net Studio» при загрузке проверяет целостность своих файлов.

Средства разработки и отладки программного обеспечения на ПЭВМ отсутствуют.

Помещение размещения АС (№ 3) оборудовано техническими средствами охраны. Все сменные носители конфиденциальной информации (с ключом подписи клиента) хранятся до передачи на виду у клиента, для которого данный закрытый ключ был сгенерирован.

Приказом от 10.05.2017 г. назначен администратор безопасности, который в своей практической работе должен руководствоваться соответствующими нормативными документами.

Администратором безопасности проводится периодическое обслуживание и тестирование функций СЗИ «Secret Net Studio». Порядок и периодичность проведения администратором технологических операций по обслуживанию и тестированию СЗИ и системы в целом определены в инструкциях для администратор безопасности.

Все МНИ, используемые в АС, подвергаются обязательному контролю на наличие компьютерных вирусов при помощи антивирусной программы Антивирус Касперского 10.

ЖМД находится под контролем антивирусной программы постоянно. Кроме того, периодически проводится антивирусный контроль ЖМД по расширенному алгоритму. Обновление баз данных антивирусного средства периодически производится администратором безопасности.

В ходе проверки установлено наличие дистрибутивов используемого общего ПО и сертифицированного ПО СЗИ «Secret Net Studio».

Для контроля целостности ПО СЗИ «Secret Net Studio» были зафиксированы контрольные суммы файлов, входящих в его состав. Расчет контрольных сумм производился на момент проведения аттестационных испытаний. Контрольные суммы вычислялись по алгоритму Уровень 1 (с постоянным кодом, вшитым в программу) с использованием специального программного обеспечения «Программа фиксации и контроля исходного состояния программного комплекса (ФИКС 2.0.1)».

Вывод: подсистема обеспечения целостности удовлетворяет требованиям РД к заявленному классу защищенности 1Г.

Обобщенный перечень требований РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» по классу защищенности 1Г представлены в таблице 4.

Таблица 4. Требования РД и выполнение их в АС

№	Подсистемы и требования	Выполнение требований	
		ПЭВМ	РД (1Г)
1	2	3	4
1. Подсистема управления доступом			
1.1.	Идентификация, проверка подлинности и контроль доступа субъектов: - в систему - к терминалам ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ - к программам - к томам, каталогам, файлам, записям, полям записей	 + + + +	 + + + +
1.2.	Управление потоками информации	—	—
2. Подсистема регистрации и учета			
2.1.	Регистрация и учет: - входа (выхода) субъектов доступа в (из) систему - выдачи печатных (графических) выходных документов - запуска (завершения) программ и процессов (заданий, задач) - доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи - доступа программ субъектов доступа к терминалам ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей - изменение полномочий субъектов доступа - создаваемых защищаемых объектов доступа	 + +— + + — + —	 + + + + + — —
2.2.	Учет носителей информации	+—	+

2.3.	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	+	+
2.4.	Сигнализация попыток нарушения защиты	+	—
3. Криптографическая подсистема			
3.1.	Шифрование конфиденциальной информации	—	—
3.2.	Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	—	—
3.3.	Использование аттестованных (сертифицированных) криптографических средств	—	—
4. Подсистема обеспечения целостности			
4.1.	Обеспечение целостности программных средств и обрабатываемой информации	+	+
4.2.	Физическая охрана средств вычислительной техники и носителей информации	+	+
4.3.	Наличие администратора (службы) защиты информации в АС	+	—
4.4.	Периодическое тестирование СЗИ от НСД	+	+
4.5.	Наличие средств восстановления СЗИ от НСД	+	+
4.6.	Использование сертифицированных средств защиты	+	—

Примечание. В графе 3 ставится:

- «+», если требование выполняется;
- «+—», если требование выполняется при помощи организационных мер;
- «—», если требование не выполняется.

В графе 4 ставится:

- «+», если требование должно выполняться;
- «—», если требование не должно выполняться.

6 ИСПЫТАНИЯ АС НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО ЗИ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

В АС для защиты от вирусов используется лицензионная антивирусная программа Антивирус Касперского 10, имеющая действующий сертификат ФСТЭК России.

Обновление вирусных баз осуществляется в соответствии с «Инструкцией по антивирусной защите», что позволяет обеспечить необходимую защиту информационных ресурсов, программных и технических средств объекта информатизации от компьютерных вирусов. Обновление программных модулей антивирусной программы для сохранения бинарной целостности отключено в настройках программы.

Правила работы в АС, направленные на предотвращение заражения компьютерными вирусами, а также меры по устранению заражения приведены в «Инструкции по проведению антивирусного контроля...».

Кроме этого, используемый на ПЭВМ МЭ из состава СЗИ «Secret Net Studio» также осуществляет защиту от вирусов путем фильтрации входящего трафика.

Вывод. Аттестуемая АС соответствует требованиям по защите информации от компьютерных вирусов при условии:

- использования на ПЭВМ лицензионных антивирусных программ и их периодического обновления;
- периодического проведения мероприятий антивирусного контроля.

Вывод.

Учитывая вышеизложенное, комиссия считает, что при выполнении положений разрешительных документов, имеющих в АС, а также при выполнении должностных обязанностей администратором безопасности и пользователями, обрабатываемая в АС информация с уровнем конфиденциальности не выше «КОНФИДЕНЦИАЛЬНО» защищена от НСД по требованиям безопасности для АС класса защищенности 1Г, при этом возможность внесения компьютерных вирусов в ПО ПЭВМ сведена к минимуму.

Аттестационная комиссия:

Руководитель аттестационной
комиссии:

Члены аттестационной комиссии:

Приложение Г

(обязательное)

Протокол оценки защищенности ОТСС из состава АС

УТВЕРЖДАЮ

Генеральный директор

11 ноября 2017 г.

ПРОТОКОЛ

оценки защищенности ОТСС из состава автоматизированной системы на базе автономной ПЭВМ (сер. № 16119497356016), расположенной в помещении № 3, от утечки конфиденциальной информации по каналу ПЭМИ

1. Измерению уровней побочных электромагнитных излучений подвергалась ПЭВМ (сер. № ...) в комплектации, приведенной в таблице 1.

