МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
НЕФТЕКАМСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Экономико-математический факультет
Кафедра математического моделирования и информационной безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
ПО ПРОГРАММЕ БАКАЛАВРИАТА

Ахатов Ранис Ринатович

Анализ системы обеспечения информационной безопасности (на примере Межрайонной инспекции Федеральной налоговой службы России № 29 по РБ)

Выполнил:
Студент(ка) 4 курса очной формы обучения группы ИБ-41
Направление подготовки «Информационная безопасность»
Направленность (профиль) «Организация и технология защиты информации»

Допущено к защите в ГЭК и
проверено на объем заимствования:

Заведующий кафедрой
д-р физ.-мат. наук, проф.

_____ / Ахтямов А.М. /
«___» _____ 2019 г.

Руководитель
канд. физ.-мат. наук, доц.

_____ / Аюпова А.Р. /

Нефтекамск 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире информационные отношения затрагивают все сферы деятельности человека, а результаты этой деятельности все больше зависят от целостности, достоверности, конфиденциальности информации. Обязательному регулированию подлежит деятельность по защите информации, а также, в определенной степени, практически все виды информационных отношений.

Известно, что всякая информация, во-первых является предметом, во-вторых средством и, в-третьих, продуктом труда для любой организации. Поэтому очень важное внимание должно уделяться защите информации от её утечки. При этом целями защиты информации в федеральных органах исполнительной власти являются:

– сохранение государственных секретов, конфиденциальной документальной информации в соответствии с законодательством;

– обеспечение правового режима документированной информации как объекта собственности;

– предотвращение разглашения, утечки и несанкционированного доступа к защищенной информации;

– пресечение противоправных действий по уничтожению, изменению, искажению, копированию, блокированию информации.

При реализации функций государственного управления и оказания государственных услуг ФНС России обрабатывается информация, составляющая:

- налоговую тайну;
- персональные данные;
- коммерческую и банковскую тайны;
- служебную тайну.

Обеспечение информационной безопасности в государственных органах исполнительной власти предполагает, прежде всего, правильное определение

угроз безопасности соответствующего субъекта, в том числе угроз в информационной сфере, а также адекватный выбор и применение средств защиты от этих угроз. Оно может быть достигнуто только комплексным использованием средств защиты по каждому виду угроз в рамках единой государственной политики, учитывающей, разумеется, федеральный, региональный и местные уровни ФНС России, которые должны быть взаимосвязаны.

На повышение информационной безопасности федеральных органов исполнительной власти оказывает создание на основе информационно-коммуникационных технологий электронного правительства, в результате чего обеспечивается современная информационная основа для принятия управленческих решений, повышается уровень информационного обеспечения, достоверность, скорость получения и полнота информации[1].

Актуальность темы выпускной квалификационной работы обусловлена тем, что Межрайонная ИФНС России является критически важной государственной структурой, в которой необходимо обеспечить требуемый уровень защиты информации.

Целью выпускной квалификационной работы является анализ системы обеспечения защиты информации в государственных органах исполнительной власти.

Объектом исследования в выпускной квалификационной работе является «Межрайонная инспекция Федеральной налоговой службы России № 29 по РБ».

Предметом исследования является система информационной безопасности.

Для достижения цели выпускной квалификационной работы, необходимо решить следующие задачи:

[1] Уткин В.Б., Балдин К.В. Информационные системы и технологии в экономике. – М.: Юнити-Дана, 2015. – С. 85.

– дать краткую характеристику организации;

– выявить возможные угрозы информационной безопасности в организации;

– рассмотреть организационно-правовое обеспечение защиты информации в организации;

– исследовать систему защиты информации в организации;

– разработать рекомендации по совершенствованию системы обеспечения безопасности информации.

Структурно работа состоит из введения, трех глав, заключения, списка использованных источников и литературы.

Введение обосновывает актуальность темы исследования, формулирует цель и задачи работы.

В первой главе приведена теоретическая часть. Рассмотрены сущность и понятие информационной безопасности, нормативно-правовая база в области защиты информации и угрозы информационной безопасности.

Во второй главе дана краткая характеристика организации, отражены актуальные и возможные угрозы объекта, исследована система обеспечения безопасности информации.

В третьей главе отражены рекомендации по совершенствованию системы обеспечения безопасности информации.

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ И НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Сущность и понятие системы обеспечения информационной безопасности

Информационная безопасность – одна из проблем современного общества. Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все больше приобретает черты информационного общества.

С понятием информационной безопасности в различных контекстах связаны различные определения. Информационная безопасность – это защита информации и поддерживающей её инфраструктуры от случайных или преднамеренных естественных или искусственных воздействий, которые могут нанести вред владельцу или пользователю информации.

В доктрине информационной безопасности РФ под информационной безопасностью понимается состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Согласно ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», защита информации (ЗИ) – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированного и непреднамеренного воздействия на защищаемую информацию[2].

На сегодняшний день сформулированы три основных принципа, которые должна обеспечивать информационная безопасность: целостность, доступность и конфиденциальность.

[2] Защита информации. Основные термины и определения [Электронный ресурс]: ГОСТ Р 50922-2006 от 27.12.2006 № 373-ст. Доступ из справ. - правовой системы «КонсультантПлюс».

Конфиденциальность – состояние информации, при котором доступ предоставляется только тем лицам, имеющим на это право.

Целостность – состояние информации, при котором нет каких-либо изменений в ней, или изменение делается только умышленно лицами, имеющими на это право.

Доступность – состояние информации, при котором субъекты, имеющие право доступа, могут беспрепятственно реализовать это.

Таким образом, концепция информационной безопасности, в целом, должна отвечать на три вопроса:

– что защищать;

– от чего (кого) защищать;

– как защитить.

Для того чтобы создать надежную систему информационной безопасности, необходимо выявить возможные угрозы, оценить их последствия, определить необходимые меры и средства защиты, оценить их эффективность. Различают технические, программно-аппаратные средства ЗИ, а также организационно-правовое обеспечение информационной безопасности[3].

Технические средства защиты информации – это устройства различного типа (механические, электромеханические, электронные), которые решают проблему ЗИ на уровне оборудования, например, защита помещения от прослушивания. Они либо предотвращают физическое проникновение, либо, если это происходит, мешают доступу к данным. Первая часть задачи выполняется с помощью замков, решеток на окнах, охранно-пожарной сигнализации. Вторая – это шумогенераторы, сканирующие радиостанции и многие другие устройства, которые «блокируют» потенциальные каналы утечки информации.

[3] Ковалев Д.В., Богданова Е.А. Информационная безопасность. – Ростов-на-Дону.: Издательство Южного федерального университета, 2016. – С. 36.

Под программно-аппаратными средствами защиты информации понимаются различные технические устройства, специальные программы, предназначенные и реализующие функции ЗИ от разглашения, утечки и несанкционированного доступа (НСД)[4].

Использование аппаратных средств позволяет решать следующие задачи:

– обнаружение каналов утечки информации на различных объектах и в помещениях;

– локализация каналов утечки информации;

– поиск и выявление промышленного шпионажа;

– противодействие НСД к источникам конфиденциальной информации и другим действиям.

Программные средства защиты информации предназначены для обеспечения безопасности конфиденциальной информации, включающие в себя:

– защиту информации от НСД;

– защиту информации от копирования;

– защиту информации от вирусов;

– программную защиту каналов связи.

Кроме того, программное и аппаратное обеспечение содержат криптографические средства защиты информации. Они представляют собой специальные математические и алгоритмические средства ЗИ, передаваемые по сетям и сетям связи, хранимые и обрабатываемые на компьютере с помощью различных методов шифрования. Современная криптография охватывает четыре больших раздела: симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной подписи, управление ключами.

