Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Институт открытого и дистанционного образования
Кафедра Техники, технологий и строительства

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____К.М. Виноградов
_____2020 г.

Проектирование системы обработки коммерческой информации

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ– 09.03.01.2020.162.ПЗ ВКР

Руководитель работы,
старший преподаватель
_____С.Н. Кононов
_____2020 г.

Автор работы
студент группы ДО – 525
_____Ю.А. Митрофанова
_____2020 г.

Нормоконтролер,
преподаватель
_____О.С. Микерина
_____2020 г.

Челябинск 2020

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Институт открытого и дистанционного образования

Направление 09.03.01 Информатика и вычислительная техника
Кафедра Техники, технологий и строительства

УТВЕРЖДАЮ
Зав. кафедрой
_____ /Виноградов К.М./
_____2020 г.

ЗАДАНИЕ

на выпускную квалификационную работу студентки

Митрофановой Юлии Азатовны

Группа ДО-525

1 Тема работы: Проектирование системы обработки коммерческой информации

утверждена приказом ректора от «___»_____ 2020 г. №_____

2 Срок сдачи студентом законченной работы __июня 2020 г.

3 Исходные данные к работе

3.1 Изучение классификации угроз безопасности

3.2 Нормативные акты РФ по защите информации

3.3 Схема офисов коммерческой организации

3.4 Определение количества необходимых рабочих мест и обрабатываемой на них информации

3.5 Техническое описание активного сетевого оборудования

3.6 Материал преддипломной практики

4 Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов)

4.1 Теоретическое обоснование темы исследования

4.1.1 Достижения информационных технологий России и зарубежных аналогов в защите обрабатываемых данных

4.1.2 Классификация СВТ и АС

4.1.3 Модель ISO OSI

4.2 Постановка задачи

4.2.1 Изучение классификации угроз безопасности

4.2.2 Выбор средств обработки и классов защиты

4.2.3 Подбор средств для организации сети и настройка доступа согласно выбранного класса защиты

5 Перечень графического материала

1 Пояснительная записка на 50–70 листах формата А4.

2 Презентация на 10–12 слайдах

Дата выдачи задания 27 января 2020 г.

Руководитель _____ Кононов С.Н.
(подпись)

Задание принял к исполнению _____ Митрофанова Ю.А.
(подпись студента)

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы	Срок выполнения этапов работы	Отметка о выполнении
Введение	24.02 –09.03	
Теоретическое обоснование темы исследования	10.03 –25.03	
Достижения информационных технологий России и зарубежных аналогов в защите обрабатываемых данных	26.03 – 05.04	
Классификация СВТ и АС	06.04 – 11.04	
Модель ISO OSI	12.04 –21.04	
Анализ и обоснование проектных решений	22.04 –30.04	
Изучение классификации угроз безопасности	01.05 – 10.05	
Выбор средств обработки и классов защиты	11.05 –15.05	
Подбор средств для организации сети и настройка доступа согласно выбранного класса защиты	16.05 –19.05	
Нормативные акты РФ по защите информации	20.05 –24.05	
Разработка схемы офисов организации	25.05 –26.05	
Разработка необходимых рабочих мест и обрабатываемой на них информации	27.05 –05.06	
Техническое описание активного сетевого оборудования	06.06 –09.06	
Заключение	10.06 –11.06	

Зав. кафедрой _____/К.М. Виноградов/
(подпись)

Руководитель работы _____/С.Н. Кононов/
(подпись)

Студент-дипломник_____/Ю.А. Митрофанова/
(подпись)

АННОТАЦИЯ

Митрофанова, Ю.А. Проектирование системы обработки коммерческой информации. – Челябинск: ФГАОУ ВО «ЮУрГУ (НИУ)», ИОДО; 2020, 47 с., 11 ил., библиографический список – 43 наименования, презентация на 13 слайдах.

В выпускной квалификационной работе проведен анализ классификации угроз информационной безопасности и нормативных актов по защите информации. Произведен анализ и сравнение отечественных и передовых зарубежных технологий и решений в области. Рассмотрены вопросы создания системы обработки коммерческой информации.

Определен состав необходимых рабочих мест, предложена схема размещения и способ их соединения. Предложен вариант настройки доступа согласно выбранному классу защиты для обрабатываемой информации, подобрана операционная система и совместимое с ней сетевое оборудование.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы.

В настоящее время в России все больше внимания уделяется сфере бизнеса. Люди, обладающие знаниями в этой области, стараются организовать свои коммерческие предприятия, целью которых является получение коммерческой выгоды. Любая такая организация функционирует в рамках сложной окружающей среды, в которую входят конкуренты, партнеры, общественные и государственные органы. Функционирование и развитие коммерческой организации не возможно без использования информационных технологий.

Любая деятельность коммерческой фирмы включает обработку, хранение, получение информации. С обеспечением сохранности коммерческой информации на рыночно – конкурентных условиях возникает основная масса проблем. Информация, которая используется для достижения поставленных целей, считается более ценной для владельца, поэтому ее разглашение может ослабить возможность конкурента в достижении поставленных целей и может принести доход ее новым обладателям. Поэтому именно информация, создающая угрозы, нуждается в защите. В связи с этим все большее значение приобретает разработка новейших методов реализации защиты и организация эффективной системы информационной безопасности.

Постоянный анализ обеспечения информационной безопасности позволяет определять ее основные направления для реализации. Обеспечение информационной безопасности является важнейшей и обязательной составляющей безопасности страны.

Цель работы – создание системы обработки коммерческой информации.

Задачи работы:

– изучить опыт отечественных и зарубежных разработчиков информационной безопасности;

– изучить классификацию угроз информационной безопасности, средств вычислительной техники и автоматизированных систем;

– подобрать соответствующий теоретический материал;

– подобрать средства для организации сети.

Объект работы – законодательство РФ и подзаконные акты в области защиты данных.

Предмет работы – план помещений, в которых ведётся обработка данных, список планируемых рабочих мест и перечисление обрабатываемой информации.

Практическая значимость выпускной квалификационной работы состоит в осуществлении желания заказчика ознакомиться с возможностями реализации системы обработки коммерческой информации.

Структура выпускной квалификационной работы состоит из введения, трех разделов, заключения и библиографического списка. Раздел 1 посвящен изучению классификации угроз информационной безопасности, средств вычислительной техники, автоматизированных систем и системам обработки информации. Раздел

2 посвящен теоретическому обоснованию темы исследования, описываются имеющиеся российские и зарубежные технологии и решения в области защиты информации. Раздел 3 посвящен анализу и обоснованию проектных решений.

Объем выпускной квалификационной работы составляет 47 страниц машинописного текста и содержит 11 иллюстраций, 2 таблицы, библиографический список из 43 наименований.

1 КЛАССИФИКАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СИСТЕМ ЕЕ ОБРАБОТКИ

Информационная безопасность Российской Федерации – одна из составляющих безопасности Российской Федерации в сферах жизнедеятельности общества и государства. Надежное обеспечение информационной безопасности является одной из ключевых задач формирования информационного общества.

Информационной безопасностью называют меры по защите информации от случайного или преднамеренного воздействия внешнего или внутреннего характера, грозящих нанесением ущерба пользователям и владельцам информации.

Принципы информационной безопасности

Вопросы защиты информации в информационных системах решаются для того, чтобы оградить нормально функционирующую информационную систему от доступа посторонних лиц, несанкционированных управляющих воздействий и программ к данным с целью хищения.

Обеспечение и поддержка информационной безопасности включают комплекс мер, которые отслеживают, предотвращают и ликвидируют несанкционированный доступ посторонних лиц. Также меры направлены на защиту от искажений, повреждений, блокировки или копирования информации. Полноценная и надежная защита обеспечивается только тогда, когда все задачи решаются одновременно.

1.1 Угрозы информационной безопасности

Угроза безопасности информационных систем подразделяются на реальные или потенциально возможные действия, которые способны изменить данные, хранящиеся в информационной системе, уничтожить или использовать их в целях, не предусмотренных регламентом заранее.

Знание угроз, а также уязвимых мест защиты, которые эти угрозы используют, необходимо для того, чтобы выбирать наиболее оптимальные средства обеспечения безопасности.

Реализации угрозы через имеющиеся факторы уязвимости называется «атакой», а тот, кто ее реализует, называется «злоумышленником».

Угрозы информационной безопасности классифицируются по признакам:

– по составляющим информационной безопасности, против которых в первую очередь направлены угрозы;

– по компонентам информационных систем, на которые угрозы нацелены;

– по характеру воздействия;

– по расположению источника угроз.

При анализе угроз информационной безопасности первым является определение составляющей информационной безопасности, которая может быть нарушена угрозой.

Угрозы по составляющим информационной безопасности – это доступность, целостность, конфиденциальность.

Доступность информации – главный аспект информационной безопасности и означает, что информация, которая находится в свободном доступе, должна предоставляться полноправным пользователям своевременно и беспрепятственно. Если получение этих услуг становится невозможным, это наносит ущерб всем субъектам информационных отношений.

Целостность информационных данных обеспечивает предотвращение умышленных изменений информации и означает способность информации сохранять изначальный вид и структуру как в процессе хранения, как и после неоднократной передачи. Только уполномоченные лица могут изменять или удалять информацию.

Конфиденциальность – один из самых сложных аспектов информационной безопасности в практической реализации. Конфиденциальность подразумевает ограничения полномочий доступа к информации для определенных пользователей. В процессе действий и операций информация становится доступной только пользователям, которые включены в информационные системы и успешно прошли идентификацию. Нарушения конфиденциальности называется «утечкой информации», которая возникает вследствие действий человека, сбоев в работе программных и аппаратных средств.

По характеру воздействия угрозы делятся на случайные или преднамеренные, действия природного или техногенного характера.

Причины случайных воздействий при эксплуатации:

– аварийные ситуации, произошедшие из-за стихийных бедствий;

– ошибки в программном обеспечении;

– неправомерное отключение оборудования или изменение режимов работы устройств и программ;

– ошибки в работе персонала, приводящие к частичному или полному отказу системы;

– помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это действия людей, носящие целенаправленный характер действий и чаще связанные с корыстными целями:

– несанкционированное копирование носителей информации;

– хищение носителей информации;

– незаконное получение паролей и реквизитов разграничения доступа;

– перехват данных, передаваемых по линиям связи;

– действия по дезорганизации функционирования системы.

Угрозы могут происходить как от внешних злоумышленников, так и от легальных пользователей сети.

Внешние угрозы обусловлены применением вычислительных сетей и созданием на их основе информационных систем.

Локальные угрозы предполагают проникновение и получение злоумышленником доступа к локальной сети или персональному компьютеру, а удаленные характерны для систем, подключенных к общедоступным глобальным сетям.

Основная особенность любой вычислительной сети состоит в том, что связь между компонентами, распределенными в пространстве, осуществляется физически с помощью сетевых соединений и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Информация, передающаяся по сетевым соединениям в таком виде, может подвергаться нападению, при этом местоположение злоумышленника будет неизвестно.

1.2 Классификация уязвимостей систем безопасности

Угрозы информационной безопасности проявляются не самостоятельно, а через возможное взаимодействие с наиболее слабыми звеньями системы защиты, то есть через факторы уязвимости.

Угроза приводит к нарушению деятельности систем на конкретном объекте – носителе.

Основные факторы уязвимости:

- несовершенство программного обеспечения, аппаратной платформы;
- разные характеристики строения автоматизированных систем в информационном потоке;
- часть процессов функционирования систем является неполноценной;
- неточность протоколов обмена информацией и интерфейса;
- сложные условия эксплуатации и расположения информации.