Таблица 1

№ п/п	Наименование ОТСС	Тип, модель	Серийный (заводской) номер
1.	Системный блок ПЭВМ в составе:	InWin	16119497356016
	- НЖМД	Seagate ST3120026A	3FN65PTF
	- DVD-ROM	Toshiba Samsung SD-M1912	68MA433632
2.	Монитор	Samsung 730BF	WM55XXXXX857629B
3.	Клавиатура	Mitsumi KFK-EA4XT	90LMFAO5CX5GMC8150*9291
4.	Манипулятор «мышь»	Logitech M-SBF90	XDB1285738
5.	Сканер	Epson J241A	FPDA979787

2. Цель проведения работ по оценке защищенности заключалась в определении возможных расстояний распространения информативных сигналов от ОТСС и установления требуемого радиуса контролируемой зоны (КЗ) R2.

Работы проводились в мае 2017 года на территории по адресу: г. Пенза.

3. При проведении оценки защищенности ОТСС использовались нормативные и методические документы по аттестации.

Измерения уровней побочных электромагнитных излучений от вышеперечисленных ОТСС проводились по электрической (канал «Е») и магнитной (канал «Н») составляющим электромагнитного поля с применением средств измерений, приведенных в таблице 2.

Таблица 2

№ п/п	Наименование	Тип, модель	Серийный номер	Дата поверки
1.	Анализатор спектра			
2.	Генератор сигналов			
3.	Генератор сигналов			
4.	Осциллограф (с многофункциональным пробником)			
5.	Антенна измерительная			
6.	Антенна измерительная			

Оценка защищенности проводилась в следующих диапазонах частот: 9 кГц – 30 МГц (канал «Н»), 9 кГц – 1,0 ГГц (канал «Е»). Измерения составляющих электромагнитного поля проводились в дБ относительно 1 мкВ/м в полосе частот 9 кГц для диапазона 0,15 – 30 МГц и 120 кГц - для диапазона частот свыше 30 МГц. Измерительные антенны размещались на расстояниях (d) не менее двух геометрических размеров антенн от источника излучения опасного сигнала (ОС) до центра соответствующей антенны, а измерения проводились в местах обнаружения максимального сигнала с наибольшим соотношением сигнал/помеха.

В качестве тестов использовались сигналы, создаваемые специализированной программой, удовлетворяющие требованиям ГОСТ 29339-92.

4. Перечень ОС и нормы их защищенности приведены в таблице 3.

Таблица 3

№ п/п	Вид ОС
1.	ОС1 – сигналы видеомонитора
2.	ОС2 – сигналы записи/считывания НЖМД
3.	ОС3 – сигналы считывания DVD-ROM
4.	ОС4 – сигналы клавиатуры
5.	ОС5 – сигналы сканера
6.	ОС6 – сигналы USB-интерфейса

5. Результаты измерений и расчетов по оценке защищенности информации приведены в таблицах №№ 1-3 приложения настоящего протокола. Сводные данные по каждому виду ОС приведены в таблице 4.

Таблица 4

Вид ОС	Fт, МГц	E _{0н} , дБ	pH _{0н} , дБ	E _{шн} , дБ	pH _{шн} , дБ	E _{сн} , мкВ/м	pH _{сн} , мкВ/м	Ri, м
ОС1	44,55	10	-	8	-	131,38	-	1,13
ОС2	25	12	-	8	-	25,4	-	0,98
ОС6	240	12	-	8	-	81,24	-	0,98

Согласно таблице 4, максимальный радиус требуемой контролируемой зоны (КЗ) для ОТСС определяется сигналами вида ОС1 и составляет 1,13 метра.

Сигналов вида ОСЗ-ОС5 на фоне собственных шумов КИА и объектовой помехи не обнаружено. Минимальное расстояние от места установки ОТСС до границы КЗ составляет 12 метров.

Вывод. Защищенность ОТСС от утечки конфиденциальной информации по каналу ПЭМИ обеспечивается, так как рассчитанный требуемый радиус КЗ не превышает минимального расстояния от ОТСС до границы КЗ.

Дополнительных мер по защите информации не требуется.

Аттестационная комиссия:

Руководитель аттестационной комиссии:

Члены аттестационной комиссии:

РЕЗУЛЬТАТЫ ИЗМЕРЕНИЙ И РАСЧЕТОВ

Сигналы монитора (OC1)F_T = 54 МГц

Разрешение – 1280x1024, 60 Гц

Тип кодирования – последовательное

Сигнал – импульсный

Расстояние до измерительной антенны – 1 м, канал «Е»

Таблица 1

№	F, МГц	Ус+п, дБ	Уп, дБ	Кпер, дБ	Есi, мкВ/м	Ешi, мкВ/м	R2, м
1	270	10,00	8,00	36,70	131,38	171,79	1,13
2	378	12,00	10,00	31,50	90,89	118,85	1,13
3	486	11,00	10,00	31,50	60,48	118,85	0,95
4	594	11,00	10,00	32,40	67,08	131,83	0,95
						Итог:	1,13

Сигналы НЖМД (OC2)F_T = 25 МГц

Тип кодирования – последовательное

Сигнал – импульсный

Расстояние до измерительной антенны – 1 м, канал «Е»

Таблица 2

№	F, МГц	Ус+п, дБ	Уп, дБ	Кпер, дБ	Есi, мкВ/м	Ешi, мкВ/м	R2, м
1	125,00	12,00	8,00	18,30	25,40	20,65	0,98
						Итог:	0,98