Основой организационного и правового обеспечения информационной безопасности является использование и подготовка нормативных документов в

[4] Громов Ю.Ю., Иванова О.Г., Стародубов К.В., Кадыков А.А. Программно-аппаратные средства защиты информационных систем. – Тамбов.: Издательство ФГБОУ ВПО «ТГТУ», 2017. – С. 122.

области информационной безопасности, которые на правовом уровне должны регулировать доступ пользователей к информации.

1.2 Нормативно-правовые акты в области информационной безопасности

Основополагающими документами по информационной безопасности являются Конституция и Доктрина информационной безопасности РФ.

Конституция РФ гарантирует «тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» (статья 23, часть 2), а также «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (статья 29, часть 4). Более того, она «гарантирует свободу массовой информации» (статья 29, часть 5), то есть массовая информация должна быть доступна гражданам[5].

В доктрине информационной безопасности РФ определены важнейшие задачи обеспечения информационной безопасности[6].

Основными нормативно-правовыми документами в области защиты информации и информационной безопасности являются:

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации». Закон регулирует отношения, возникающие при получении, передаче, производстве и распространении информации; использовании информационных технологий; обеспечении информационной безопасности[7];

– Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» регулирует отношения, возникающие в связи с отнесением сведений к

[5] Конституция РФ от 12.12.1993 [Электронный ресурс]. Доступ из справ. - правовой системы «КонсультантПлюс».
[6] Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс]: Указ Президента РФ от 05.12.2016 № 646. Доступ из справ. - правовой системы «КонсультантПлюс».
[7] Об информации, информационных технологиях и о защите информации [Электронный ресурс]: Федеральный закон от 27.07.2006 № 149-ФЗ. Доступ из справ. - правовой системы «КонсультантПлюс».

государственной тайне, их засекречиванием или рассекречиванием, защитой в интересах обеспечения безопасности РФ[8];

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» регулирует отношения, связанные с обработкой персональных данных федеральными органами государственной власти[9];

– Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций[10];

– Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам[11];

– Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности». Постановление определяет правовое положение информации ограниченного доступа[12].

---

[8] О государственной тайне [Электронный ресурс]: Закон РФ от 21.07.1993 № 5485-1. Доступ из справ. - правовой системы «КонсультантПлюс».

[9] О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ. Доступ из справ. - правовой системы «КонсультантПлюс».

[10] Об электронной подписи [Электронный ресурс]: Федеральный закон от 06.04.2011 № 63-ФЗ. Доступ из справ. - правовой системы «КонсультантПлюс».

[11] О коммерческой тайне [Электронный ресурс]: Федеральный закон от 29.07.2004 № 98-ФЗ. Доступ из справ. - правовой системы «КонсультантПлюс».

[12] Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности [Электронный ресурс]: Постановление Правительства РФ от 03.11.1994 № 1233. Доступ из справ. - правовой системы «КонсультантПлюс».

1.3 Основные виды угроз информационной безопасности

Под угрозой информационной безопасности понимается совокупность условий и факторов, создающие потенциальную опасность, которая приводит к нарушению целостности, конфиденциальности и доступности информации[13].

В настоящее время классификация угроз информационной безопасности выделяет угрозы нарушения:

– конфиденциальности (несанкционированный доступ к данным, например, получение информации о состоянии счетов клиентов банка);

– целостности (несанкционированное изменение, добавление или уничтожение данных, например, изменение учетных записей);

– доступности (ограничение или блокировка доступа к данным, например, невозможность подключения к серверу с базой данных в результате атаки).

К основным случайным угрозам безопасности информации относятся:

– непреднамеренное заражение компьютера вирусами;

– неосторожные действия, влекущие за собой раскрытие конфиденциальной информации;

– потеря, передача кому-либо или раскрытие идентификаторов, которые включают в себя пароли, ключи шифрования, пропуски, идентификационные карточки;

– несоблюдение политики безопасности или других установленных правил работы с системой;

– отправка данных на неверный адрес абонента.

К основным преднамеренным угрозам можно отнести следующие угрозы:

– взяточничество, шантаж и другие способы воздействия на персонал или отдельных пользователей, обладающих определенными полномочиями;

[13] Петренко В.И. Теоретические основы защиты информации. – Ставрополь.: СКФУ, 2015. – С. 25.

– использование подслушивающих устройств, удаленная фото- и видеосъемка;

– перехват побочных электромагнитных излучений и наводок (ПЭМИН);

– перехват данных, передаваемых по каналам связи;

– кража носителей информации (магнитные диски, ленты, запоминающие устройства);

– несанкционированное копирование средств массовой информации;

– кража источников информации (распечатки, отчеты и другие);

– незаконное получение паролей и других реквизитов.

Таким образом, с учетом угроз конфиденциальности, целостности и доступности информации, угроза безопасности информации есть совокупность условий и факторов (явлений, действий или процессов), которые создают потенциальную опасность, в результате которого может произойти утечка информации, модификация (искажение, подмена), уничтожение информации или незаконное блокирование доступа к ней.

2 АНАЛИЗ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МЕЖРАЙОННОЙ ИФНС РОССИИ № 29 ПО РБ

2.1 Краткая характеристика Межрайонной ИФНС России № 29 по РБ

Межрайонная ИФНС России № 29 по РБ (Инспекция) является государственной организацией, которая выполняет функции, связанные с соблюдением гражданами и государством налогового законодательства РФ.

Задачами Инспекции являются:

– контроль за соблюдением законодательства о налогах и сборах;

– контроль за правильностью исчисления, за полнотой и своевременностью внесения государственных налогов в соответствующий бюджет;

– бесплатно информирует налогоплательщиков о действующих налогах и сборах;

– осуществляет государственную регистрацию юридических и физических лиц в качестве индивидуальных предпринимателей.

Инспекция обслуживает налогоплательщиков городов Нефтекамск, Агидель, Янаул, Балтачевского, Бураевского, Татышлинского, Янаульского, Калтасинского, Краснокамского районов Республики Башкортостан.

Структура Инспекции включает следующие отделы[14]:

– отдел информационных технологий;

– отдел камеральных проверок № 1;

– общий отдел;

– отдел обеспечения;

– отдел выездных проверок;

– отдел камеральных проверок № 2;

[14] Межрайонная инспекция ФНС России № 29 по РБ // NALOG.RU: Официальный сайт Федеральной налоговой службы. URL: https://www.nalog.ru/rn02/ifns/imns02_29/ (дата обращения 03.05.2019).

– отдел учета и работы с налогоплательщиками;

– отдел урегулирования задолженности и обеспечения процедур банкротства;

– правовой отдел;

– отдел кадров и безопасности;

– отдел предпроверочного анализа и истребования документов;

– отдел камеральных проверок № 3.

При реализации функций государственного управления и предоставлении государственных услуг в Инспекции обрабатывается информация, которая содержит сведения, составляющие налоговую, коммерческую, банковскую, служебную тайны и персональные данные.

Положение о категорировании информации и информационных ресурсов Инспекции устанавливает двенадцать категорий информации, представленных в таблице 1.

Таблица 1 – Категории информации

Группа	Вид информации	Категория информации (ресурса)	Рекомендуемый класс защищенности автоматизированной системы (подсистемы)
1	Налоговая тайна Коммерческая тайна Банковская тайна Профессиональная, адвокатская и иная, охраняемая законом тайна Персональные данные	И-4 (Р-4) И-5 (Р-5) И-6 (Р-6) И-7 (Р-7) И-8 (Р-8)	1В, 1Г
2	Служебная информация Общедоступная информация (предоставляемая)	И-9 (Р-9) И-10 (Р-10)	1Д
3	Рабочая (технологическая) информация Общедоступная информация (распространяемая)	И-11 (Р-11) И-12 (Р-12)	2Б или электронная подпись

Категории подразделяются на три группы, отличающиеся особенностями сбора, обработки, хранения, предоставления и распространения и, как следствие, подходом к выбору методов и средств ЗИ. Категорирование

информационного ресурса производится ответственным структурным подразделением, в ведении которого находится данный ресурс, на основе категорий информации, содержащихся в ресурсе, с привлечением Администратора ИБ.