Чаще всего источники угрозы запускаются с целью получения незаконной выгоды вследствие нанесения ущерба информации. Но возможно и случайное действие угроз из-за недостаточной степени защиты и массового действия угрожающего фактора.

Классы уязвимостей:

– объективные;

– случайные;

– субъективные.

Если устранить или ослабить влияние уязвимостей, то можно избежать угрозы, направленной на систему хранения информации.

Непрерывность процесса обеспечения безопасности должна гарантировать борьбу с угрозами на всех этапах информационного цикла: сбора, хранения, обработки, использования и передачи информации.

1.3 Правовые основы защиты информации

Стремление оградить информацию от угроз лежит в основе создания систем информационной безопасности. В обеспечении информационной безопасности нуждаются четыре разные категории субъектов:

– государство в целом;

– государственные организации;

– коммерческие структуры;

– отдельные граждане.

Под защитой информации понимается:

– комплекс правовых мер;

– административных мер;

– организационно – технических мер, направленных на предотвращение реальных или предполагаемых угроз или на устранение последствий.

Первый уровень правовой охраны и защиты информации состоит из международных договоров о защите информации и государственной тайны, к которым присоединилась и Российская Федерация с целью обеспечения надежной информационной безопасности РФ.

Поддерживающее правовое обеспечение информационной безопасности нашей страны осуществляет Доктрина информационной безопасности Российской Федерации [42].

Доктрина – нормативно-методический документ, который представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

В Доктрине под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Доктрина служит основой для формирования государственной политики в области обеспечения информационной безопасности и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

Правовую основу Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

Правовое обеспечение информационной безопасности в Российской Федерации:

– Конституция РФ (статья 23 определяет право граждан на тайну переписки, телефонных, телеграфных и иных сообщений) [30];

– Уголовный кодекс РФ (статья 272 – определяет ответственность за неправомерный доступ к компьютерной информации; статья 273 – за создание, использование и распространение вредоносных программ для ЭВМ; статья 274 – за нарушение правил эксплуатации ЭВМ, систем и сетей) [31];

– Закон РФ «О государственной тайне» от 21 июля 1993 г. N 5485–1 [29];

– Федеральный закон РФ «О коммерческой тайне» от 29 июля 2004 г. N 98–ФЗ [35];

– Федеральный закон РФ «Об информации, технологиях и о защите информации» от 27 июля 2006 г. N 149–ФЗ [36]. Закон регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации.

– Федеральный закон РФ «О персональных данных» от 27 июля 2006 г. N 152–ФЗ [37]. Регулирует деятельность при обработке персональных данных, обеспечивает защиту прав и свобод человека. Конкретные нормы содержатся в приказе ФСТЭК от 18 февраля 2013 г. № 21 [41];

– Федеральный закон РФ «Об электронной подписи» от 06 апреля 2011 г. № 63–ФЗ [38].

Правовое обеспечение информационной безопасности в РФ находится на высоком уровне. Благодаря федеральному закону о защите информации, компании могут рассчитывать на защиту и правовую охрану информации, полную экономическую информационную безопасность.

На базе основополагающих нормативных актов разрабатываются ведомственные нормативные акты и постановления правительства, посвященные частным вопросам о защите информации.

Решения для защиты персональных данных в российских учреждениях и компаниях формируются на базе мер организационно-технического характера. Решения должны соответствовать нормам правовых актов и специальным требованиям регуляторов.

Функции регуляторов выполняют:

- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций – Роскомнадзор;
- Федеральная служба по техническому и экспортному контролю – ФСТЭК;
- Федеральная служба безопасности – ФСБ.

Роскомнадзор следит за исполнением законодательства, касающегося персональных данных в целом.

ФСТЭК – это федеральный орган исполнительной власти РФ, находящийся в подчинении у Министерства обороны.

Основные функции ФСТЭК – контроль над обеспечением безопасности информации, имеющей критическую важность для существования и правильного функционирования нашего государства, борьба с техническими разведками других государств на территории страны, контроль экспорта товаров двойного назначения и товаров, ограниченных в международном обороте при внешнеэкономической деятельности.

ФСТЭК и ФСБ формируют требования к методологическим, техническим и организационным условиям защищенности информационных систем обработки персональных данных.

Помимо правовых документов, в Российской Федерации действуют нормативно-методические документы:

– методические документы государственных органов России: документы Федеральной службы по техническому и экспортному контролю, ведомственные приказы;

– стандарты информационной безопасности: международные стандарты, Государственные стандарты РФ, рекомендации по стандартизации, методические указания.

В целом развитие законодательной базы в области информационной безопасности идет по четырем основным направлениям:

– защита сведений, составляющих государственную тайну;

– защита конфиденциальной информации;

– защита авторского права в сфере информатизации;

– защита права на доступ к информации.

1.4 Объекты защиты в концепциях информационной безопасности

Различие в субъектах порождает различия в объектах защиты. Основные группы объектов защиты:

– информационные ресурсы всех видов (жесткий диск, любой носитель информации, документ с данными и реквизитами);

– права граждан, организаций и государства на доступ к информации, возможность получить ее в рамках закона;

– система создания, использования и распространения данных;

– система формирования общественного сознания.

Каждый из объектов предполагает особую систему мер защиты от угроз информационной безопасности и общественному порядку.

Обеспечение информационной безопасности в каждом случае должно опираться на системный подход, учитывающий специфику объекта.

Российская правовая система и сложившиеся общественные отношения классифицируют информацию по критериям доступности. Это позволяет уточнить существенные параметры, необходимые для обеспечения информационной безопасности:

– информация ограниченного доступа и использования, то есть содержащая сведения, составляющие определенный вид тайны и подлежащие защите, охране, наблюдению (в соответствии с Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 06 марта 1997 г. № 188.) [32];

– общедоступная открытая информация, используемая в работе без специального разрешения и публикуемая в средствах массовой информации.

1.5 Средства защиты информационной безопасности

Средства защиты подразделяются на формальные, которые выполняют защитные функции строго по заранее запланированной процедуре и без участия человека и неформальные, которые определяются целенаправленной деятельностью человека или регламентируют эту деятельность.

В зависимости от способа реализации формальные можно разделить на группы:

а) физические средства защиты – электрические механические, электронные механизмы, которые функционируют независимо от информационных систем и создают препятствия для доступа к ним;

б) аппаратные средства защиты – электрические, оптические, электронные, лазерные устройства, которые встраиваются в информационные и телекоммуникационные системы. Перед внедрением их в информационные системы необходимо удостовериться в совместимости;

в) программные средства защиты – простые и системные, комплексные программы, предназначенные для решения частных и комплексных задач, связанных с обеспечением информационной безопасности. Пример комплексных решений:

– SIEM-системы – обеспечивают защиту от инцидентов в сфере информационной безопасности;

– DLP-системы служат для предотвращения утечки, переформатирования информации и перенаправления информационных потоков.

г) специфические средства – различные криптографические алгоритмы, позволяющие шифровать информацию на диске и перенаправляемую по внешним каналам связи. Преобразование информации может происходить при помощи программных и аппаратных методов, работающих в корпоративных информационных системах.

Деятельность человека регламентируют неформальные средства защиты:

– законодательные средства – определяются законодательными актами РФ, которые регламентируют правила использования, обработки, передачи информации ограниченного доступа и устанавливают меры ответственности за их нарушение. Распространяются на всех субъектов информационных отношений;

– организационные средства – организационно–технические и организационно–правовые мероприятия, осуществляемые в течение всего жизненного цикла защищаемой информационной системы.

Средства уровня организации, регламентирующие перечень лиц, оборудования, материалов, имеющих отношение к информационным системам, режимов их работы и использования. К организационным мерам также относят сертификацию информационных систем или их элементов, аттестацию объектов и субъектов на выполнение требований обеспечения безопасности;

– морально – этические средства, которые реализуются в виде всевозможных норм, которые сложились традиционно по мере распространения вычислительной техники и средств связи в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, но их несоблюдение чаще приводит к потере авторитета и престижа человека.

В мировой практике при разработке нормативных средств ориентируются на стандарты защиты информационной безопасности, основный – ISO/IEC 27000, созданный двумя организациями:

– ISO – Международная комиссия по стандартизации, которая разрабатывает и утверждает большинство признанных на международном уровне методик сертификации качества процессов производства и управления;

– IEC – Международная энергетическая комиссия, которая внесла в стандарт свое понимание систем информационной безопасности, средств и методов ее обеспечения.

Для обеспечения безопасности нужно регулярно проводить мониторинг новых разработок, программных и аппаратных средств защиты, угроз и своевременно вносить изменения в собственные системы защиты от несанкционированного доступа.

Адекватность и оперативность реакции на угрозы поможет добиться высокого уровня конфиденциальности в работе.

Существует множество способов передачи конфиденциальной информации на расстоянии, среди которых можно выделить три основных:

– создать защищенный канал передачи данных между абонентами;

– использовать общедоступный канал связи, но скрыть сам факт передачи информации. Разработкой средств и методов скрытия факта передачи сообщения по каналам связи занимается стеганография, которая в применении совместно с криптографическими методами дает наиболее эффективный результат;

– использовать общедоступный канал связи, но передавать по нему нужную информацию в таком преобразованном виде, чтобы восстановить ее мог только адресат. Разработкой методов преобразования информации с целью ее защиты от несанкционированного прочтения занимается криптография.

Задачи криптографии – обеспечение конфиденциальности и обеспечение целостности информации.

Под методом шифрования понимается совокупность обратимых преобразований открытой информации в закрытую, в соответствии с алгоритмом шифрования.

Основные методы шифрования – симметричное и асимметричное.

В симметричном методе один и тот же ключ используется и для шифровки, и для расшифровки сообщений. В асимметричном применяются два ключа, один из которых «открытый» передается по открытому каналу и используется и используется для проверки электронной подписи и для шифрования сообщения, другой «секретный», известный только получателю и применяется для расшифровки.

Преимущества асимметричного шифрования перед симметричным:

– не требует предварительной передачи секретного ключа по надёжному каналу;

– ключ дешифрования, который необходимо держать в секрете, известен только одной стороне (в симметричной – такой ключ известен и должен держаться в секрете обеими сторонами);

– в больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

Недостатки асимметричного шифрования перед симметричным:

– в алгоритм сложно внести изменения;

– более длинные ключи;

– шифрование – расшифровывание с использованием пары ключей проходит на два – три порядка медленнее, чем шифрование – расшифрование симметричным алгоритмом;

– требуются существенно большие вычислительные ресурсы, поэтому асимметричные криптосистемы используются в сочетании с другими алгоритмами.

1.6 Средства защиты от несанкционированного доступа

В информационных системах для защиты информации от несанкционированного доступа (НСД) применяются средства защиты, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК, или на соответствие требованиям, указанным в технических условиях (34).

Функции безопасности таких средств должны обеспечивать выполнение настоящих требований согласно Приказу ФСТЭК от 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [40].

Под системой защиты информации от НСД ФСТЭК понимает совокупность мер организационного характера и программно – технических средств защиты. Эти средства входят в состав средств вычислительной техники (СВТ) и автоматизированных систем (АС) в виде совокупности программного и технического обеспечения.

Функциональность средств защиты от НСД должна затруднять или предотвращать несанкционированное проникновение в обход правил разграничения доступа, реализованных штатными средствами.

В руководящем документе от 30 марта 1992 г. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» [27] устанавливается семь классов защищенности средств вычислительной техники от несанкционированного доступа к информации. Самый низкий – седьмой класс, самый высокий – первый. Классы подразделяются на группы, которые отличаются между собой качественным уровнем защиты.