Сигналы USB-интерфейса (OC6)F_T = 240 МГц

Тип кодирования – последовательное

Сигнал – импульсный

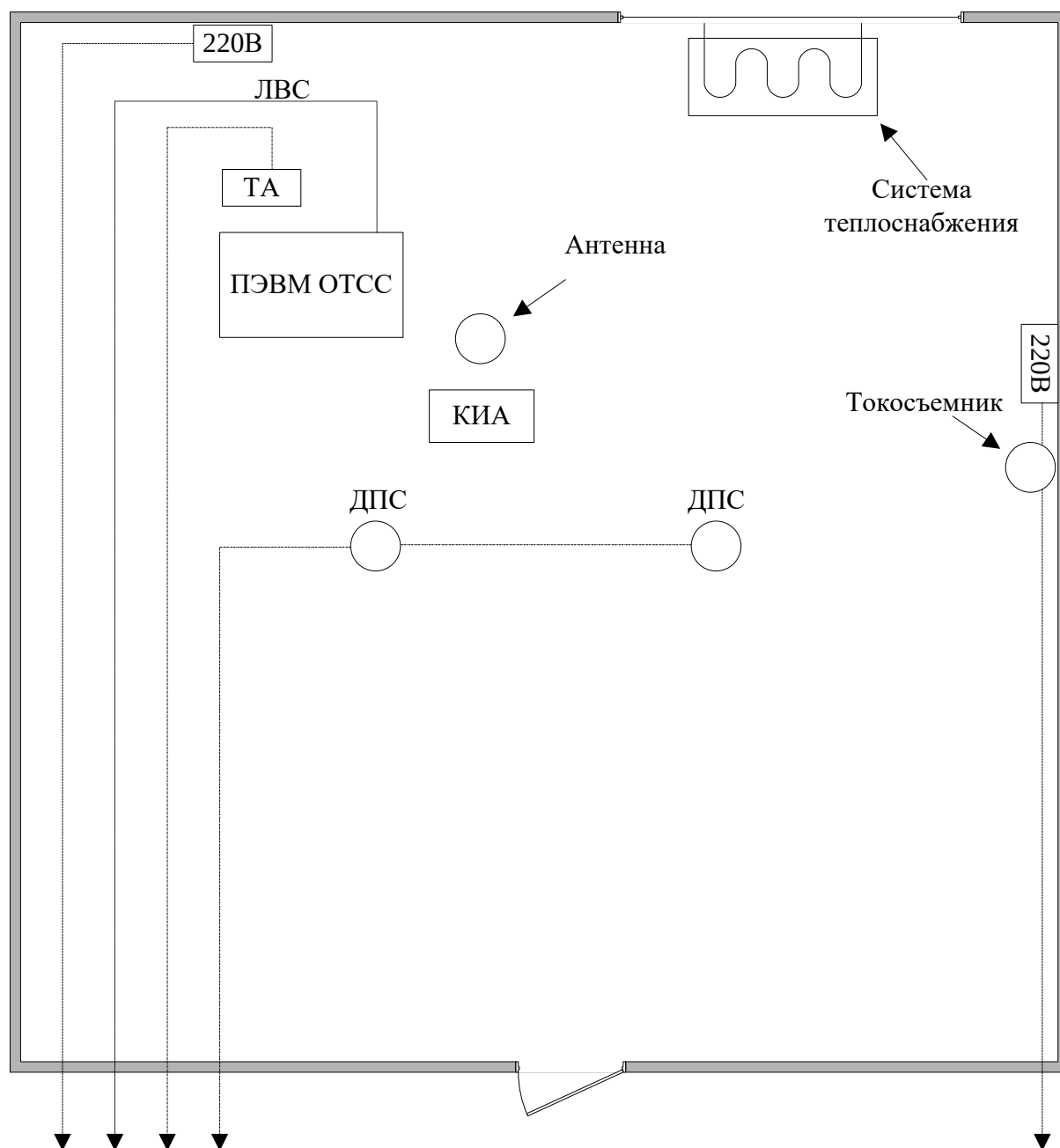
Расстояние до измерительной антенны – 1 м, канал «Е»

Таблица 3

№	F, МГц	Ус+п, дБ	Уп, дБ	Кпер, дБ	Есi, мкВ/м	Ешi, мкВ/м	R2, м
1	240,00	9,00	8,00	36,70	87,42	171,79	0,73
2	720,00	12,00	8,00	28,40	81,24	66,07	0,98
						Итог:	0,98

Сигналы вида OC3-OC5 в условиях объекта не обнаружены.

СХЕМА
проведения измерений



Приложение Д

(обязательное)

Протокол оценки защищенности конфиденциальной информации от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации, имеющие выход за пределы контролируемой зоны

Экз. № 1

УТВЕРЖДАЮ

Генеральный директор

11 ноября 2017 г.

ПРОТОКОЛ

оценки защищенности конфиденциальной информации, обрабатываемой ОТСС из состава автоматизированной системы на базе ПЭВМ (сер. № 16119497356016), расположенной в помещении № 3, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации, имеющие выход за пределы контролируемой зоны

1. Измерениям подвергались информативные сигналы от ОТСС из состава автоматизированной системы на базе ПЭВМ (сер. № 1...) (далее - АС), наведенные на совместно расположенные линии и коммуникации, выходящие за пределы контролируемой зоны (КЗ).

Состав ОТСС и ВТСС приведен в таблицах 1-2.

Таблица 1

№ п/п	Наименование ОТСС	Тип, модель	Серийный (заводской) номер
1.	Системный блок ПЭВМ в составе:	InWin	16119497356016
	- НЖМД	Seagate ST3120026A	3FN65PTF
	- DVD-ROM	Toshiba Samsung SD-M1912	68MA433632
2.	Монитор	Samsung 730BF	WM55XXXXX857629B
3.	Клавиатура	Mitsumi KFK-EA4XT	90LMFAO5CX5GMC8150*9291
4.	Манипулятор «мышь»	Logitech M-SBF90	XDB1285738
5.	Сканер	Epson J241A	FPDA979787

Таблица 2

№ п/п	Наименование ВТСС	Тип, модель	Серийный (заводской) номер
1.	Телефонный аппарат	Atlinks FS29169GE2-C	29911734
2.	Датчик пожарной сигнализации (2 шт.)	-	б/н

К таким линиям и коммуникациям на объекте применения АС относятся телефонная линия, сеть электропитания (~380/220 В), и система теплоснабжения.

Поскольку контур заземления расположен в пределах КЗ, то система заземления как канал утечки не рассматривается и проведение оценки защищенности не требуется.

Поскольку аттестуемая АС подключена к учрежденческой ЛВС через межсетевой экран к серверному и коммутационному оборудованию и далее к каналу связи Internet, при этом магистраль канала связи с Internet выполнена оптоволоконным кабелем, то данный канал утечки не рассматривается и проведения оценки защищенности не требуется.

Поскольку, линия пожарной сигнализации на объекте не имеет выхода за пределы КЗ, то данный канал утечки не рассматривается и проведения оценки защищенности не требуется.

2. Работы проводились в ноябре 2017 года.

При проведении оценки защищенности информации использовались нормативные и методические документы в области аттестации автоматизированных систем.

3. Измерения проводились с применением средств измерений, приведенных в таблице 3.

Таблица 3

№ п/п	Наименование	Тип, модель	Серийный номер	Дата поверки
1.	Анализатор спектра			
2.	Генератор сигналов			
3.	Генератор сигналов			
4.	Осциллограф (с многофункциональным пробником)			
5.	Антенна измерительная			
6.	Антенна измерительная			

4. Уровни наведенных опасных сигналов (ОС) измерялись в исследуемых линиях на частотах обнаружения информативных сигналов в диапазоне частот 0,1 - 250 МГц посредством подключения к ним с помощью измерительных токосъемников, подсоединяемых к входу контрольно-измерительной аппаратуры.