Перечень информационных ресурсов утверждается руководителем (лицом его замещающим) налогового органа и ежегодно уточняется.

Инспекция имеет около 193 рабочих персональных компьютеров вместе с серверами, подключенных к локальной сети. Провайдером Интернета является компания ПАО «Ростелеком».

Отдел информационных технологий является структурным подразделением Инспекции, основной задачей которого является обеспечение информационной безопасности организации. Также данный отдел организует внедрение и эксплуатацию автоматизированной информационной системы по налогам и сборам АИС «Налог-3» на федеральном, региональном и местном уровнях на основе единой методологии, разработанной самой инспекцией.

Сотрудники отделов Инспекции ведут работу в АИС Налог-3. В данной системе обрабатывается большое количество важной информации, поэтому основное внимание было уделено исследованию системы обеспечения безопасности информации (СОБИ).

АИС «Налог-3» является единой информационной системой, обеспечивающей автоматизацию деятельности Инспекции по следующим функциям: прием, обработка, предоставление данных; анализ информации; формирование статистических данных и сведений для принятия управленческих решений.

Класс защищенности данной государственной информационной системы (ГИС): третий класс (К3). Уровень значимости (критичности) информации: третий (УЗ3).

В ГИС 3 класса защищенности должны применяться:

– средства защиты информации 6 класса;

– средства обнаружения вторжений и антивирусной защиты не ниже 4 класса;

– средства вычислительной техники не ниже 5 класса;

– межсетевой экран не ниже 3 класса.

Основными угрозами АИС Налог-3 являются следующие угрозы:

− компьютерные злоумышленники;

− криминальные элементы, террористы;

− сотрудники налоговых органов, являющиеся законными участниками процессов в АИС и действующие вне рамок предоставленных полномочий;

− сотрудники налоговых органов, являющиеся законными участниками процессов в АИС и действующие в рамках предоставленных полномочий, но в личных интересах;

− подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования АИС и его ремонт.

Для эффективной работы с документами в Инспекции внедрена система электронного документооборота «СЭД-регион» на платформе Lotus Notes/Domino. Документооборот включает в себя несколько этапов:

– прием и первичная обработка поступающих документов;

– предварительное рассмотрение документов уполномоченной службой;

– оформление документов;

– организация движения документов внутри организации (в том числе информационно-справочная работа, доведение документов до исполнителей, контроль их исполнения, а также утверждение и подписание проектов документов);

– обработка оформленных и отправляемых документов.

Весь документооборот налоговых органов состоит из потоков документов, представляющих собой поток документов, циркулирующих между

точками обработки и создания информации, и точками технической обработки документов: секретариатом, копировально-множительной службой[15].

Функции делопроизводства налоговой инспекции возложены на отдел общего и хозяйственного обеспечения. Права, обязанности и ответственность сотрудников отдела общего и хозяйственного обеспечения, а также работников других отделов, связанных с делопроизводством, определяются соответствующими должностными инструкциями.

Основным документом, регламентирующим документооборот в Инспекции, является Временная типовая инструкция по ведению делопроизводства в Управлении ФНС по Республике Башкортостан, разработанная на основе положений нормативных правовых и методических актов в области организации и введения делопроизводства.

Архитектура СЭД основана на иерархической структуре налоговых органов и содержит более 50 баз данных.

Главной особенностью СЭД является трехуровневая система канцелярий. Собственную канцелярию имеет не только начальник отдела, но и его заместители, а также руководители отделов. В связи с этим на уровне центрального аппарата и управлений действует многоканцелярская структура, которая позволяет работать с документами разных групп только тем пользователям, которые имеют определённые права доступа.

Сотрудники районных инспекций работают с базами данных «Канцелярия-ИФНС», созданными специально для каждой инспекции.

СЭД автоматически генерирует еженедельные реестры документов, доставленных и зарегистрированных в налоговых органах, которые передаются в центральный аппарат. Аналогичные реестры поступают от районных инспекций в соответствующий отдел.

Кроме того, такие базы данных, как «Для служебного пользования» (для документов с высокой степенью конфиденциальности) и «Заявления граждан»

[15] Информационная безопасность в налоговых органах Российской Федерации // CYBERLENINKA.RU: Научная электронная библиотека КиберЛенинка. URL: https://www.cyberleninka.ru/article/v/informatsionnaya-bezopasnost-v-nalogovyh-organah-rossiyskoy-federatsii (дата обращения 17.05.2019).

(для налогоплательщиков) разделены для центрального аппарата, управлений и инспекций.

Для обмена электронными, юридически значимыми документами между компаниями, с использованием электронной подписи в Инспекции используется СЭД «Счета-Фактуры», подсистема защиты которой обеспечивает выполнение всех требований к автоматизированным системам этого типа. Подсистема защиты информации СЭД «Счета-Фактуры» состоит из следующих подсистем:

– управление доступом к информационным ресурсам;

– регистрация и учет;

– обеспечение целостности;

– защита соединения;

– криптографическая защита информации;

– контроль эффективности информационной безопасности.

В то же время, защита информации обеспечивается набором программного и аппаратного обеспечения:

– комплексом средств защиты информации семейства ViPNet;

– инструментами аутентификации eToken, USB-ключ;

– криптографическими средствами защиты КриптоПРО CSP и КриптоАРМ;

– средствами мониторинга и отслеживания состояния различных сервисов компьютерной сети, серверов и сетевого оборудования;

– инструментами записи и мониторинга трафика (ведение журнала и аудит).

При собственноручном подписании документов, единственным подтверждением сделанной на нем подписи, может быть графологическая экспертиза.

Подпись, которая имеет удостоверяющую подлинность и авторство, называется неквалифицированной электронной подписью. Она может

использоваться как для внутреннего, так и для внешнего документооборота. Продукт изготовлен с использованием современных методов криптографической защиты. Для налоговой инспекции ЭП должна быть квалифицированной. Криптографические системы, используемые для ключей в этом цифровом подтверждении, сертифицируются органами безопасности после прохождения соответствующих проверок в ФСБ. Таким образом, использование квалифицированной ЭП ограничивает доступ к конфиденциальной информации и защищает её от кражи.

Важно учитывать, что, помимо отчетности для налоговиков, для взаимоотношений с другими органами (например, таможенными), а также с целью подписания электронных счетов-фактур, применяется именно квалифицированная ЭП. Для подписания же первичных бухгалтерских документов может применяться любая электронная подпись[16].

2.2 Анализ внутренних и внешних источников угроз информационной безопасности

В наши дни любая организация ставит перед собой главную задачу – обеспечение информационной безопасности. Система налоговой безопасности определяется как совокупность правовых, организационных, финансовых и институциональных отношений, организуемых государством в целях защиты финансовых интересов всех её субъектов от объективно существующих внешних и внутренних угроз. Угроза налоговой безопасности представляет собой совокупность условий и факторов, влияющих на устойчивость налоговой системы.

Базовая модель угроз информационной безопасности ФНС России определяет общие угрозы информационной безопасности: угрозы целостности

[16] О переходе Удостоверяющего центра ФНС России на выпуск квалифицированных сертификатов ключей проверки электронной подписи [Электронный ресурс]: Приказ от 11.12.2012 № ММВ-7-4/942@. Доступ из справ. - правовой системы «КонсультантПлюс».

данных – повреждение или уничтожение данных серверов вирусом; угроза конфиденциальности – незаконное раскрытие, утрата или повреждение информации; угрозы доступности информации – отказ в обслуживании из-за действий злоумышленников.