Классификация защищенности АС устроена несколько иначе. Нормативной базой является руководящий документ от 30 марта 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Классификация автоматизированных систем и требования по защите информации» [28], который устанавливает девять классов защищенности АС от НСД.

Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения, обоснованных мер по достижению требуемого уровня защиты информации. Каждый класс характеризуется определенной совокупностью требований к средствам защиты и подразделяется на три группы, отличающиеся между собой спецификой обработки информации в АС.

Классификация автоматизированных систем необходима для более детальной, дифференцированной разработки требований по защите от несанкционированного доступа.

К основным параметрам определения класса защищенности автоматизированных систем относятся:

– информационные, определяющие ценность информации, ее объем и степень конфиденциальности, а также возможные последствия неправильного функционирования АС из-за искажения или потери информации;

– организационные, определяющие полномочия пользователей;

– технологические, определяющие условия обработки информации.

Комплекс программно-технических средств и организационных решений по защите информации от несанкционированного доступа реализуется в рамках системы защиты информации от НСД, условно состоящей из четырех подсистем:

– управления доступом;

– криптографической;

– регистрации и учета;

– обеспечения целостности.

В зависимости от класса автоматизированных систем в рамках этих подсистем должны быть реализованы требования в соответствии с таблицей в руководящем документе [28].

Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Программно-технические средства защиты не должны ухудшать основные функциональные характеристики АС такие как надежность, быстродействие, возможность изменения конфигурации.

Защита автоматизированных систем должна предусматривать контроль эффективности средств защиты от несанкционированного доступа. Контроль может быть периодическим или производиться по мере необходимости контролирующими органами или пользователем АС.

Отличие двух направлений защиты в том, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации (ЗИ). Помимо пользовательской информации при создании АС, появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

Вывод по первому разделу

Для выполнения поставленных задач изучена классификация информационной безопасности и системы ее обработки, законодательство Российской Федерации, подзаконные и нормативные акты, в области защиты данных. Помимо правовых исследованы государственные стандарты РФ, нормативно – методические документы ФСТЭК России и требования, предъявляемые к техническим и организационным условиям защищенности информационных систем от несанкционированного доступа.

2 СРАВНЕНИЕ ОТЕЧЕСТВЕННЫХ И ПЕРЕДОВЫХ ЗАРУБЕЖНЫХ ТЕХНОЛОГИЙ И РЕШЕНИЙ

Важнейшим этапом в становлении теории информационной безопасности во многих странах стало принятие в 1985 году Министерством Обороны США стандарта «Критерии оценки доверенных компьютерных систем (Trusted Computer System Evaluation Criteria)», наиболее известным под названием «Оранжевая книга». Именно в ней впервые появились такие понятия как «администратор безопасности», «политика безопасности» и «монитор безопасности обращений».

Стандарт стал первым в истории общедоступным оценочным стандартом в области информационной безопасности.

Цели стандарта:

- предоставить производителям стандарт, устанавливающий, какими средствами безопасности следует оснащать свои новые и планируемые продукты, чтобы поставлять на рынок доступные системы, удовлетворяющие требованиям гарантированной защищенности для использования при обработке ценной информации;
- обеспечить базу для исследования требований к выбору защищенных систем;
- предоставить метрику для приемки и оценки защищенности для обработки служебной и другой ценной информации.

В «Оранжевой книге» определены четыре уровня безопасности – D, C, B и A и шесть классов информационной безопасности – C1, C2, B1, B2, B3 и A1.

Недостатки «Оранжевой книги» и предложенный подход к классификации АС стали проявляться постепенно. Принципиальные изменения аппаратной базы средств вычислительной техники, распространение распределённых вычислительных систем и сетей, особенности которых никак не учитывались, вопросы обеспечения доступности информации сделали «Оранжевую книгу» устаревшей.

Стараясь не отстать от развивающихся информационных технологий, разработчики «Оранжевой книги» вплоть до 1995 г. выпустили целый ряд вспомогательных документов, известных как «Радужная серия», которые содержали рекомендации по применению положений «Оранжевой книги» для различных категорий автоматизированных систем, а также вводили ряд дополнительных требований.

Наибольший интерес в «Радужной серии» представляют три документа: «Интерпретация для защищённых сетей», «Интерпретация для защищённых СУБД» и «Руководство по управлению паролями».

В настоящее время «Оранжевая книга» представляет интерес исключительно с исторической точки зрения.

Современные стандарты, используемые в Российской Федерации, во многом сходны со стандартом «Критерии оценки доверенных компьютерных систем».

Создание основы для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий является главной задачей стандартов безопасности.

Специалисты по сертификации и эксперты по квалификации рассматривают стандарты как инструмент, позволяющий им оценить уровень безопасности, обеспечиваемый продуктами информационных технологий, и предоставить потребителям возможность сделать обоснованный выбор, а производителям – получить объективную оценку возможностей своего продукта.

Благодаря использованию стандартов:

– пользователь может сократить свои затраты на сертификацию продуктов;

– сертифицирующие органы могут привлечь дополнительный поток заказов на сертификацию из-за рубежа;

– производители высокотехнологичных продуктов могут получить международные сертификаты, что может позволить им выйти на закрытые ранее рынки.

Еще один стандарт, который описывает классы информационной безопасности – «Критерии безопасности информационных технологий» (Information Technology Security Evaluation Criteria), разработан рядом западноевропейских государств. Стандарт, вышедший в 1991 году, содержит согласованные критерии оценки безопасности информационных технологий, выработанные в ходе общеевропейской интеграции, и описывает классы функциональности систем информационной безопасности, характерные для правительственных и коммерческих структур. Некоторые из этих классов соответствуют классам информационной безопасности «Оранжевой книги».

Стандарт ISO/IEC 15408–1999 «Common Criteria for Information Technology Security Evaluation» был разработан совместными усилиями специалистов Канады, США, Великобритании, Германии, Нидерландов и Франции в период с 1990–1999 гг., развитие стандарта непрерывно продолжается. Исторически за стандартом закрепилось разговорное название «Общие критерии» (Common Criteria).

В России аутентичный перевод «Общих критериев» версии 2.0 принят в качестве ГОСТ Р ИСО/МЭК 15408–2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» в 2002 году и введён в действие с 1 января 2004 г. (в настоящее время заменен на ГОСТ Р ИСО/МЭК 15408–2008) [3].

«Оранжевая книга» также послужила и источником при разработке Руководящего документа «Средства вычислительной техники (СВТ). Защита от несанкционированного доступа (НСД) к информации. Показатели защищенности от НСД к информации», который устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Руководящие документы (РД) Гостехкомиссии России действуют и активно используются при проведении сертификации средств защиты информации в

системах сертификации ФСТЭК России, Минобороны России, а также в ряде добровольных систем сертификации.

Основные стандарты в области информационной безопасности, имеющие в настоящее время официальный статус в Российской Федерации:

Стандарт ГОСТ Р ИСО/МЭК 15408–2008, известный как «Общие критерии», действует и применяется при проведении сертификации средств защиты, не предназначенных для работы с информацией, составляющей государственную тайну.

Стандарт ГОСТ Р ИСО/МЭК 17799–2005 идентичен международному стандарту ИСО/МЭК 17799:2000 «Информационная технология. Практические правила управления информационной безопасностью». (ISO/IEC 17799:2000 «Information technology. Code of practice for security management») [4].

Стандарт ГОСТ Р ИСО/МЭК 27001–2006 идентичен международному стандарту ИСО/МЭК 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (ISO/IEC 27001:2005 «Information technology – Security techniques Information security management systems – Requirements», IDT) [5].

Криптографические стандарты, являющиеся обязательными для применения в системах защиты информации – ГОСТ 3410–2012 [7] и ГОСТ 34.11–2012 [39].

Информационная безопасность – одно из немногих ИТ–отраслей, где Россия пытается поддерживать собственные стандарты. В открытых источниках мало работ, посвященных анализу стандартов ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012, в отличие от работ, посвященных анализу стандартов США DES и AES. По результатам открытых работ можно сделать вывод о достаточно высокой криптостойкости российских стандартов шифрования.

Среди комбинированных методов шифрования наиболее распространенными являются методы блочного шифрования. Блочное шифрование предполагает разбиение исходного открытого текста на равные блоки, к которым применяется однотипная процедура шифрования. В настоящее время блочные шифры широко используются на практике. Бывший российский ГОСТ 28147–89 и бывший американский стандарт шифрования DES относятся именно к этому классу шифров.

DES (Data Encryption Standard, стандарт шифрования данных) – федеральный стандарт шифрования США в 1977–2001гг. для использования во всех несекретных правительственных каналах связи. Несмотря на то, что в настоящий момент федеральным стандартом шифрования США является AES (Rijndael), значение DES для теоретической и прикладной криптографии невозможно переоценить. Рассмотрение DES позволяет понять основные принципы блочного шифрования.

Похожий на DES шифр ГОСТ 28147–89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» [6] много лет являлся действующим стандартом шифрования в РФ. Стандарт был отменен на территории России и СНГ с 31 мая 2019 года в связи с принятием

новых, полностью его заменяющих, межгосударственных стандартов ГОСТ 34.12–2018 [43] и ГОСТ 34.13–2018 [8].

Алгоритм DES правительство США признало ненадежным в 2000 году по причине проявившихся в процессе эксплуатации неудобств и не полной приспособленности к новым запросам. И новым стандартом шифрования в США с 2001 года стал AES, который предложили бельгийские криптографы, использовавшие в своей разработке высшие разделы модульной алгебры.

После введения в США стандарта шифрования AES возник вопрос о применении шифра ГОСТ. Предпринятые с этой целью исследования показали, что удобства в эксплуатации, криптостойкость и эффективность алгоритмов ГОСТ и AES вполне сопоставимы.

Вывод по второму разделу

В разделе произведен анализ и сравнение отечественных и передовых зарубежных технологий и решений в области информационной безопасности. Определены действующие в РФ стандарты и руководящие документы.

3 ПРАКТИЧЕСКАЯ ЧАСТЬ

Проектируемая система обработки коммерческой информации была выбрана с учетом технических требований заказчика, которые устанавливают порядок организации работ, работоспособность технических средств, обеспечение защиты конфиденциальной информации от несанкционированного доступа в процессе ее обработки, передачи и хранения.

Для проектирования сети рассматривается отдельное здание, имеющее два этажа и шесть помещений внутри. Учитывая примерное количество сотрудников в организации, необходимо для начала продумать примерный план размещения по кабинетам, подобрать оборудование, необходимое для функционирования сети и обосновать его выбор, описать топологию, которой будем придерживаться, проектируя сеть и обосновать ее выбор.

Наличие нескольких компьютеров в организации и потребность в быстрой передаче информации между ними предполагает объединить компьютеры в локальную сеть, выбрав способом соединения отдельных ее компонентов – топологию «звезда», используя сетевые коммутаторы в качестве центральных узлов.

Топология «звезда» выбрана ввиду простой реализации и высокой надежности.

При использовании топологии «звезда» надежность сети значительно повышается, поскольку при возникновении проблем, связанных с одним из конкретных узлов, это никак не повлияет на производительность других, так как все компьютеры не связаны между собой. Кроме этого будет гораздо проще обнаружить поврежденный участок кабеля или неисправную сетевую карту.

При топологии «звезда» сеть легко масштабируется. Для расширения сети достаточно будет новый персональный компьютер просто подключить к свободному порту свитча (коммутатора).