В качестве тестов использовались сигналы, создаваемые специализированной программой, удовлетворяющие требованиям ГОСТ 29339-92.

Схема размещения технических средств (ОТСС и ВТСС), средств защиты и линий, имеющих выход за пределы КЗ, а также места подключения измерительного оборудования приведена в приложении настоящего Протокола.

Результаты измерений наведенного информативного сигнала и расчета значений требуемой длины линий (коммуникаций) в пределах КЗ (R_i , м) приведены в таблицах №№ 1-9 приложения к настоящему протоколу. Защищенность информации, обрабатываемой на данной АС, определяется сигналами вида ОС1, ОС2 и ОС6. Сводные данные по результатам расчета для данных сигналов приведены в таблице 4.

Таблица 4

Вид ОС	Р _т , МГц	Ус+ш, дБ	Уш _т , дБ	Кп, дБ/м	Р _и , м	Р _{кз} , м	Соответствие (Р _и <Р _{кз})
Сеть электропитания							
ОС1	44,55	10	8	2,3043	3,33	>30	соответствует
ОС2	25	13	8	2,025	1,65	>30	соответствует
ОС6	240	13	8	2,46	1,36	>30	соответствует
Система теплоснабжения							
ОС1	44,55	9	8	2,3043	1,79	>15	соответствует
ОС2	25	12	8	2,025	0,89	>15	соответствует
ОС6	240	12	8	2,46	0,73	>15	соответствует
Телефонная линия							
ОС1	44,55	9	8	0,2227	18,55	>30	соответствует
ОС2	25	12	8	0,185	9,7	>30	соответствует
ОС6	240	12	8	0,24	7,48	>30	соответствует

Для сигналов вида ОС1, ОС2 и ОС6 расчетные значения длин пробегов отходящих линий (коммуникаций) (R_и) не превышают фактических длин пробегов отходящих линий (коммуникаций) (R_{кз}).

Вывод. Защищенность конфиденциальной информации, обрабатываемой ОТСС из состава АС, от ее утечки за счет наводок информативного сигнала в отходящие линии обеспечивается.

Дополнительных мер по защите информации не требуется.

Аттестационная комиссия:

Руководитель аттестационной комиссии:

Члены аттестационной комиссии:

РЕЗУЛЬТАТЫ ИЗМЕРЕНИЙ И РАСЧЕТОВ

Сигналы монитора (ОС1)

F_т = 54 МГц

Разрешение – 1280x1024, 60 Гц

Тип кодирования – последовательное

Сигнал – импульсный

Сеть электропитания

Таблица 1

№	F, МГц	Ус+п, дБ	Уп, дБ	Кпер, дБ	Кпi, дБ	Ri, м	Соответствие
1	270	10,00	8,00	-3,00	2,3043	3,33	соответствует
Итог:					Ri, м	3,33	соответствует

Система теплоснабжения

Таблица 2

№	F, МГц	Ус+п, дБ	Уп, дБ	Кпер, дБ	Кпi, дБ	Ri, м	Соответствие
1	270	9,00	8,00	-3,00	2,3043	1,79	соответствует
Итог:					Ri, м	1,79	соответствует

Телефонная линия

Таблица 3

№	F, МГц	Ус+п, дБ	Уп, дБ	Кпер, дБ	Кпi, дБ	Ri, м	Соответствие
1	270	9,00	8,00	-3,00	0,2227	18,55	соответствует
Итог:					Ri, м	18,55	соответствует

Сигналы НЖМД (ОС2)

F_т = 25 МГц

Тип кодирования – последовательное

Сигнал – импульсный

Сеть электропитания

Таблица 4

№	F, МГц	Ус+п, дБ	Уп, дБ	Кпер, дБ	Кпi, дБ	Ri, м	Соответствие
1	125,00	13,00	8,00	-6,20	2,025	1,65	соответствует
Итог:					Ri, м	1,65	соответствует

Система теплоснабжения

Таблица 5

№	F, МГц	Ус+п, дБ	Уп, дБ	Кпер, дБ	Кпi, дБ	Ri, м	Соответствие
1	125,00	12,00	8,00	-6,20	2,025	0,89	соответствует
Итог:					Ri, м	0,89	соответствует

Телефонная линия

Таблица 6

№	F, МГц	Ус+п, дБ	Уп, дБ	Кпер, дБ	Кпi, дБ	Ri, м	Соответствие
1	125,00	12,00	8,00	-6,20	0,185	9,70	соответствует
Итог:					Ri, м	9,70	соответствует

Сигналы USB-интерфейса (ОС6)

F_т = 240 МГц

Тип кодирования – последовательное

Сигнал – импульсный

Сеть электропитания

Таблица 7

№	F, МГц	Ус+п, дБ	Уп, дБ	Кпер, дБ	Кпi, дБ	Ri, м	Соответствие
1	240,00	13,00	8,00	-3,00	2,46	1,36	соответствует
Итог:					Ri, м	1,36	соответствует

Система теплоснабжения

Таблица 8

№	F, МГц	Ус+п, дБ	Уп, дБ	Кпер, дБ	Кпi, дБ	Ri, м	Соответствие
1	240,00	12,00	8,00	-3,00	2,46	0,73	соответствует
Итог:					Ri, м	0,73	соответствует