Нарушение одного из элементов может привести к ухудшению нормальной работы организации. Как внутренние, так и внешние угрозы влияют на производительность. Информационное общество стремительно развивается, поэтому можно сделать вывод о том, что количество источников угроз информационной безопасности растет.

Модель реализации угроз безопасности представлена на рисунке 1.

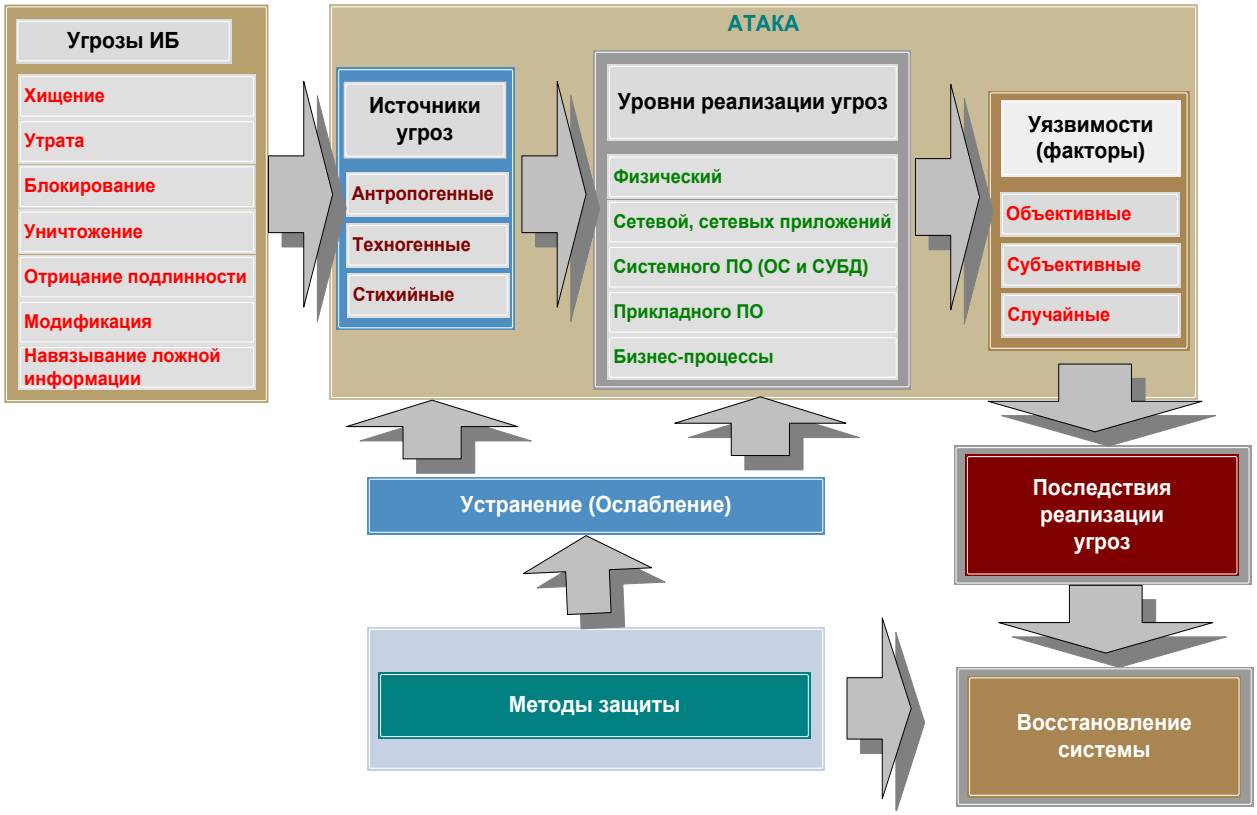


Рисунок 1 – Модель реализации угроз безопасности

Для объектов информатизации налоговых органов основными источниками угроз и уязвимостями информационной безопасности являются:

– иностранные службы технической разведки (для информации, содержащей государственные секреты);

– террористы, криминальные элементы;

– компьютерные злоумышленники, которые осуществляют целенаправленные разрушительные воздействия, в том числе с использованием компьютерных вирусов и других типов вредоносных кодов;

– подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования информационных систем налоговых органов и его ремонт;

– сотрудники налоговых органов, которые являются законными участниками процессов обработки информации и действуют вне рамок предоставленных полномочий;

– неблагоприятные события техногенного характера, в том числе аварии, вызванные средствами инженерных коммуникаций, объектами телекоммуникационной инфраструктуры, отказами оборудования;

– утечка информации по техническим каналам;

– внедрение электронных устройств с целью перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи;

– уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

– перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

– применение подслушивающих устройств, внедрение аппаратных устройств.

Для Межрайонной ИФНС № 29 России по РБ актуальными угрозами и уязвимостями на сегодняшний день остаются:

– сетевые атаки (атаки на рабочие станции инспекции);

– сотрудники налоговых органов, которые не соблюдают или нарушают меры безопасности при работе в информационных системах. Пользователь обязан блокировать доступ к своей рабочей станции, когда он покидает свое рабочее место. Часто происходит, что некоторые сотрудники забывают об этом.

Эта обязанность прописана в Политике безопасности рабочих станций и серверов и подлежит обязательному исполнению;

– сбои, отказы и аварии систем обеспечения (пропадание электропитания и как следствие отключение средств защиты);

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

– перехват (утечка) информации по каналам связи в ЛВС.

Прежде чем приступить к защите информационной системы, необходимо провести анализ рисков – оценку вероятности появления угрозы и определение необходимых затрат на её устранение. Для этого рассматриваются условия, при которых может возникнуть та или иная угроза, поэтому в первую очередь необходимо:

– определить, есть ли у организации информация, которую нельзя защищать;

– определить конкретную информацию, подлежащую защите, для чего и от кого её защищать, а также степень надежности такой защиты;

– определить полномочия конкретных лиц по доступу к информации.

Под уязвимостью информационной безопасности понимается совокупность условий и факторов, создающих потенциальный или реальный риск утечки защищаемой информации, несанкционированного или непреднамеренного воздействия на неё.

Моделирование процессов нарушения информационной безопасности осуществляется применительно к объекту информатизации на основе рассмотрения логической цепочки взаимодействия при реализации угрозы: «угроза – источник угрозы – уровень реализации – уязвимость – последствия». Источниками возникновения уязвимостей могут быть как субъекты (личность), так и объективные проявления.

В налоговой инспекции актуальными на сегодняшний день возможными уязвимостями могут быть:

– воздействие вредоносных программ и компьютерных вирусов на программное обеспечение;

– наличие программных и аппаратных уязвимостей;

– отказы технических средств, ошибки при подготовке и использовании программного обеспечения;

– установка несанкционированного программного обеспечения, нарушение порядка обработки и обмена информацией, хранения и уничтожения носителей информации;

– недостатки в организации охраны и технического укрепления объектов Инспекции, в том числе нарушения режима охраны (доступ к объекту, к техническим средствам).

При разработке, внедрении, эксплуатации и совершенствовании информационных объектов Инспекции, субъектам правоотношений могут быть нанесены следующие виды ущерба (вреда):

– материальный ущерб любому лицу от разглашения защищенной информации;

– моральный и материальный ущерб любому субъекту персональных данных от их разглашения или нарушения конституционных прав и свобод граждан;

– материальный и моральный ущерб от несвоевременного получения информации потребителями государственных информационных услуг или от нарушения целостности предоставленной информации.

Причиненный ущерб может быть классифицирован как преступление по уголовному праву или сопоставлен с рисками потери, предусмотренными гражданским, административным или арбитражным законодательством.