Достоинства топологии «звезда»:

– высокая расширяемость и продуктивность;

– надежность и полная защищенность данных;

– поиск и устранение вышедшего из строя компьютера или кабеля, соединяющего его с коммутатором;

– быстродействие сети.

Из минусов в топологии «звезда» можно выделить два основных – это подчиненность всех узлов компьютера свитчу и увеличение количества кабеля для прокладки сети.

Предложенная схема организации сети (рисунок 3.1)

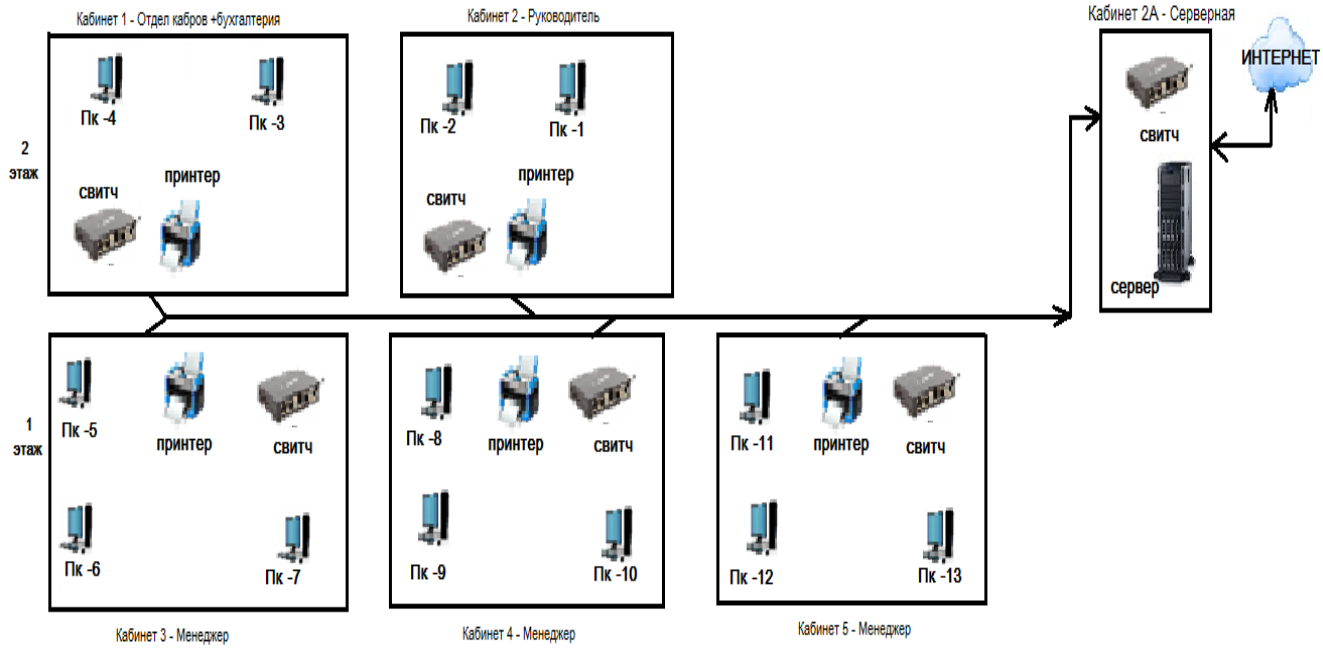

Рисунок 3.1 – Схема организации сети

Согласно предложенной схеме:

На 2 этаже располагаются три кабинета. Один из них предполагает рабочее место руководителя, второй – рабочие места для работников отдела кадров и бухгалтерии предприятия. Каждый из этих кабинетов предполагает наличие двух персональных компьютеров (ПК), коммутатора для передачи данных и принтера. Третье помещение, не имеющее окон и расположенное в стороне, будет оборудовано под серверную, занимаемую оборудованием и подразумевающую ограниченный доступ людей.

На 1 этаже три кабинета будут организованны для специалистов, в данном случае для менеджеров, которые будут непосредственно заниматься обработкой, хранением и передачей информации и являться непосредственными пользователями установленных ПК.

Итогом распределения рабочих мест получается наличие в здании 13 персональных компьютеров, которые нужно объединить в локальную сеть.

Соединение каждого компьютера с коммутатором осуществляется с использованием кабеля «витая пара» категории 5е.

Через коммутатор передается вся информация между клиентами, но принимают ее только те, кому она предназначена.

Все свитчи кабинетов подключаются к расположенному в серверной коммутатору здания, подключенному к серверу, который осуществляет также выход во внешнюю среду Internet.

Установленные в каждом кабинете принтеры предназначены для вывода текстовой информации на бумагу и будут настроены для печати через общий доступ.

3.1 Защита информации

Для выбора способов и методов защиты информации в информационных системах, нужно знать, с какой информацией будет работать организация.

Данное предприятие будет специализироваться на заключении сделок, соответственно будет иметь дело с обработкой информации, относящейся к персональным данным и конфиденциальной информации, представляющей собой коммерческую тайну.

Использование конфиденциальной информации регулируется законодательством РФ, а защита персональных данных – Федеральным законом [7].

Для защиты данных можно использовать информационную систему персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

В зависимости от уровня защищенности персональных данных к ИСПДн предъявляется перечень требований к техническим средствам и программному продукту, выполнение которых необходимо для нейтрализации угроз безопасности ПДн даже при минимальном уровне защищенности:

– контроль за выполнением требований;
– контроль доступа и физическая безопасность;
– безопасность носителей;
– перечень допущенных лиц;
– сертифицированные средства защиты.

Для соотнесения типа ИСПДн к тому или иному уровню защищенности необходимо:

а) Определить категорию обрабатываемых данных

Категории персональных данных (ПДн) разделяются на 4 группы:

– 1 группа – персональные данные, касающиеся национальной и расовой принадлежности, религиозных, философских убеждений, политических взглядов, состояние здоровья и интимной жизни;

– 2 группа – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нём дополнительную информацию, за исключением персональных данных, относящихся к группе 1;

– 3 группа – общедоступные персональные данные, которые позволяют идентифицировать субъекта персональных данных;

– 4 группа – обезличенные и общедоступные персональные данные.

По форме отношений между организацией и субъектами обработка подразделяется на 2 вида:

– обработка персональных данных работников (субъектов, с которыми ваша организация связана трудовыми отношениями);

– обработка персональных данных субъектов, не являющихся работниками организации.

б) Определить объем персональных данных, обрабатываемых в информационной системе:

– одновременно обрабатываются персональные данные до 100 000 субъектов персональных данных;

– одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных.

По результатам исходных данных ИСПДн присваивается один из классов защищенности (таблица 1).

Таблица 1 – Присваивание класса защищенности

Объем /Категория	Объем < 100 000	Объем > 100 000
4 группа (общедоступные)	Класс-4	Класс-4
3 группа (идентификационные)	Класс-3	Класс-2
2 группа (идентификационные и еще)	Класс-2	Класс-1
1 группа (специальные)	Класс-1	Класс-1

Класс защищенности (К–4) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Класс защищенности (К–3) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных.

Класс защищенности (К–2) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных.

Класс защищенности (К–1) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных.

Информационная система для обработки персональных данных должна соответствовать действующим требованиям руководящих документов ФСТЭК России (таблица 2).

Таблица 2 – Соответствия между требованиями к классам

Класс ИСПДн / класс по РД ФСТЭК	К1	К2	К3
Средства вычислительной техники (СВТ)	5	5	5
Автоматизированные системы (АС)	1Г+	1Д	1Д
Межсетевые экраны (МЭ)	3	4	4
Недекларированные возможности (НДВ)	4	-	-

Исходя из результатов данных ИСПДн, работа менеджеров организации относится к 3 классу защищенности, отдела кадров и бухгалтерии – к 2 классу, руководителя к 1 классу.

В зависимости от уровня защищенности персональных данных к ИСПДн предъявляется перечень требований к техническим средствам и программному продукту, выполнение которых необходимо для нейтрализации угроз безопасности персональных данных даже при минимальном уровне защищенности:

Требования к автоматизированным системам по защите информации от НСД для 1, 2, 3классов (для всех работников):

– идентификация, проверка подлинности и контроль доступа субъектов в систему;

– регистрация и учет входа (выхода) субъектов доступа в (из) систему(ы);

– учет носителей информации;

– обеспечение целостности программных средств и обрабатываемой информации;

– физическая охрана средств вычислительной техники и носителей информации.

Только к автоматизированным системам 1 класса (руководитель):

– идентификация, проверка подлинности и контроль доступа субъектов к терминалам, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, к программам, каталогам, файлам, записям;

– регистрация и учет выдачи печатных (графических) выходных документов, запуска (завершения) программ и процессов, доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи;

– очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.

Все 3 класса образуют вторую группу защиты для средств вычислительной техники, которая отличается наличием дискреционного управления доступом, что позволяет задавать правила доступа пользователей к различным ресурсам, в которых явно указано, что именно можно делать субъекту: читать содержимое файла, выполнять запуск программы и т. д.

Требования, предъявляемые к межсетевым экранам 3 и 4 класса защиты в автоматизированных системах, могут быть полностью удовлетворены, если использовать операционную систему Astra Linux, потому что она соответствует по требованиям безопасности информации, установленным в ФСТЭК России.

Помимо требований к защите, следует определиться с тем, кто будет обеспечивать безопасность персональных данных. Крупные организации могут позволить себе иметь собственную службу безопасности, а вот мелким и средним организациям это экономически не выгодно. Менее затратным и более разумным для них будет вариант привлечь лицензиатов ФСТЭК. Это организации, которые профессионально занимаются защитой информации. Специалисты лицензиатов уже обладают всеми знаниями нормативной и технической базы, имеют опыт создания комплексных систем безопасности, в том числе информационной. Выбор таких специалистов сократит расход предприятия на содержание штатного персонала и позволит переложить большинство рисков, связанных с безопасностью информации.

Для защиты информации, составляющей коммерческую тайну на предприятии обязательным со стороны руководителя, будет составление перечня сведений, на которые распространяется режим коммерческой тайны, список лиц, допущенных к этой информации и оформление обязательств с ними о неразглашении коммерческой информации.

3.2 Программное обеспечение

В качестве программного обеспечения выбрана Astra Linux – современная отечественная операционная система, которая может решать задачи различного уровня и применяться в различных сферах.

Для того чтобы посмотреть как работает ОС Astra Linux был использован VirtualBox – программный продукт виртуализации для операционных систем и гостевая операционная система Astra Linux, а установка и настройка произведена в хостовой операционной системе Window 7 (рисунок 3.2).