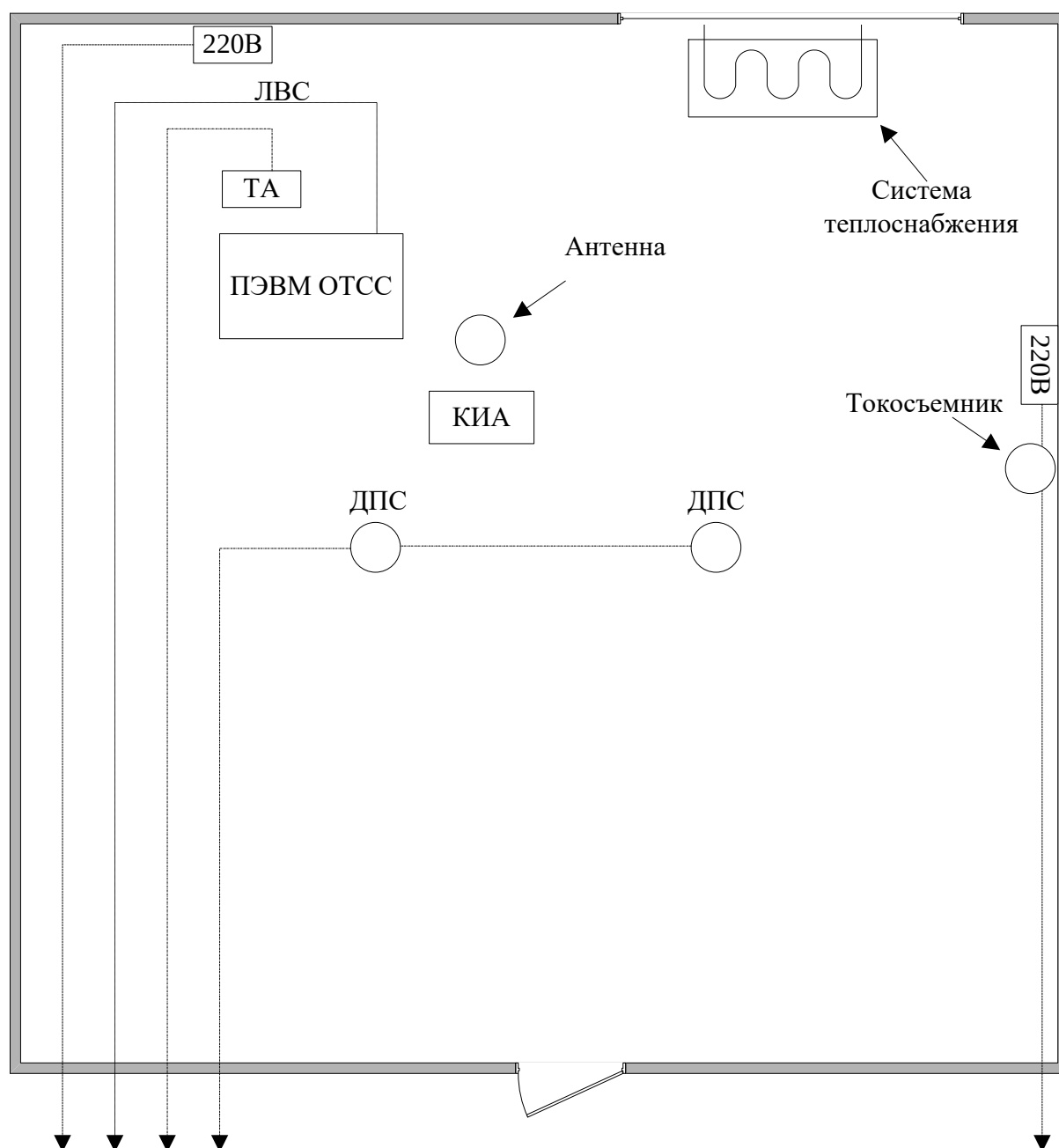
Телефонная линия

Таблица 9

№	F, МГц	Ус+п, дБ	Уп, дБ	Кпер, дБ	Кпi, дБ	Ri, м	Соответствие
1	240,00	12,00	8,00	-3,00	0,24	7,48	соответствует
Итог:					Ri, м	7,48	соответствует

Сигналы вида ОСЗ-ОС5 в условиях объекта не обнаружены.

СХЕМА проведения измерений



Приложение Е

(обязательное)

Предписание на эксплуатацию АС

Экз. № 1

УТВЕРЖДАЮ

Генеральный директор

12 ноября 2017 г.

П Р Е Д П И С А Н И Е

на эксплуатацию автоматизированной системы на базе автономной
ПЭВМ (сер. № ...), расположенную в помещении № 3

2017

135

1. Настоящее предписание распространяется на автоматизированную систему на базе автономной ПЭВМ (сер. № ...) (далее - АС), расположенную в помещении № 3.

2. Перечень технических средств (ОТСС и ВТСС) приведен в таблицах 1-2.

Таблица

1

№ п/п	Наименование ОТСС	Тип, модель	Серийный (заводской) номер
1.	Системный блок ПЭВМ в составе:	InWin	16119497356016
	- НЖМД	Seagate ST3120026A	3FN65PTF
	- DVD-ROM	Toshiba Samsung SD-M1912	68MA433632
2.	Монитор	Samsung 730BF	WM55XXXXX857629B
3.	Клавиатура	Mitsumi KFK-EA4XT	90LMFAO5CX5GMC8150*9291
4.	Манипулятор «мышь»	Logitech M-SBF90	XDB1285738
5.	Сканер	Epson J241A	FPDA979787

Таблица

2

№ п/п	Наименование ВТСС	Тип, модель	Серийный (заводской) номер
1.	Телефонный аппарат	Atlinks FS29169GE2-C	29911734
2.	Датчик пожарной сигнализации (2 шт.)	-	б/н

3. Для обеспечения защиты конфиденциальной информации, обрабатываемой на АС, от ее утечки по каналам ПЭМИН необходимо:

3.1. Использовать в составе АС технические средства, перечень которых приведен в таблицах 1-2 настоящего Предписания, при этом уровень обрабатываемой информации на ОТСС из состава АС не должен превышать «КОНФИДЕНЦИАЛЬНО».

3.2. Обеспечить размер контролируемой зоны (КЗ) вокруг ОТСС радиусом не менее 3 метров. План размещения технических средств в помещении размещения АС приведен на рис. 1 настоящего предписания.

3.3. Эксплуатировать видеомонитор из состава ОТСС в штатном режиме работы (разрешение экрана 1280x1024, 60 Гц).

3.4. Электропитание осуществлять от промышленной электросети, при этом протяженность магистрали сети электропитания в пределах КЗ объекта должна быть не менее 5 метров.

3.5. Специальных требований к заземлению ОТСС объекта не предъявляется.