2.3 Система обеспечения информационной безопасности в Межрайонной ИФНС России № 29 по РБ

2.3.1 Комплекс организационных и правовых мер обеспечения информационной безопасности

Для обеспечения информационной безопасности налоговых органов созданы специальные отделы, которые в некоторых инспекциях носят режимный характер. Приказом Государственной налоговой службы России от 26 апреля 1993 г. № ВГ-3-12/32 в налоговых органах созданы отделы информатизации. С тех пор круг задач, решаемых этими отделами, значительно расширился[17].

Организационные методы в основном ориентированы на работу с личным составом, выбору места расположения объектов защиты, организацию физической защиты, противопожарной охраны, контроль за выполнением принятых мер, наложение персональной ответственности за выполнение мер защиты.

В Инспекции организован пропускной и внутриобъектовый режимы. Внутри здания объекта установлен турникет-трипод Perco KT 02.9B с биометрическим считывателем (отпечаток пальца), показанный на рисунке 2.

[17] Об образовании отделов информатизации в государственных налоговых инспекциях по республикам в составе Российской Федерации, краям, областям, автономным образованиям, городам Москве и Санкт-Петербургу [Электронный ресурс]: Приказ Госналогслужбы РФ от 26.04.1993 № ВГ-3-12/32. Доступ из справ. - правовой системы «КонсультантПлюс».

Рисунок 2 – Турникет-трипод Perco KT 02.9B

Более того для сотрудников Инспекции создаются пропуски в виде карты EM-Marine, позволяющие перемещаться по территории. В случае, если пропуск больше не используется сотрудником, следовательно, должен быть немедленно возвращен в отдел кадров и безопасности для последующего уничтожения. Замки от кабинетов опечатываются с устройством для опечатывания дверей, колба с ключами опечатывается и сдается сотруднику охраны по обеспечению пропускного и внутриобъектового режимов.

В инспекции регулярно проводятся проверки и инструктажи:

– инструктажи по гражданской обороне, пожарной безопасности, антитеррористической направленности, охране труда;

– ознакомление сотрудников под роспись об ответственности за разглашение конфиденциальной информации;

– практические тренировки по эвакуации персонала;

– проверка работоспособности средств контроля доступа, охранно-пожарной сигнализации, системы видеонаблюдения.

Помимо всего этого, разрабатываются инструкции и памятки о порядке действий в случае угрозы террористического акта, создаются информационные

стенды об угрозе терроризма, поддерживается оперативное взаимодействие с правоохранительными органами.

Основной частью обеспечения информационной безопасности является организация работы с документами. Это создание оптимальных условий для всех видов работ с документами, начиная с создания или получения документа, и заканчивая его уничтожением или передачей на архивное хранение. В органах ФНС на данный момент не предусмотрен отдел конфиденциального делопроизводства. За конфиденциальное, так и за открытое делопроизводство в Инспекции в целом отвечает уполномоченный сотрудник Общего отдела.

Основа правового обеспечения деятельности ФНС России устанавливается Налоговым кодексом Российской Федерации, внедряющим понятие налоговой тайны[18].

Правовые методы в основном направлены на устранение угроз, создаваемых антропогенными источниками, и являются основой для реализации всех других методов защиты[19].

Недостаточное правовое регулирование порядка обмена конфиденциальной информацией налоговых органов с субъектами, имеющими право на её получение, также приводит к её незаконному раскрытию. Положения Приказа Министерства по налогам и сборам «Об утверждении Порядка доступа к конфиденциальной информации налоговых органов» от 3 марта 2003 года № БГ-3-28/96 не содержат каких-либо ссылок на законодательные акты, устанавливающие санкции за раскрытие этой информации[20].

Нормативные акты условно можно разделить на две группы: непосредственно относящиеся к Межрайонной ИФНС России № 29 по РБ (на местном уровне) и к ФНС (на федеральном уровне).

---

[18] Налоговый кодекс РФ от 31.07.1998 № 146-ФЗ [Электронный ресурс]. Доступ из справ. - правовой системы «КонсультантПлюс».

[19] Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Рудановский М.В. Аудит информационной безопасности органов исполнительной власти. – 4 изд. – М.: Издательство «Флинта», 2016. – С. 44.

[20] Об утверждении Порядка доступа к конфиденциальной информации налоговых органов [Электронный ресурс]: Приказ МНС РФ от 03.03.2003 № БГ-3-28/96. Доступ из справ. - правовой системы «КонсультантПлюс».

Основными внутренними нормативными документами, относящимися к первой группе, являются:

– Политика по организации информационной безопасности;

– Модель угроз информационной безопасности на объекте информатизации;

– Политика безопасности рабочих станций и серверов;

– Порядок доступа к информационным, программным и аппаратным ресурсам объекта информатизации;

– Порядок использования глобальной сети Интернет и средств электронной почты;

– Политика управления парольной защитой;

– Положение об идентификации пользователей.

Вторая группа включает в себя:

– Концепцию информационной безопасности Федеральной налоговой службы, которая представляет собой систематическое изложение целей, задач, принципов построения организационных и технических аспектов информационной безопасности[21];

– Памятку сотрудника налогового органа по информационной безопасности;

– Приказ о резервном и архивном копировании баз данных;

– Приказ об обработке и защите персональных данных в Управлении Федеральной налоговой службы России по Республике Башкортостан;

– Приказ об утверждении Порядка использования электронных носителей информации;

– Приказ об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в налоговых органах;

– Инструкцию на рабочее место сотрудника;

[21] Об утверждении Концепции информационной безопасности Федеральной налоговой службы [Электронный ресурс]: Приказ ФНС России от 13.01.2012 № ММВ-7-4/6@. Доступ из справ. - правовой системы «КонсультантПлюс».

– Приказ об утверждении Типового порядка использования средств криптографической защиты информации и управления ключевой информацией в Управлении Федеральной налоговой службы по Республике Башкортостан;

– Руководство по организации информационной безопасности на объектах информатизации Федеральной налоговой службы;

– Перечень должностных лиц Федеральной налоговой службы, имеющих право доступа к служебной тайне и полномочиями, определенными их должностным регламентом.

Разумеется, все эти нормативные документы разрабатываются специалистами в области информационной безопасности совместно с соответствующими отделами организации, и после их утверждения руководством, подлежат также совместному контролю за их исполнением.

2.3.2 Анализ программно-аппаратных средств защиты информации для реализации основных методов защиты информации

Программно-аппаратные методы направлены на устранение проявления угроз, непосредственно связанных с процессом обработки и передачи информации в информационных системах налоговой инспекции. Без этих методов невозможно построить полноценную систему информационной безопасности. Содержание программно-аппаратных методов соответствует классам функциональных компонентов, перечисленных в ГОСТ Р ИСО/МЭК 15408-1-2012[22]. Внедрение программно-технических методов значительно снижает воздействие внутренних антропогенных источников угроз.

Вредоносная программа – компьютерная программа или переносимый код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе. Вредоносное программное обеспечение включает

[22] Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель [Электронный ресурс]: ГОСТ Р ИСО/МЭК 15408-1-2012 от 15.11.2012 № 814-ст. Доступ из справ. - правовой системы «КонсультантПлюс».

сетевых червей, классических файловых вирусов, троянов, хакерских утилит и других программ, наносящих ущерб компьютеру, на котором они запущены, или другим компьютерам в сети[23].

Независимо от типа вредоносные программы могут нанести значительный ущерб, реализуя любые угрозы информации – угрозы целостности, конфиденциальности, доступности. Место глобального распространения вредоносного программного обеспечения – это, конечно же, Интернет.

Защита рабочих станций и серверов от НСД является основой для обеспечения информационной безопасности инфраструктуры организации. Угрозы НСД приводят к утечке конфиденциальных данных и потере их целостности, что, в свою очередь, приводит к ряду негативных последствий для организации: от ущерба репутации и финансовых потерь, до приостановки бизнес-процессов.