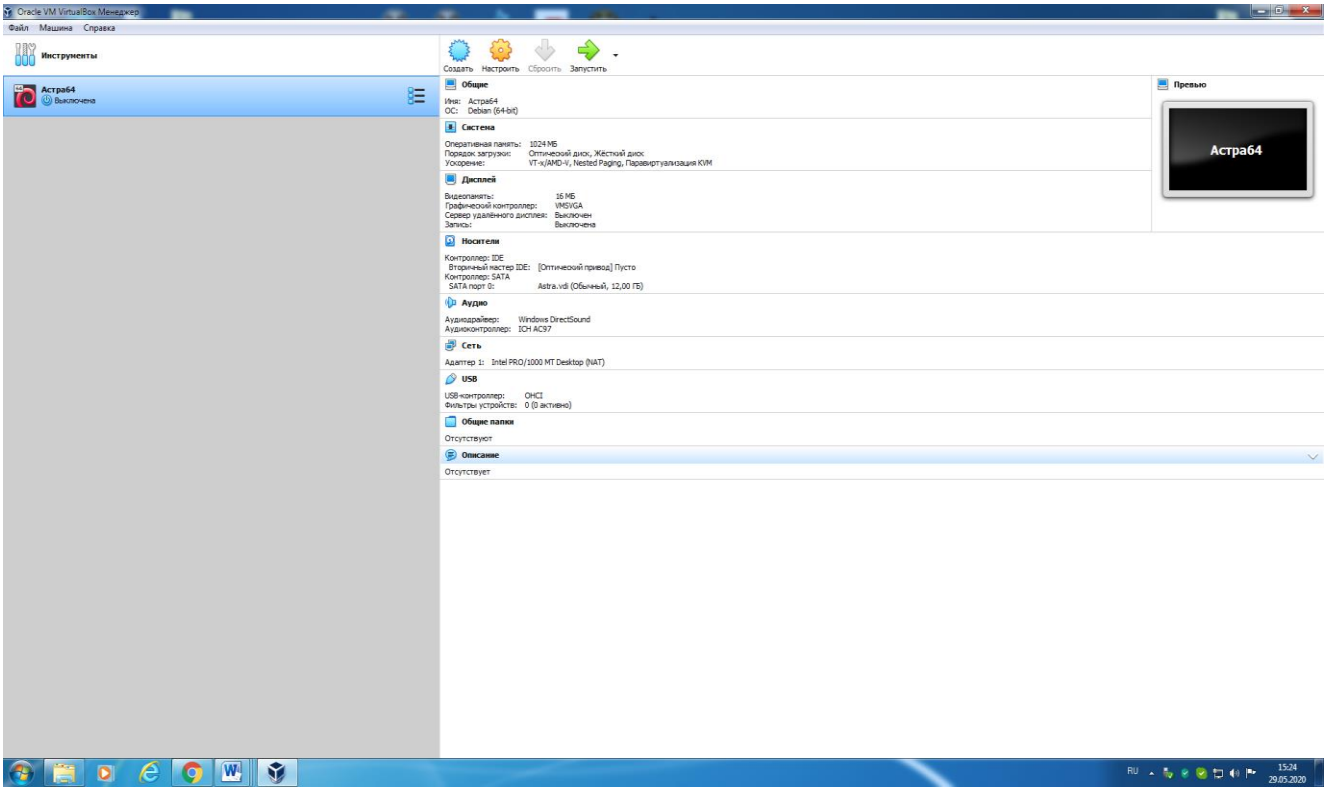

Рисунок 3.2 – Скриншот запуска VirtualBox

При запуске VirtualBox машина предлагает запустить Astra Linux, запрашивая пароль пользователя (рисунок 3.3).

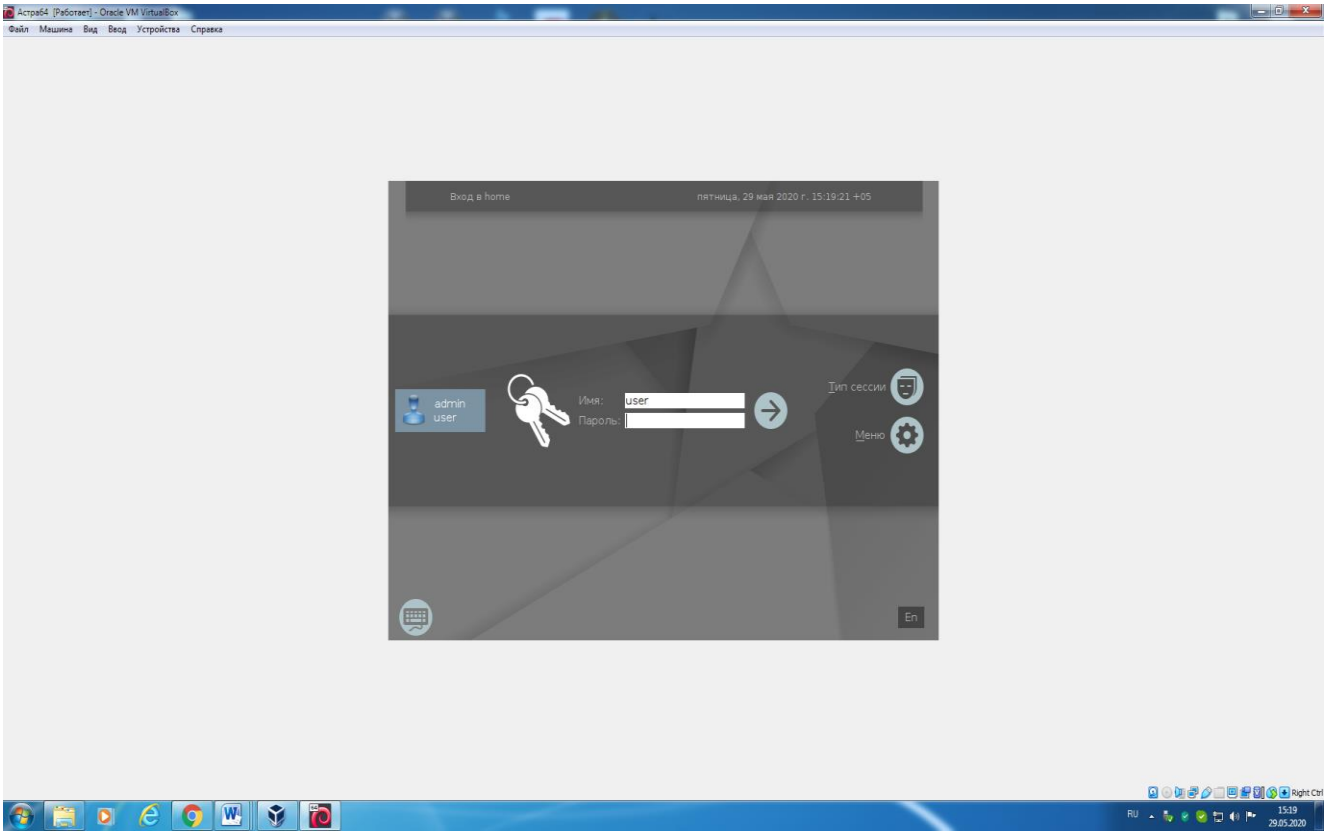

Рисунок 3.3 – Скриншот запуска Astra Linux

Система имеет простой графический интерфейс, который легко адаптируется под все виды устройств, начиная от обычных компьютеров и заканчивая смартфонами (рисунок 3.4).

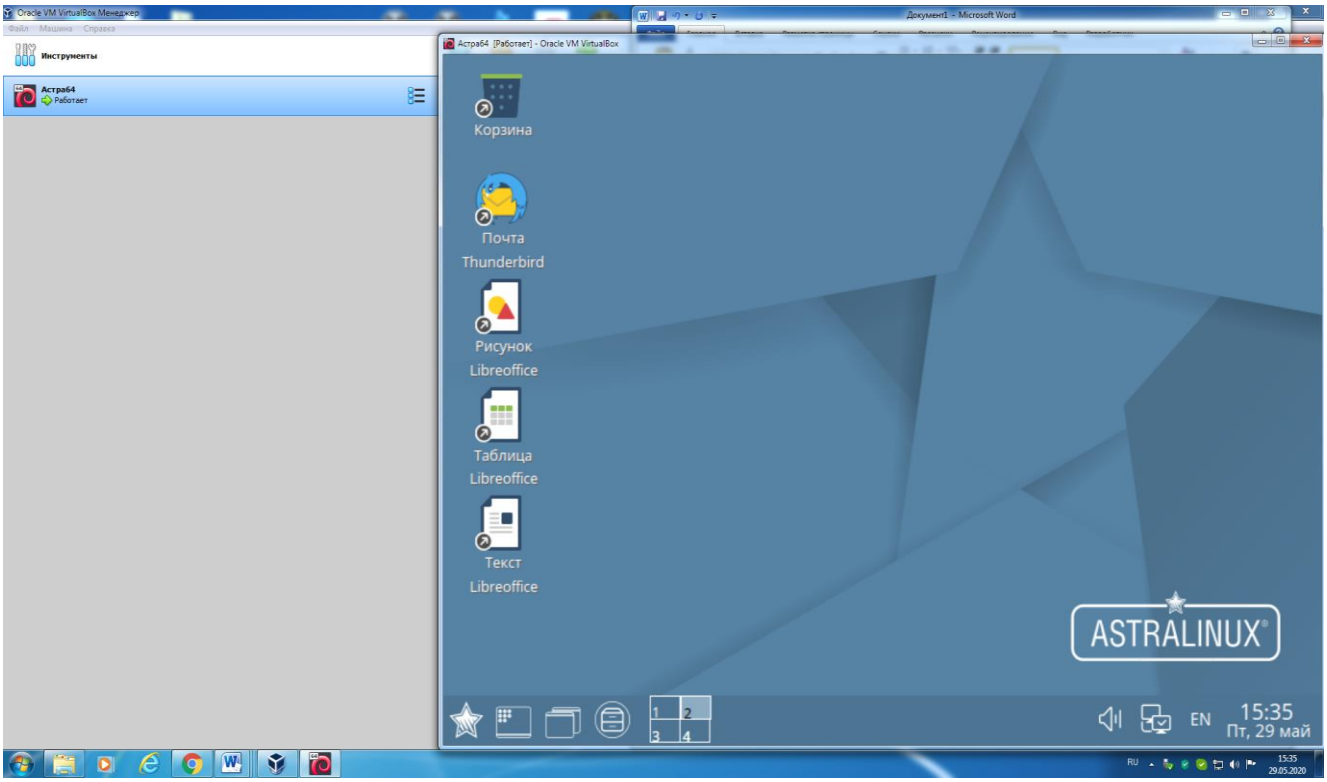

Рисунок 3.4 – Скриншот интерфейса

У системы есть все необходимое для решения обычных задач, таких как работа с документами и электронной почтой, поиском в Интернете, просмотром мультимедиа, управлением и синхронизацией данных (рисунок 3.5).