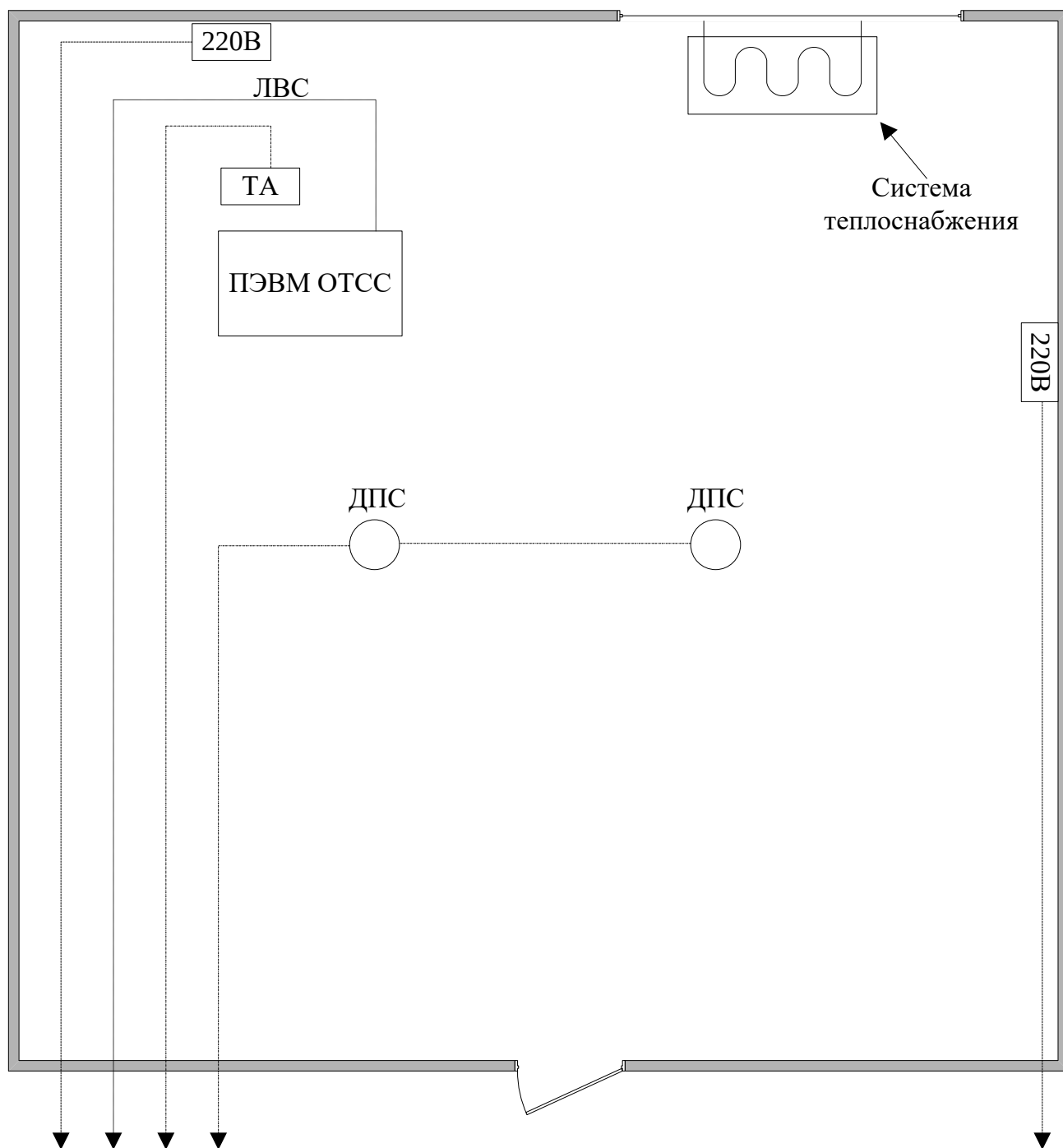
3.6. **Запрещается:**

–вносить изменения в состав и размещение технических средств (ОТСС, ВТСС) АС, а также в схемы прокладки магистралей проводов и кабелей ВТСС;

–обрабатывать конфиденциальную информацию с открытым кожухом системного блока ПЭВМ (сер. № ...);

–вести в помещении размещения АС переговоры конфиденциального характера.

ПЛАН
размещения технических средств в помещении № 39



Аттестационная комиссия:
Руководитель аттестационной комиссии:
Члены аттестационной комиссии:

Приложение Ж

(обязательное)

Заключение по результатам проведения аттестационных испытаний

АС

Экз. № 1

УТВЕРЖДАЮ

Генеральный директор

12 ноября 2017 г.

ЗАКЛЮЧЕНИЕ

по результатам проведения аттестационных испытаний автоматизированной системы на базе автономной ПЭВМ (сер. №), расположенной в помещении № 3, на соответствие требованиям по безопасности информации

2017

Принятые сокращения

АС	- автоматизированная система
НСД	- несанкционированный доступ
ОТСС	- основные технические средства и системы
ВТСС	- вспомогательные технические средства и системы
ПЭМИН	- побочные электромагнитные излучения и наводки
РД	- руководящий документ
СЗИ	- система защиты информации
КЗ	- контролируемая зона

1. Условия и порядок проведения аттестационных испытаний АС

Аттестационные испытания АС на базе автономной ПЭВМ (сер. № ...) проводились в соответствии с «Программой и методиками...».

Испытания АС проведены в ноябре 2017 года.

При проведении аттестационных испытаний применялись следующие методы проверок и испытаний:

- экспертно-документальный метод;
- инструментальная оценка защищенности информации, обрабатываемой ОТСС из состава АС, от её утечки по каналам ПЭМИН;
- проверка функций или комплекса функций защиты информации от несанкционированного доступа (НСД).

Испытания проводились в соответствии с требованиями следующих руководящих и методических документов:

- Закон Российской Федерации «О безопасности» № 2446-1 от 05.03.1992;
- Федеральный Закон «Об информации, информационных технологиях и защите информации» № 149-ФЗ от 27.07.2006;
- «Положение по аттестации объектов информатизации по требованиям безопасности информации», Гостехкомиссия России, 1994;

2. Состав средств контроля, использованных при аттестационных испытаниях АС в части защиты от НСД

Для контроля защищенности АС от НСД в ходе аттестационных испытаний использовались сертифицированные ФСТЭК России программные средства контроля эффективности применения СЗИ:

- средство создания модели системы разграничения доступа «Ревизор 1 ХР», имеющая сертификат № 989 от 08.02.2005 г., выданный ФСТЭК России и лицензию на право использования.
- программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 ХР», имеющая сертификат № 990 от 08.02.2005 г., выданный ФСТЭК России.
- программа фиксации и контроля исходного состояния программного комплекса «ФИКС» версия 2.0.2, имеющая сертификат № 1548 от 15.01.2008 г., выданный ФСТЭК России и лицензию на право использования.