Если организация работает с информацией ограниченного доступа, например, с личными данными или государственными секретами, то неизбежно сталкивается с многочисленными требованиями ФСТЭК и ФСБ России. Например, в ФСТЭК России включены требования по защите рабочих станций и серверов в обязательные для исполнения приказов: о защите персональных данных[24] и о защите ГИС[25].

Основным программно-аппаратным средством защиты информации в Инспекции является «Блокхост-сеть 2.0». Оно предназначено для комплексной и многофункциональной защиты информационно-программных ресурсов от НСД[26].

---

[23] Загинайлов Ю.Н. Основы информационной безопасности. – М.: Директ-Медиа, 2015. – С. 55.

[24] Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: Приказ ФСТЭК России от 18.02.2013 № 21. Доступ из справ. - правовой системы «КонсультантПлюс».

[25] Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс]: Приказ ФСТЭК России от 11.02.2013 № 17. Доступ из справ. - правовой системы «КонсультантПлюс».

[26] Комплексная защита информационных ресурсов рабочих станций и серверов «Блокхост-сеть 2.0» // GAZ-IS.RU: Официальный сайт Блокхост-сеть 2.0. URL: https://www.gaz-is.ru/produkty/zashchita-rabochih-stancii-i-serverov/blockhost-set.html (дата обращения 03.06.19).

Реализованные в СЗИ «Блокхост-сеть 2.0» механизмы ЗИ позволяют администратору безопасности решать следующие задачи:

– усиление защиты от НСД в систему;

– разграничение доступа пользователей к ресурсам;

– разграничение доступа к запуску программ;

– контроль целостности объектов файловой системы и реестра;

– контроль вывода информации на печать, маркировка документов;

– разграничение доступа пользователей к администрированию СЗИ;

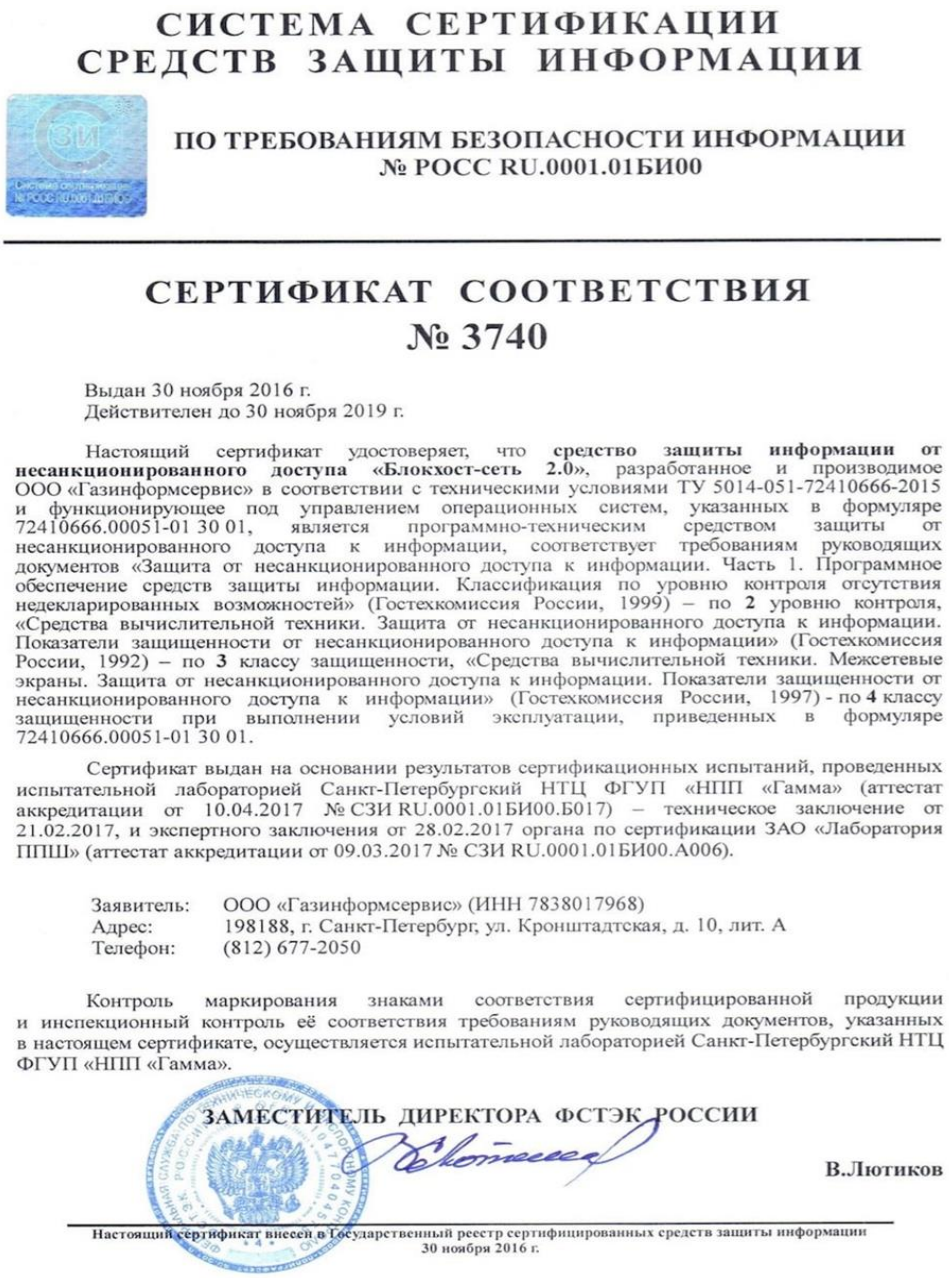
– контроль событий, связанных с безопасностью защищаемой информации;

– имеет двухфакторную аутентификацию.

Средство защиты информации «Блокхост-сеть 2.0» дополняет функциональные возможности операционной системы по ЗИ. Таким образом, информация защищается от НСД следующими компонентами, показанными на рисунке 3.

Рисунок 3 – Компоненты защиты от несанкционированного доступа

Блокхост-сеть 2.0 имеет сертификат ФСТЭК России № 3740 от 30 ноября 2016 года, который действителен до 30 ноября 2019 года. Данный сертификат представлен на рисунке 4.



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3740

Выдан 30 ноября 2016 г.
Действителен до 30 ноября 2019 г.

Настоящий сертификат удостоверяет, что **средство защиты информации от несанкционированного доступа «Блокхост-сеть 2.0»**, разработанное и производимое ООО «Газинформсервис» в соответствии с техническими условиями ТУ 5014-051-72410666-2015 и функционирующее под управлением операционных систем, указанных в формуляре 72410666.00051-01 30 01, является программно-техническим средством защиты от несанкционированного доступа к информации, соответствует требованиям руководящих документов «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по **2** уровню контроля, «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по **3** классу защищенности, «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) - по **4** классу защищенности при выполнении условий эксплуатации, приведенных в формуляре 72410666.00051-01 30 01.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией Санкт-Петербургский НТЦ ФГУП «НПП «Гамма» (аттестат аккредитации от 10.04.2017 № СЗИ RU.0001.01БИ00.Б017) – техническое заключение от 21.02.2017, и экспертного заключения от 28.02.2017 органа по сертификации ЗАО «Лаборатория ППШ» (аттестат аккредитации от 09.03.2017 № СЗИ RU.0001.01БИ00.А006).

Заявитель: ООО «Газинформсервис» (ИНН 7838017968)
Адрес: 198188, г. Санкт-Петербург, ул. Кронштадтская, д. 10, лит. А
Телефон: (812) 677-2050

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям руководящих документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией Санкт-Петербургский НТЦ ФГУП «НПП «Гамма».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
30 ноября 2016 г.