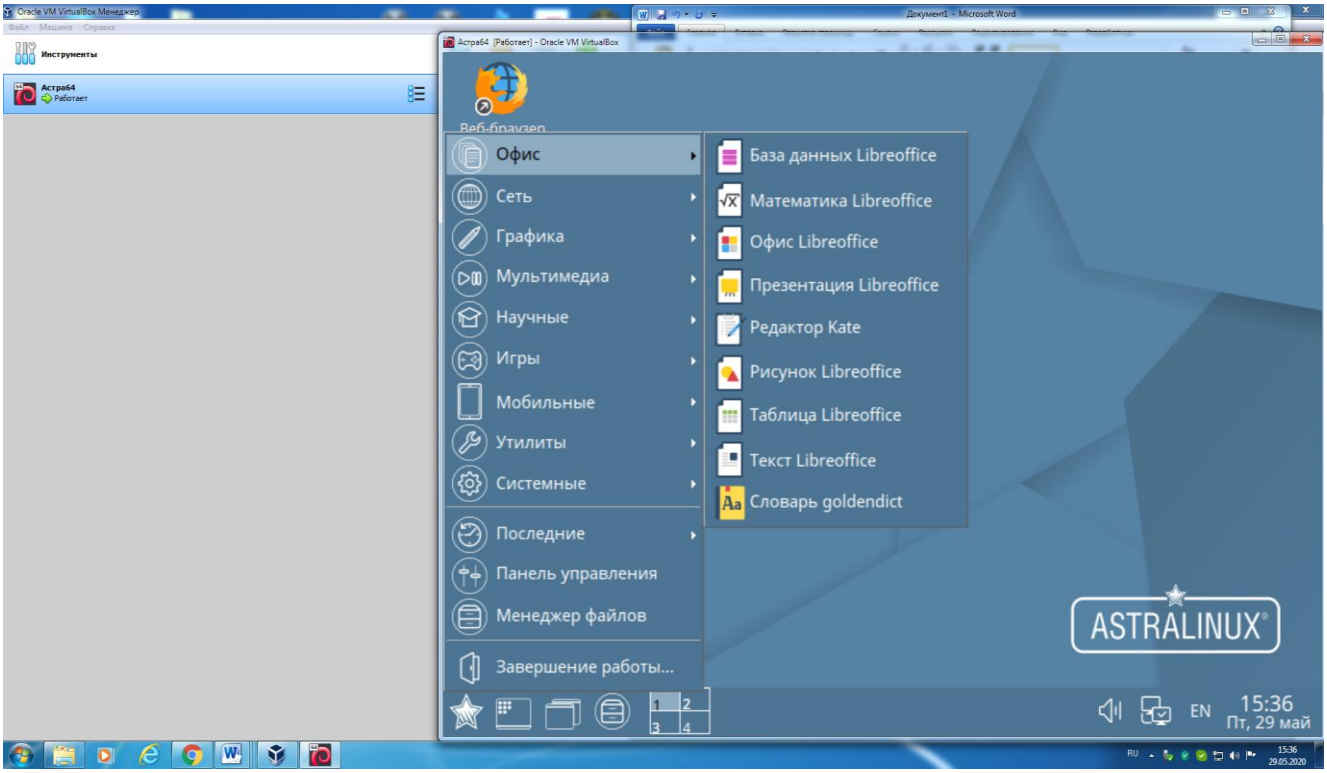

Рисунок 3.5 – Скриншот меню

Помимо основных программ российская ОС Astra Linux совместима с большим количеством дополнительных приложений и средствами обработки информации. Все это делает ее универсальным инструментом для создания систем различной сложности, как для внедрения в центр обработки данных, так и для личного пользования (рисунок 3.6).

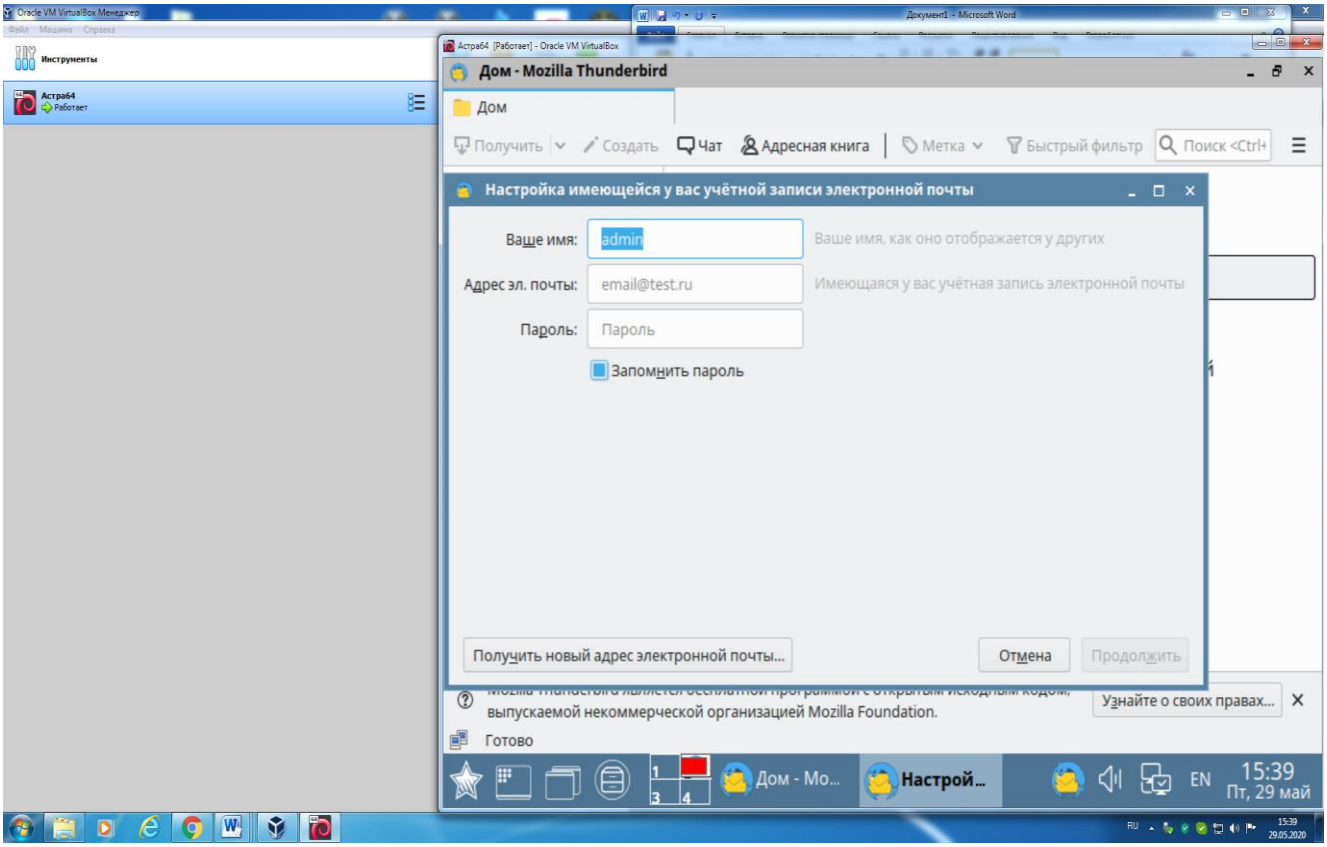

Рисунок 3.6 – Скриншот настройки электронной почты

Еще одним преимуществом российской системы Astra Linux является безопасность (рисунок 3.7; 3.8).