- программа поиска и гарантированного уничтожения информации на дисках «Terrier 3.0», имеющая сертификат № 1193 от 16.05.2006 г., выданный ФСТЭК России и лицензию на право использования.
- система анализа программного и аппаратного обеспечения TCP/IP сетей (сетевой сканер) «Ревизор Сети» версии 3.0, имеющая сертификат № 3413 от 02.06.2015 г., выданный ФСТЭК России и лицензию на право использования.
- сетевой сканер «Nessus 3.0.3».

3. Условия эксплуатации АС и ее состав

АС расположена в помещении № 3 по адресу: г. Пенза.

Состав технических средств (ОТСС и ВТСС), СЗИ и используемого программного обеспечения АС представлен в таблицах 1-4.

Таблица 1

№ п/п	Наименование ОТСС	Тип, модель	Серийный (заводской) номер
1.	Системный блок ПЭВМ в составе:	InWin	16119497356016
	- НЖМД	Seagate ST3120026A	3FN65PTF
	- DVD-ROM	Toshiba Samsung SD-M1912	68MA433632
2.	Монитор	Samsung 730BF	WM55XXXXX857629B
3.	Клавиатура	Mitsumi KFK-EA4XT	90LMFAO5CX5GMC8150*9291
4.	Манипулятор «мышь»	Logitech M-SBF90	XDB1285738
5.	Сканер	Epson J241A	FPDA979787

Таблица 2

№ п/п	Наименование ВТСС	Тип, модель	Серийный (заводской) номер
1.	Телефонный аппарат	Atlinks FS29169GE2-C	29911734
2.	Датчик пожарной сигнализации (2 шт.)	-	б/н

Таблица 3

№ п/п	Наименование СЗИ	Заводской номер	Номер знака соответствия	Сведения о сертификате	Место и дата установки
1.	Secret Net Studio 8.0	KLTRCP7	М 673056	сертификат ФСТЭК России № 3675 от 12.12.2016 г., действителен до 12.12.2019 г.	ПЭВМ, сер. № 11458720921807, 01.11.2017
2.	Kaspersky Endpoint Security 10 для Windows	СМП8877-2387	Л 729365	сертификат ФСТЭК России № 3025 от 25.11.2013 г., действителен до 25.11.2019 г.	ПЭВМ, сер. № 23678912459490, 01.11.2017

Таблица 4

№ п/п	Наименование ПО
1.	ОС Microsoft Windows 7 Профессиональная SP1 x32, лиц. №
2.	Пакет офисных приложений Microsoft Office 2010, лиц. № в составе: Word, Excel
3.	Почтовая программа Mozilla Thunderbird 52.2.0, свободно-распространяемое ПО
4.	Программа чтения файлов в формате pdf Foxit Reader 7.3.6.321, свободно-распространяемое ПО
5.	Программа работы со сканером Epson Scan, свободно-распространяемое ПО
6.	СКЗИ КриптоПро CSP 3.9, лиц. №
7.	Антивирусная программа Касперского 10 (Kaspersky Endpoint Security 10 для Windows), лицензия
8.	СЗИ от НСД «Secret Net Studio 8.0» (редакция: Постоянная защита), лиц. №

4. Результаты аттестационных испытаний АС

4.1. Результаты проверки состояния технологического процесса обработки конфиденциальной информации на АС.

Технологический процесс обработки конфиденциальной информации на АС, описан внутренними организационно-распорядительными документами, соответствует реальной практике и требованиям нормативно-методических документов.

Носитель, предназначенный для обработки и хранения конфиденциальной информации (НЖМД), зарегистрирован в соответствующем подразделении, использующем данный носитель информации, в соответствии с требованиями локальных нормативных актов.

4.2. Результаты проверки АС на соответствие организационно-техническим требованиям по ЗИ.

При проведении испытаний аттестационной комиссией были представлены следующие документы и исходные данные:

- приказ о назначении администратора безопасности;
- акт классификации автоматизированной системы;
- перечень сведений конфиденциального характера, подлежащих защите;
- разрешительная система доступа к информационным ресурсам автоматизированной системы;
- описание технологического процесса обработки информации в автоматизированной системе;
- инструкция администратору безопасности АС;
- инструкция по работе пользователей АС;
- инструкция по проведению антивирусного контроля;
- список лиц, имеющих право доступа в помещение № 3.

– протокол оценки защищенности ОТСС автоматизированной системы на базе автономной ПЭВМ (сер. № ...), расположенной в помещении № 3, от утечки конфиденциальной информации по каналу ПЭМИ;

– протокол контроля защищенности конфиденциальной информации, обрабатываемой ОТСС автоматизированной системы на базе автономной ПЭВМ (сер. № ...), расположенной в помещении № 3, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации, имеющие выход за пределы контролируемой зоны;

– предписание на эксплуатацию автоматизированной системы на базе автономной

ПЭВМ (сер. № ...), расположенной в помещении № 3;

- протокол испытаний комплексной системы защиты информации автоматизированной системы на базе автономной ПЭВМ (сер. № ...), расположенной в помещении № 3, на соответствие требованиям по безопасности информации в части защиты от НСД и компьютерных вирусов.

Перечень подготовленных документов является достаточным для проведения аттестационных испытаний АС.

Содержание представленных документов и их оформление соответствует установленным требованиям.

Ответственность за организацию работ в АС, ее эксплуатацию, а также за выполнением требований по защите информации определена внутренней организационно-распорядительной документацией. Назначен администратор безопасности.

Сотрудники, участвующие в использовании и обслуживании АС, в вопросах защиты конфиденциальной информации и требованиях, предъявляемых к эксплуатации АС, подготовлены в достаточной степени.

Вывод: аттестуемая АС соответствует организационно-техническим требованиям, предъявляемым к АС, обрабатывающим конфиденциальную информацию.

4.3. Результаты испытаний АС на соответствие требованиям по защите информации от утечки по каналам ПЭМИН.

Оценка защищенности информации от ее утечки за счет ПЭМИН была проведена инструментально – расчетным методом в соответствии с временными методиками ФСТЭК России от 2001 года.

По результатам проведенных работ составлены протоколы оценки защищенности информации, обрабатываемой на АС, которые содержат:

- результаты измерений уровней ПЭМИ от ОТСС;
- результаты расчетов контролируемой зоны;
- результаты оценки защищенности АС от утечки конфиденциальной информации за счет наводок информативного сигнала на линии (коммуникации), выходящие за пределы контролируемой зоны.