Рисунок 4 – Сертификат ФСТЭК России «Блокхост сеть 2.0»

Для защиты от вирусов, сетевых угроз в Инспекции применяется мощное антивирусное решение Kaspersky Endpoint Security, основными компонентами и задачами которого являются: файловый антивирус, почтовый антивирус, веб-

антивирус, сетевой экран, защита от сетевых атак, контроль запуска программ, мониторинг уязвимостей, контроль устройств, веб-контроль.

Для защиты компьютеров корпоративных пользователей в Инспекции применяется программный комплекс ViPNet, который позволяет организовывать защиту информации в крупных сетях и создавать защищенную, доверенную среду передачи информации ограниченного доступа с использованием публичных и выделенных каналов связи. Программное обеспечение направлено на решение двух важных задач информационной безопасности:

– создание защищенной, доверенной среды передачи информации ограниченного доступа с использованием публичных и выделенных каналов связи путем организации виртуальной частной сети (VPN);

– развертывание инфраструктуры открытых ключей (PKI) с организацией Удостоверяющего центра по использованию механизмов ЭП в прикладном программном обеспечении заказчика, с поддержкой возможности взаимодействия с PKI-продукцией других отечественных производителей.

Этот набор аппаратно-программных средств позволяет надежно обеспечивать и защищать информацию, передаваемую по каналам связи.

2.3.3 Средства криптографической защиты информации

Криптография является одним из наиболее надежных способов защиты информации, поскольку она защищает саму информацию, а не доступ к ней.

Средства криптографической защиты информации (СКЗИ) – аппаратные, программные средства, системы и комплексы, которые реализуют алгоритмы криптографического преобразования информации. Они предназначены для защиты информации при передаче по каналам связи и от НСД во время её обработки и хранении.

Основными СКЗИ в Инспекции являются КриптоПро CSP и Крито АРМ.

КриптоПро CSP предназначен для шифрования и расшифрования данных; создания и проверки ЭП; управления цифровыми сертификатами, ключами пользователя и криптопровайдерами; имеет возможность совместимости с ключевыми носителями eToken, Рутокен.

КриптоПРО CSP содержит следующие реализуемые алгоритмы:

– выработки значения хэш-функции;

– формирования и проверки ЭП;

– зашифрования и расшифрования данных, вычисление имитовставки.

КриптоАРМ используется во многих информационных системах, в которых требуется обеспечить:

– надежную защиту данных от НСД;

– подлинность и авторство электронных документов;

– согласовывать электронных документов;

– целостность данных при их передаче по незащищенным каналам связи.

Для обмена данными между налогоплательщиками и налоговыми органами по электронной почте через Интернет в Инспекции применяется почтовая программа «DioPost». В эту программу внедрен модуль криптографической защиты, отправленные файлы подписываются электронной подписью и зашифровываются криптографическими средствами с гарантированной стойкостью для защиты от несанкционированного просмотра и искажения. Программа «DioPost» настроена на соблюдение правил регламента электронного документооборота между налогоплательщиками и налоговыми инспекциями. Все нормативные действия со стороны налогоплательщика обрабатываются автоматически.

Модуль криптографической защиты информации в составе «DioPost» осуществляет шифрование файлов и их защиту с использованием ЭП. Этот модуль автоматически вызывается программой «DioPost» в процессе подготовки файлов отчетности к отправке. Модуль сертифицирован Федеральным агентством правительственной связи и информации при

Президенте РФ (ФАПСИ) на право использования для защиты информации, не содержащей государственной тайны.

2.3.4 Инженерно-техническая защита информации от утечки по каналам связи

Инженерно-технические методы основаны на применении специальных технических СЗИ, контроля ситуации и ориентированы на устранение угроз, связанных с действиями внешних антропогенных источников угроз информации с помощью технических средств. Некоторые из этих методов позволяют устранить влияние техногенных источников угроз и уменьшить влияние объективных, субъективных и случайных уязвимостей.

Можно выделить три направления работ по защите информации:

– разработка СЗИ;

– теоретические исследования;

– обоснование способов использования СЗИ.

Большинство из этих способов защиты реализованы с использованием криптографических методов.

Методы защиты от НСД сети включают в себя:

– абонентское шифрование;

– шифрование пакетов;

– криптографическую аутентификацию абонентов;

– электронную подпись.

Одним из таких средств в Межрайонной ИФНС № 29 России по РБ является широкополосный генератор помех для телефонных линий «SP-17D/SI-2060», представленный на рисунке 5. Данное устройство защиты телефонной линии позволяет предотвратить прослушивание переговоров от телефонного аппарата до автоматической телефонной станции (АТС).

Рисунок 5 – Широкополосный генератор помех «SP-17D/SI-2060»

Прибор обеспечивает эффективное противодействие следующим средствам несанкционированного съема информации:

– телефонным радиопередатчикам;

– аппаратуре магнитной записи, подключаемые к линии через контактные адаптеры или индуктивные датчики;

– микрофонам, радиомикрофонам.

3 СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В МЕЖРАЙОННОЙ ИФНС РОССИИ № 29 ПО РБ

Сотрудники отделов Инспекции ведут работу в АИС Налог-3. В данной системе обрабатывается большое количество важной информации, поэтому основное внимание было уделено исследованию системы обеспечения безопасности информации (СОБИ) АИС Налог-3.

АИС «Налог-3» является единой информационной системой, которая обеспечивает автоматизацию деятельности Инспекции по таким выполняемым функциям, как: прием, обработка, предоставление данных, анализ информации, формирование статистических данных и сведений.

Класс защищенности государственной информационной системы: третий класс (К3). Уровень значимости (критичности) информации: третий (УЗ3).

Исследование СОБИ было выполнено по архитектуре, представленной на рисунке 6. Она включает в себя:

– организационную базу (должностные лица, пользователи АИС Налог-3);

– исполнительный механизм (встроенные в ПО АИС Налог-3 функции безопасности, технические СЗИ, средства мониторинга и аудита);

– комплекс организационных, инженерно-технических, технических мер.