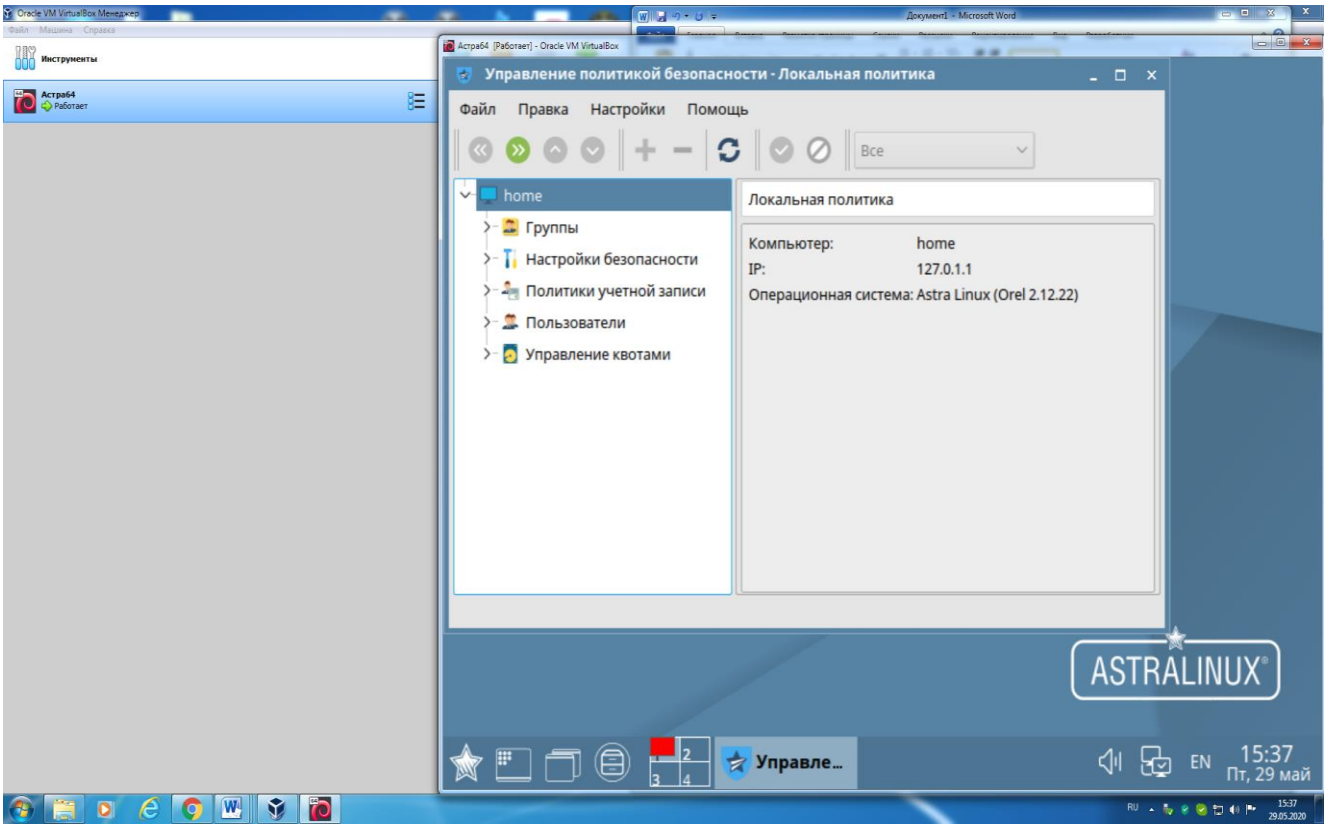

Рисунок 3.7 – Скриншот вкладки управление безопасности

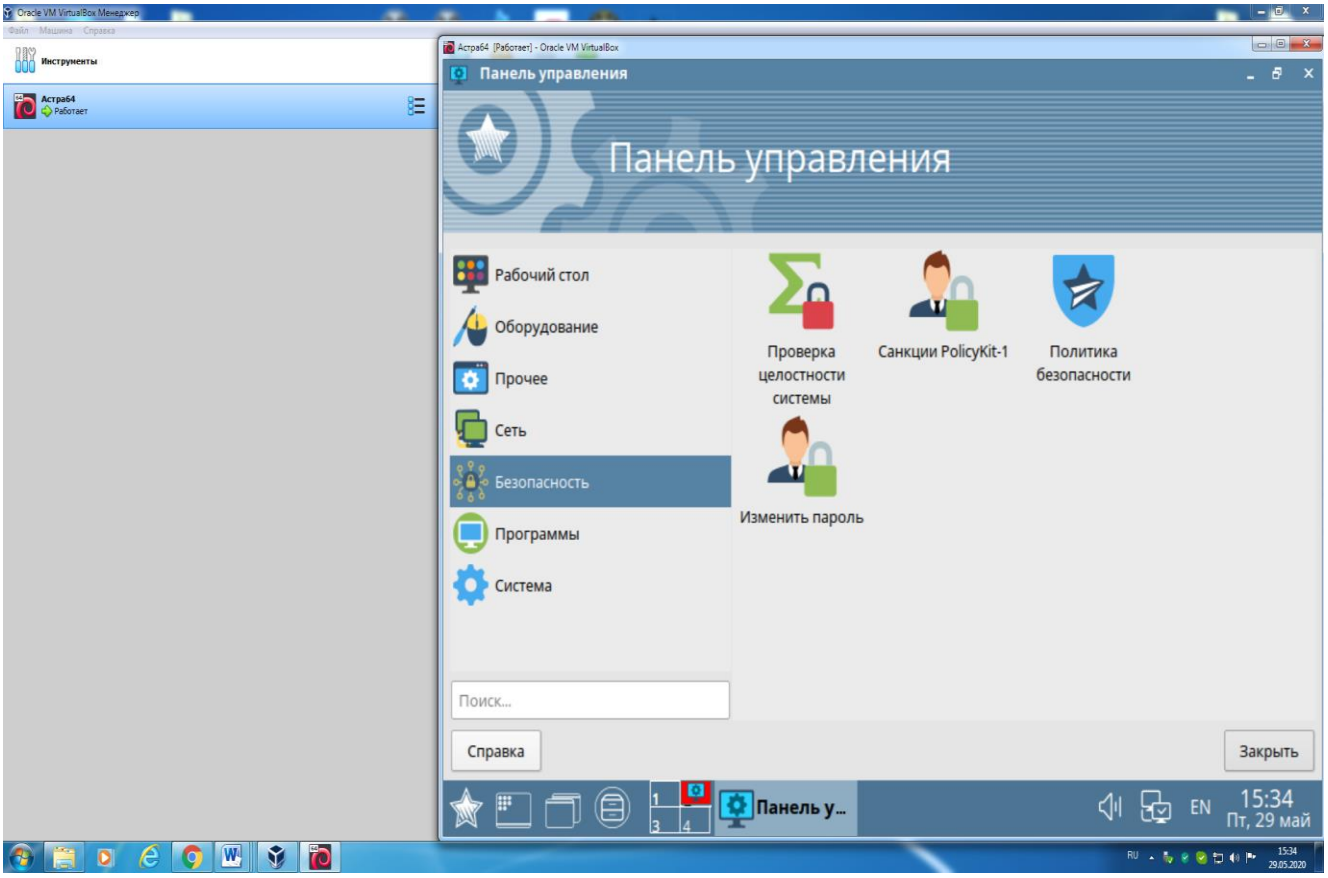

Рисунок 3.8 – Скриншот вкладки безопасность

Astra Linux имеет сертификаты Минобороны, ФСТЭК и ФСБ России и включена в единый реестр российских программ Министерства цифрового развития, связи и массовых коммуникаций РФ. Это является подтверждением ее высоких показателей качества и безопасности.

ОС рекомендуется для применения в системах, хранящих персональные данные и любую другую информацию, подлежащую защите (коммерческую, государственную, банковскую, медицинскую и налоговую).

Применяя ОС Astra Linux, можно решать личные задачи и быть уверенным в сохранности данных.

3.3 Подбор оборудования

Выбор активного оборудования очень важен и определяется требованиями, предъявляемыми к сети. Как правило, его стоимость составляет большую часть от всей стоимости сети.

Задача подбора оборудования содержит много аспектов.

На начальном этапе, исходя из исходных данных, невозможно рассматривать вопросы необходимости дальнейшего масштабирования сети, стоимость совокупного владения системой и другие. Тем не менее необходимо выдать рекомендации и предложить к рассмотрению список оборудования.

Так как одно из помещений определено под серверную, то правильным решением для размещения активного оборудования будет приобретение коммуникационного напольного шкафа.

Выбор серверного шкафа определен количеством оборудования и типом устройств, которые необходимо в нем разместить. Расположение большого количество серверного оборудования, удобный подход для обслуживания устройств, защита от несанкционированного доступа и малая площадь помещения, являются основными показателями для установки серверного шкафа. Качество используемого материала, наличие вентиляционного блока в паре с блоком терморегулятора существенно увеличивает его стоимость.

На каждый сервер или коммутационный шкаф необходимо также рассмотреть установку источника бесперебойного питания, который позволит избежать выхода из строя оборудования и защитит от помех в сети при отключении основного источника мощности питания.

Такие источники обеспечивают автономную кратковременную работу подключенного оборудования при полном отключении электроэнергии.

При выборе источника нужно обратить внимание на основной показатель подбора – мощность блока питания, необходимого для конкретного сетевого и сервисного оборудования.

Выбор можно остановить на источниках бесперебойного питания с двойным преобразованием, которые рекомендованы для работы с серверным и сетевым оборудованием и отвечают современным требованиям к надежности электроснабжения.

Решение вопроса о необходимости приобретения шкафа и установке источника бесперебойного питания остается на усмотрение владельца и его готовности сделать вложение в такое оборудование.

В качестве серверной системы можно использовать совместимый с ОС Astra Linux программно-аппаратный комплекс «Аквариус – Бастион» (Приложение А).

Программно-аппаратный комплекс (ПАК) «Аквариус – Бастион» позволяет решить проблему разворачивания защищенной ИТ-инфраструктуры объекта с наименьшими затратами, обеспечив требуемый уровень информационной безопасности (рисунок 3.9).

Рисунок 3.9 – Программно-аппаратный комплекс «Аквариус – Бастион»

Комплекс имеет:

– модульное решение;

– высочайшее качество исполнения;

– полная защита всей инфраструктуры;

– отказоустойчивость и резервирование компонентов;

– сертифицированные компоненты.

Основные характеристики программно-аппаратный комплекс «Аквариус – Бастион» в Приложении А.

Необходимо учесть, что стоимость предложенного решения очень высока, а предлагаемые возможности, возможно, перекроют потребности заказчика в разы.

Более адекватным в таком случае будет вариант с сетевым шкафом и системным блоком, работающим в режиме сервера.

Одинаково надёжно реализовать сервер и автоматизированное рабочее место (АРМ) с высокой степени защиты можно на основе АРМ «Аквариус – Бастион» (Приложение Б).

АРМ «Аквариус – Бастион» в исполнениях С и СС может применяться в автоматизированных системах, обрабатывающих сведения, составляющие государственную тайну до грифа «совершенно секретно» включительно (рисунок 3.10).

Рисунок 3.10 – АРМ «Аквариус – Бастион»

АРМ в защищенном исполнении:

– сертифицированная ОС Astra Linux;

– совместимость и работоспособность СЗИ с аппаратной платформой;

– компоненты, сертифицированные ФСТЭК и ФСБ России.

Основные характеристики АРМ «Аквариус – Бастион» в Приложении Б.

Аквариус «Бастион – К» предлагается использовать в качестве рабочего места для построения ИСПДн 1 и 2 уровней защищенности (Приложение В).

АРМ «Бастион – К» обеспечивает максимально высокий уровень защиты конфиденциальной информации и персональных данных и оснащен сертифицированными ФСТЭК по требованиям безопасности информации средствами защиты.

Основные характеристики АРМ Аквариус «Бастион – К» в Приложении В.

Выбор коммутатора определяется необходимыми параметрами и функциями.

Сетевой коммутатор (свитч) используется для распределения сигнала сети Enternet между всеми персональными компьютерами. Свитч передает данные получателю, которому они предназначаются. Выбор свитчей обосновывается в основном желаемым количеством портов, скоростью передачи и способом установки.

Для организации выбран недорогой 8 – портовый свитч Fast Ethernet TP-Link TL-SF-1008D – настольного исполнения и скоростью передачи до 100Мбит/с (рисунок 3.11).

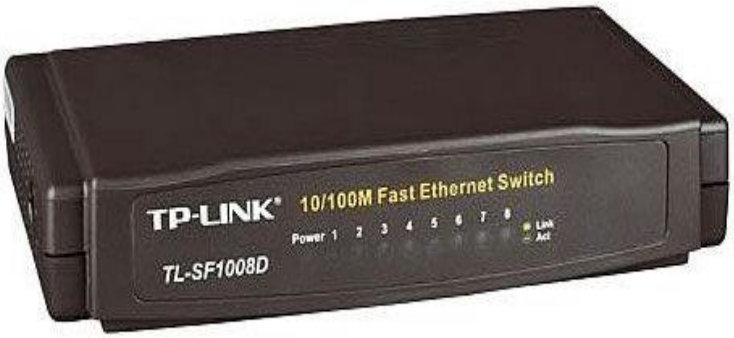

Рисунок 3.11 – Свитч TP-Link TL-SF-1008D

Кабель для разводки сети является не маловажной деталью. Вот на нем то, как раз и не желательно экономить. Хорошая витая пара – это хорошее вложение денег.

Кабель категории 5 (CAT 5e) – наиболее распространенное решение при проектировании современных информационных систем.

CAT 5e – тип кабеля для передачи сигналов, состоящий из 4 витых пар. Свивание проводков в кабеле требуется для снижения электромагнитных помех, вызванных посторонними источниками и для повышения связи проводов одной пары.

При прокладке кабеля следует учитывать расстояние до силовых кабелей и до источников электромагнитных полей.

Кабель подключается к сетевым устройствам при помощи коннекторов. При использовании 4 пар можно поддерживать скорость для сетевого оборудования 1 ГБ/с.

Выбор оргтехники осуществляется как из соображений безопасности, так и целесообразности. Поскольку неизвестна планируемая разовая и ежемесячная нагрузка на принтер, подбор его затрудняется.

Основным же соображением в выборе печатающего устройства остается организация защиты информации.

Поскольку в сети находятся данные, относящиеся к конфиденциальным, то их вывод на бумажный носитель должен быть ограничен. Проще всего обеспечить безопасность, используя сетевой принтер для каждой группы отдельно. При этом необходима настройка ведения логов печати, чтобы можно было определить, кто, какой документ отправлял на печать.

Два этих аспекта помогут определиться с выбором оргтехники.

Вывод по третьему разделу

В практической части разработана схема сети, определено количество рабочих мест и их соединение (топология), определен класс защиты информации от

несанкционированного доступа в процессе ее обработки, передачи и хранения в автоматизированных системах для персонала и руководителя.

Выбор операционной системы обоснован надежностью защиты информации.

Рекомендации по выбору оборудования даны исходя из технических требований заказчика. Предложен список оборудования, совместимого с операционной системой, позволяющей реализовать защиту любого класса.

ЗАКЛЮЧЕНИЕ

Цель выпускной работы состояла в проектировании системы обработки коммерческой информации.

В ходе выполнения поставленных задач была изучена классификация информационной безопасности и системы ее обработки. Произведен анализ и сравнение отечественных и передовых технологий и решений в этой области. Изучено законодательство Российской Федерации, подзаконные и нормативные акты, в области защиты данных. Помимо правовых исследованы государственные стандарты РФ, нормативно – методические документы ФСТЭК России и требования, предъявляемые к техническим и организационным условиям защищенности информационных систем обработки персональных данных.

Для достижения цели решены следующие задачи: разработана схема сети, определено количество рабочих мест и их соединение, определен класс защиты информации от несанкционированного доступа в процессе ее обработки, передачи и хранения в автоматизированных системах.

Требования в надежности защиты системы, хранящей персональные данные и коммерческую информацию, были реализованы при выборе операционной системы и сетевого оборудования.

Выбор операционной системы Astra Linux объясняется тем, что она имеет высокие показатели качества и безопасности, способна решать задачи различного уровня и применяться в системах, хранящих персональные данные и любую другую информацию, подлежащую защите.

Рекомендации по выбору оборудования даны исходя из технических требований заказчика. Предложен список оборудования, совместимого с операционной системой, позволяющей реализовать защиту любого класса.

Реализация проекта в предложенном варианте обойдётся владельцу дорого. Тем не менее, необходимым будет учесть тот факт, что стоимость защищаемой информации может быть несоизмеримо выше.

Исходя из всего вышеизложенного, можно сделать вывод, что проект актуален для воплощения на практике.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 ГОСТ Р ИСО/МЭК 27000–2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» [Электронный ресурс]. – http://docs.cntd.ru/document/1200102762.

2 ГОСТ Р ИСО/МЭК 13335–1–2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий (с Поправкой)» [Электронный ресурс]. – http://docs.cntd.ru/document/1200048398.