На основании результатов расчетов выдано предписание на эксплуатацию АС.

При проведении работ использовалась контрольно – измерительная аппаратура и тестовые программы в соответствии с рекомендациями методических документов ФСТЭК России.

Электропитание ОТСС объекта осуществляется от трансформаторной подстанции, расположенной за пределами КЗ.

Заземление ОТСС объекта осуществляется на контур заземления, расположенный в пределах КЗ.

Инженерные коммуникации, к которым относится система теплоснабжения здания, в том числе помещение размещения АС, имеют выход за пределы КЗ.

Линия системы пожарной сигнализации выведена на пульт дежурного, расположенный в пределах единой КЗ.

Телефонная линия, заведенная в помещение № 39, имеет выход за пределы КЗ.

Аттестуемая АС подключена к учрежденческой ЛВС через межсетевой экран к серверному и коммутационному оборудованию и далее к каналу связи Internet, при этом магистраль канала связи с Internet выполнена оптоволоконным кабелем.

Расчетный размер КЗ от оборудования АС составляет 1,13 метра, что не превышает фактический размер КЗ – 12 метров.

Вывод: Защищенность обрабатываемой информации на АС от утечки за счет ПЭМИН обеспечивается, дополнительных средств защиты не требуется.

4.4. Результаты испытаний АС на соответствие требованиям по ЗИ от НСД.

При испытании СЗИ от НСД рассматривалось ее соответствие требованиям нормативно- методических документов по защите конфиденциальной информации в части НСД, проводился контроль работоспособности систем управления доступом, регистрации и учета, обеспечения целостности. Проводился анализ, и оценка технологического процесса обработки информации в части НСД.

АС располагается в помещении № 3, дверь оборудована замком. Окно помещения № 3 оборудовано жалюзи.

Режим работы пользователей в АС - коллективный. Пользователи имеют различные права доступа (полномочия) к информации, обрабатываемой и хранимой на АС и носителях информации. Хранение конфиденциальной информации в АС - на жестком магнитном диске (ЖМД) и сменных машинных носителях информации (МНИ) осуществляется в соответствии с внутренней организационно-распорядительной документацией. В соответствии с классификационными признаками, установленными РД «Автоматизированные системы. Защита информации от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» АС относится к классу защищенности 1Г.

Проведенный контроль настроек СЗИ от НСД показал их соответствие требованиям нормативно-методических документов по защите конфиденциальной информации в части НСД, при этом требования РД «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации», РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» в аттестуемой АС выполняются.

Проведенный анализ технологического процесса обработки информации показал, что требования руководящих, нормативных и методических документов по защите конфиденциальной информации выполняются. При соблюдении требований организационно-режимной документации и установленного технологического процесса обработки информации в АС защита конфиденциальной информации от раскрытия, нарушения целостности и блокирования обеспечивается.

Вывод: АС соответствует требованиям нормативно-методических документов по защите конфиденциальной информации от НСД.

Заключение. Требования нормативно-методических документов по защите конфиденциальной информации, обрабатываемой в АС на базе автономной ПЭВМ (сер. № ...), расположенной в помещении № 3, выполняются.

Защита конфиденциальной информации, обрабатываемой в АС, от её раскрытия, нарушения целостности и блокирования обеспечивается.

Комиссия считает возможным выдать «Аттестат соответствия» на АС (автономная ПЭВМ сер. № ...) с разрешением обработки и хранения конфиденциальной информации сроком на 3 года.

Аттестационная комиссия:

Руководитель аттестационной комиссии:

Члены аттестационной комиссии:

Приложение И

(обязательное)

Аттестат соответствия требованиям безопасности информации

Экз. № 1

УТВЕРЖДАЮ

Генеральный директор

12 ноября 2017 г.

АТТЕСТАТ СООТВЕТСТВИЯ

требованиям по безопасности информации

автоматизированной системы на базе автономной ПЭВМ (сер. № ...),
расположенной в помещении № 3

Выдан 12 ноября 2017 г.

1. Настоящим АТТЕСТАТОМ удостоверяется, что автоматизированная система на базе автономной ПЭВМ (сер. № ...), класс защищенности – 1Г, соответствует требованиям нормативной документации по безопасности информации.

Состав комплекса технических средств автоматизированной системы (АС) с указанием заводских номеров, модели, изготовителя, номеров сертификатов соответствия, схема размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств, а также средств защиты (с указанием изготовителя и номеров сертификатов соответствия) указаны в «Техническом паспорте на АС...».

Организационная структура и уровень подготовки специалистов обеспечивают поддержание уровня защищенности АС в процессе эксплуатации в соответствии с установленными требованиями.

2. Аттестация АС выполнена в соответствии с «Программой и методиками аттестационных испытаний...», утвержденными руководителем органа по аттестации.

3. С учетом результатов аттестационных испытаний в АС разрешается обработка конфиденциальной информации.

4. При эксплуатации АС запрещается:

- вносить изменения в комплектность АС, которые могут снизить уровень защищенности информации;
- проводить обработку защищаемой информации без выполнения всех мероприятий по защите информации;
- подключать к основным техническим средствам нештатные блоки и устройства;
- вносить изменения в состав, конструкцию, конфигурацию, размещение средств вычислительной техники;
- допускать к обработке защищаемой информации лиц, не оформленных в установленном порядке;
- производить копирование защищаемой информации на неучтенные носители информации, в том числе для временного хранения информации;
- работать при отключенном заземлении ОТСС;
- обрабатывать на ПЭВМ защищаемую информацию при обнаружении каких-либо неисправностей;
- осуществлять другие технические и организационные мероприятия, которые могут создать предпосылки для утечки защищаемой информации за счет ПЭМИН и несанкционированного доступа к информации.

6. Контроль за эффективностью реализованных мер и средств защиты возлагается на ответственного (администратора) по защите информации.

7. Результаты аттестационных испытаний приведены в «Заключении аттестационной комиссии...», от 11.11.2017 г., и протоколах испытаний 11.11.2017 г.

8. «Аттестат соответствия» выдан на 3 года, в течение которых должна быть обеспечена неизменность условий функционирования АС и технологии обработки защищаемой информации, могущих повлиять на характеристики защищенности АС.

Руководитель аттестационной комиссии

Генеральный директор

»

12 ноября 2017 г.

Приложение К

(обязательное)

Протокол проверки на оригинальность в системе «Антиплагиат.ВУЗ»