3 ГОСТ Р ИСО/МЭК 15408–2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» [Электронный ресурс]. – http://docs.cntd.ru/document/gost-r-iso-mek-15408-1-2008.

4 ГОСТ Р ИСО/МЭК 17799–2005 «Информационная технология. Практические правила управления информационной безопасностью» [Электронный ресурс]. – http://docs.cntd.ru/document/gost-r-iso-mek-17799-2005.

5 ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования» [Электронный ресурс]. – http://docs.cntd.ru/document/gost-r-iso-mek-27001-2006.

6 ГОСТ 28147–89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» [Электронный ресурс]. – http://docs.cntd.ru/document/gost-28147-89.

7 ГОСТ 3410–2012 «Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» [Электронный ресурс]. – http://docs.cntd.ru/document/gost-r-34-10-2012.

8 ГОСТ 34.13–2018 «Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров» [Электронный ресурс]. – http://docs.cntd.ru/document/1200161709.

9 Аверченков, В.И. Защита персональных данных в организации: монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. – Москва: Флинта, 2016. – 124 с.

10 Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. – М.: Риор, 2017. – 400 с.

11 Воробьев, Е.Г. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных: Учебное пособие / Е.Г. Воробьев. – Санкт-Петербург: ИЦ «Интермедия», 2016. – 432 с.

12 Вострецова, Е.В. Основы информационной безопасности: Учебное пособие для студентов вузов / Е.В. Вострецова. – Екатеринбург: издательство Урал, 2019. – 204 с.

13 Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие / А.М. Голиков, Томский Государственный Университет

Систем Управления и Радиоэлектроники (ТУСУР) – Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с.

14 Грязнов, Е.С. Безопасность локальных сетей / Е.С. Грязнов, С.А. Панасенко. – М.: Вузовский учебник, 2006.– 525 с.

15 Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие для вузов / П.Н. Девянин. – М.: Горячая линия – Телеком, 2012. – 320 с.

16 Девянин, П.Н. Моделирование и верификация политик безопасности управления доступом в операционных системах / П.Н. Девянин, П.Н. Ефремов, В.В. Кулямин. – М.: Горячая линия – Телеком, 2019. – 214 с.

17 Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 – Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. – М.: ГЛТ, 2006. – 536 с.

18 Кияев, В.И. Безопасность информационных систем: курс / В.И. Кияев, О.Н. Граничин. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с.

19 Корт, С.С. Теоретические основы защиты информации: Учебное пособие / С.С. Корт. – М.: Гелиос АРВ, 2004. – 240 с.

20 Петрыкина, Н.И. Правовое регулирование оборота персональных данных: теория и практика / Н.И. Петрыкина. – Москва: Статут, 2011. – 134 с.

21 Проскурин, В.Г. Защита в операционных системах: Учебное пособие для вузов / В.Г. Проскурин. – Москва: Горячая линия – Телеком, 2014. – 192 с.

22 Силаенков, А.Н. Проектирование системы информационной безопасности: Учебное пособие / А.Н. Силаенков. – Омск: ОмГТУ, 2009. – 128 с.

23 Скрипник, Д.А. Обеспечение безопасности персональных данных: курс / Д.А. Скрипник, Национальный Открытый Университет «ИНТУИТ» – Москва: Интернет-Университет Информационных Технологий, 2011. – 109 с.

24 Сычев, Ю.Н. Основы информационной безопасности: Учебно-практическое пособие / Ю.Н. Сычев. – Москва: Евразийский открытый институт, 2010. – 328 с.

25 Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – М.: ДМК, 2014. – 702 с.

26 Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008.– 416 с.

27 Руководящий документ от 30 марта 1992 г. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» [Электронный ресурс]. – https://fstec.ru/tekhnicheskaya-zashchita-informatsii/ dokumenty/114-spetsialnye-normativnye-dokumenty/387-rukovodyashchij-dokument-reshenie-predse-datelya-gostekhkomissii-rossii-ot-30-marta-1992-g4.

28 Руководящий документ от 30 марта 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Классификация автоматизированных систем и требования по защите информации» [Электронный ресурс]. – https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyash-chij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g.

29 Закон Российской Федерации от 21 июля 1993 г. N 5485-I «О государственной тайне» [Электронный ресурс]. – http://www.consultant.ru/document/cons_doc_ LAW_2481/.

30 Конституции Российской Федерации от 12 декабря 1993 г. (статья 23) [Электронный ресурс]. – http://www.consultant.ru/document/cons_doc_LAW_28399/.

31 Уголовный кодекс РФ от 13 июня 1996 г. (статья 272, 273, 274) [Электронный ресурс].http://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/.

32 Указ Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера» [Электронный ресурс]. – http://base.garant.ru/10200083/#ixzz6NdjLrmNR.

33 Руководящий документ от 25 июля 1997 года «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» [Электронный ресурс]. – https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyash-chij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g.

34 Руководящий документ от 4 июля 1999 года «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» [Электронный ресурс]. – https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/382-rukovodyashchij-dokument-prikaz-pred-sedatelya-gostekhkomissii-rossii-ot-4-iyunya-1999-g-n-114.

35 Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» [Электронный ресурс]. – http://www.consultant.ru/document/cons_doc_LAW_48699/.

36 Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – http://www.consultant.ru/document/cons_doc_LAW_61798/c 5051782233acca771e9adb35b47d3fb82c9ff1c/.

37 Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» [Электронный ресурс]. – http://www.consultant.ru/document/cons_doc_LAW_61801/.

38 Федеральный закон от 26 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [Электронный ресурс]. – http://www.consultant.ru/document/ cons_doc_LAW_ 112701/.

39 ГОСТ 34.11–2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» [Электронный ресурс]. – http://docs. cntd.ru/document/gost-r-34-11-2012.

40 Приказ ФСТЭК от 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс]. – https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17.

41 Приказ ФСТЭК от 18. февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – https://fstec.ru/ normotvor-cheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21.

42 Указ Президента Российской Федерации от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. – http://base.garant.ru/71556224/.

43 ГОСТ 34.12–2018 «Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры» [Электронный ресурс]. – http://docs. cntd.ru/document/1200161708.

ПРИЛОЖЕНИЕ А
Программно-аппаратный комплекс «Аквариус – Бастион»

Общее описание решения

Программно-аппаратный комплекс (ПАК) «Аквариус – Бастион» позволяет решить проблему разворачивания защищенной ИТ-инфраструктуры объекта с наименьшими затратами, обеспечив требуемый уровень информационной безопасности.

ПАК «Аквариус – Бастион» имеет модульное исполнение и обладает возможностью масштабирования, что позволяет значительно наращивать мощность и увеличивать количество автоматизируемых пользователей.

Защищенный программно-аппаратный комплекс «Аквариус – Бастион» подходит для комплексной автоматизации деятельности любых государственных и частных учреждений, обладающих территориально-распределенной структурой.

Кроме того ПАК «Аквариус – Бастион» отличается простотой в обслуживании и высокой надежностью.

Средства защиты, входящие в состав ПАК «Аквариус – Бастион», сертифицированы в системах сертификации по требованиям безопасности, что позволяет использовать ПАК «Аквариус – Бастион» как для обеспечения высоких уровней защищенности персональных данных, так и для защиты сведений, составляющих государственную тайну.

Основные преимущества решения:

1. Компактное

Полноценная ИТ-инфраструктура «все – в – одном», которая не требует затрат на подготовку отдельного серверного помещения;

2. Масштабируемое

Различные варианты исполнения как по размеру (шкафы различной высоты), так и по производительности (широкий выбор конфигураций серверного оборудования);

3. Бесшумное

Система активного шумоподавления позволяет размещать стойку в помещении без специальной подготовки. Не мешает работающим рядом людям;

4. Импортозамещение

Обеспечивает функционирование информационных систем объекта в доверенной среде;

5. Тиражируемое

Возможность оперативной поставки типовых решений в территориально распределенные объекты;

6. Информационная безопасность

Встроенные средства защиты информации сертифицированы в системах сертификации по требованиям безопасности.

Реализуемые характеристики по безопасности:

- контроль отсутствия недекларированных возможностей в программном обеспечении средств защиты информации;
- противодействие угрозам безопасности информации на самом низком уровне (на уровне базовой системы ввода – вывода);
- обнаружение «хакерских атак» и аномалий сетевого трафика в периметре локальной вычислительной сети (система обнаружения вторжений уровня сети и хостовые датчики на узлах);
- разграничение доступа к сегментам локальной вычислительной сети, контроль сетевого трафика (периметровый межсетевой экран);
- совместимость оборудования с операционными системами как Windows, так и Linux (в т. ч. МСВС);
- на все изделия имеются сертификаты по электромагнитной совместимости и электробезопасности.

ПРИЛОЖЕНИЕ Б
АРМ «Аквариус – Бастион» (версия С и СС)

АРМ «Аквариус – Бастион» в исполнениях С и СС может применяться в автоматизированных системах, обрабатывающих сведения, составляющие государственную тайну до грифа «совершенно секретно» включительно.

Средства защиты информации в составе данной модели удовлетворяют требованиям ТТЗИ (Приказ ФСТЭК № 025) и требованиям к АС до класса 1Б включительно (согласно РД АС).

Данная модель предназначена исключительно для государственных Заказчиков. В составе линейки есть сертифицированные по требованиям ФСТЭК и ФСБ исполнения.

Состав решения:

– сертифицированная ОС;

– персональные идентификаторы пользователей;

– антивирусное программное обеспечение;

– встроенное в ОС средство защиты информации от несанкционированного доступа.

Опционально возможна установка любых дополнительных модулей расширения (КСЗИ, оптическая сетевая карта и т. д.).

Преимущества решений АРМ «Аквариус – Бастион»:

- 100% совместимость и работоспособность СЗИ, предлагаемых в составе решения АРМ «Аквариус – Бастион» с аппаратной платформой;
- любая из базовых моделей линейки защищенных решений АРМ «Аквариус – Бастион» может быть дополнена необходимыми для выполнения требований заказчика средствами защиты как локального, так и сетевого уровня;
- гибкость решения, возможность обеспечения защиты как автономных ПК, так и ПК в составе локальной вычислительной сети;
- оптимальная стоимость с учетом необходимости и достаточности для защиты информационных систем различных классов защищенности;
- вариативность исполнения: решение может состоять из сертифицированных компонентов, что позволяет создавать необходимую конфигурацию, или предлагается целиком сертифицированное ФСБ или ФСТЭК исполнение.

ПРИЛОЖЕНИЕ В
АРМ Аквариус «Бастион – К»

АРМ «Бастион – К» обеспечивает максимально высокий уровень защиты конфиденциальной информации и оснащен сертифицированными ФСТЭК по требованиям безопасности информации средствами защиты.

Назначение

Защищенный АРМ «Аквариус – Бастион» версии К обеспечивает высокий уровень защиты конфиденциальной информации (в т. ч. персональных данных) и является оптимизированным решением для построения ГИС (ИСПДн) до 1 класса (уровня) защищенности включительно.

Модель оснащена сертифицированными средствами защиты информации, необходимыми и достаточными для применения в информационных системах любого класса защищенности.

Решение предназначено для крупных государственных учреждений и коммерческих компаний, в которых есть необходимость обработки большого объема данных, требующих наивысшей степени защиты.

Состав:

– антивирусное программное обеспечение;

– средство защиты от несанкционированного доступа;

– персональные USB-идентификаторы пользователей;

– средство резервного копирования и восстановления.

Опции:

– модуль доверенной загрузки (электронный замок, в т. ч. уровня загрузочной записи (БСВВ, BIOS, UEFI);

– средство криптографической защиты информации.