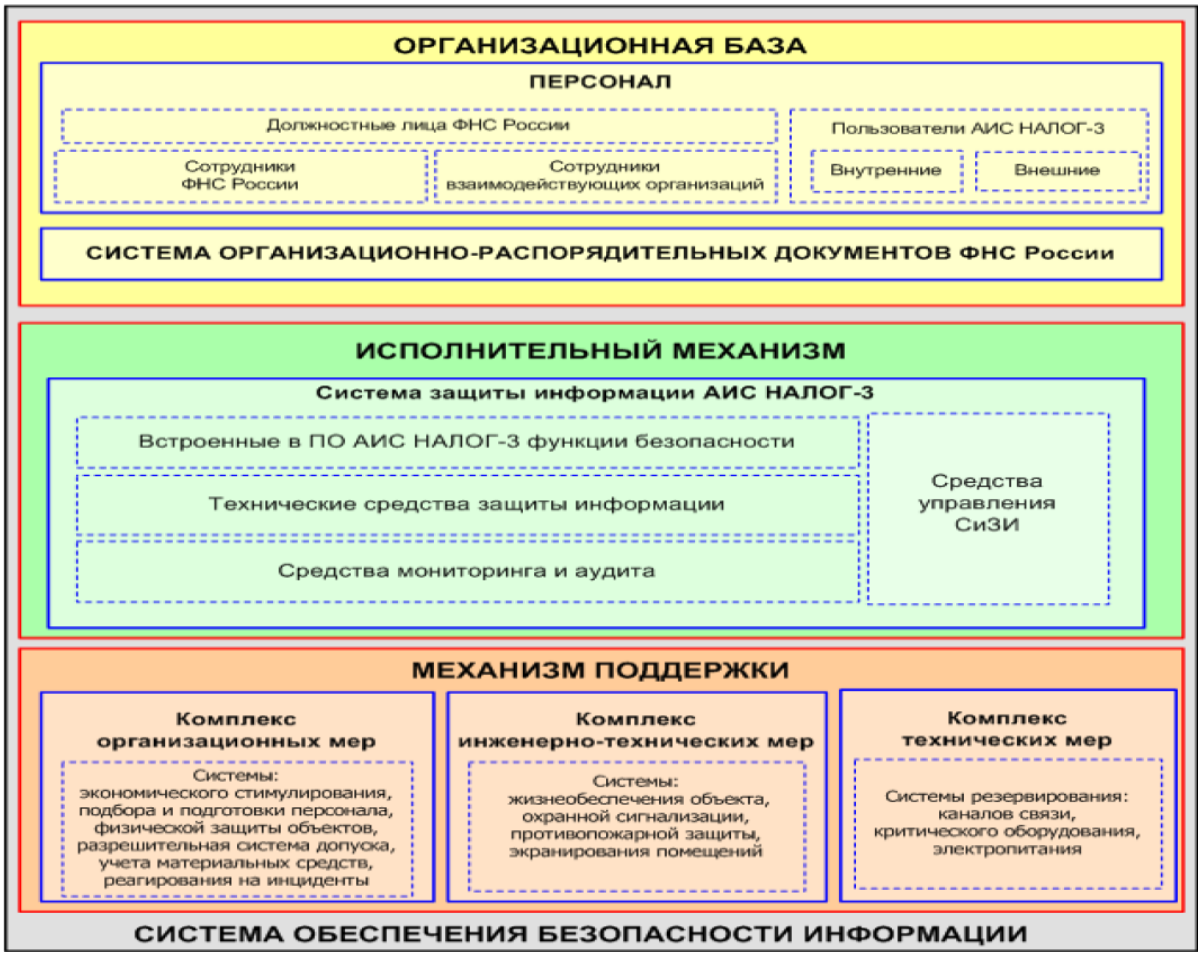


Рисунок 6 – Архитектура системы обеспечения безопасности информации

Комплекс организационных и инженерно-технических мер в Инспекции включает в себя:

– физическую защиту объектов. Внутри здания объекта в коридорах установлены купольные IP-видеокамеры RVI-IPC34VM4, на территории объекта уличные видеокамеры RVI-165C, представленные на рисунке 7. Некоторые видеокамеры оснащены с датчиками движения, которые начинают функционировать после включения «режима охраны». Видеозапись с камер видеонаблюдения хранится 30 дней. Недостатком физической защиты объекта является то, что отсутствует охрана окон (решетки на окнах, датчики разбития окон);

Рисунок 7 – Видеокамеры RVI-IPC34VM4 и RVI-165C

– систему жизнеобеспечения объекта. Вентиляционные установки, кондиционеры, устройства пожаротушения, оборудования систем электроснабжения и освещения установлены в Инспекции и полностью находятся в рабочем состоянии;

– систему охранной сигнализации и противопожарной защиты. В Инспекции она функционирует и состоит из следующих устройств: устройство оконечное объектовое приемно-контрольное ВЭРС-ПК 4; блок радиоканальный объектовый Струна-5 БРО-4-GSM; контроллер двухпроводной линии связи С2000-КДЛ, оптико-электронные извещатели ИП 212-4С и другие.

Технические меры в Инспекции обеспечены:

– системой резервирования каналов связи. Есть возможность подключения на резервный канал связи через спутник;

– системой резервирования критического оборудования, электропитания. В Инспекции применяются источники бесперебойного питания СКАТ-1200 сугубо для охранно-пожарной сигнализации и системы видеонаблюдения, а для серверов источники бесперебойного питания ИБПС-24-2000. Данные системы представлены на рисунке 8.

Рисунок 8 – Источники бесперебойного питания СКАТ-1200 и ИБПС-24-2000

В целях совершенствования СОБИ были разработаны следующие рекомендации.

Для усиления существующей программно-аппаратной защиты было предложено СЗИ от НСД Secret Net Studio. Сравнивая функциональные возможности и ценовые характеристики установленного и предлагаемого комплекса, можно сделать вывод о том, что стоимость Secret Net Studio не значительно выше, при условии, что его функционал на много выше. Исходя из этого, рекомендовано использование Secret Net Studio. Сравнительный анализ приведен в таблице 2.

Таблица 2 – Сравнение функциональных и ценовых характеристик двух продуктов

Возможности по защите информации	СЗИ от НСД «Блокхост-сеть 2.0»	СЗИ от НСД «Secret Net Studio»
Антивирусная защита	нет	есть
Контроль целостности данных	есть	есть
Межсетевое экранирование (брандмауэр или firewall)	нет	есть
Двухфакторная аутентификация	есть	есть
Контроль доступа к объектам при сетевых обращениях	есть	нет
Шифрование контейнеров	нет	есть

Продолжение таблицы 2

Контроль печати	есть	есть
Обнаружение и предотвращение вторжений	нет	есть
Наличие глобальных политик (установка прав по умолчанию на объекты, доступ к которым не был настроен)	есть	нет
Контроль устройств	есть	есть
Теневое копирование	нет	есть
Дискреционный и мандатный механизмы контроля доступа	есть	есть
Возможность удаленного администрирования средствами клиентской части	есть	нет
Авторизация сетевых соединений	нет	есть
Стоимость продукта (одна лицензия)	7918 руб.	6035 руб.

Комплексное решение для обеспечения безопасности рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования имеет следующие механизмы защиты информации, показанные на рисунке 9.

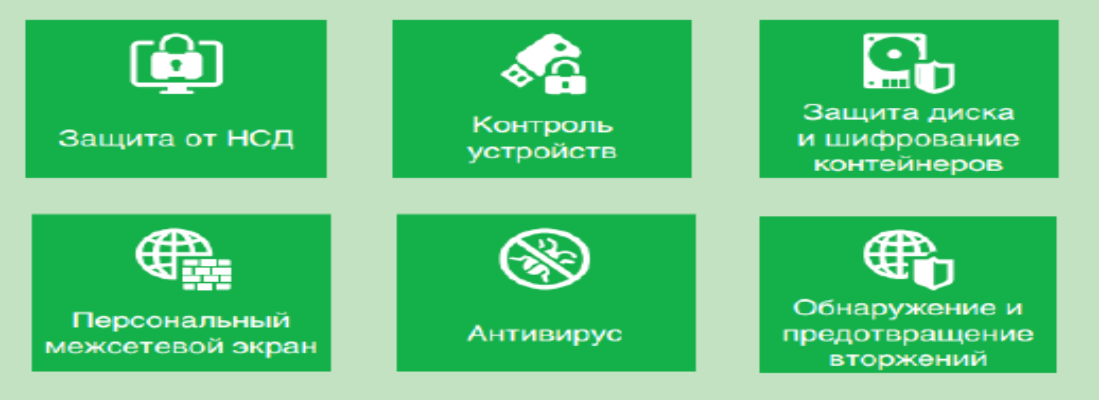


Рисунок 9 – Основные механизмы защиты информации

Концепция продукта выделяет следующую взаимосвязь задач, показанную на рисунке 10.

Рисунок 10 – Концепция продукта

Secret Net имеет сертификат соответствия ФСТЭК России № 3745, который действителен до 16.05.2020 и соответствует СВТ-5, СКСН-4 (уровень подключения), МЭ-4 (тип «В»), СОВ-4 (уровень узла), САВЗ-4 (все типы), НДВ-4. Может применяться в АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно.

Минимальные системные требования к компьютерам (рабочим станциям) на которых предлагается установить Secret Net Studio, показаны на рисунке 11.

КЛИЕНТ

№	Аппаратный ресурс	Secret Net Studio
1	Процессор	В соответствии с требованиями ОС
2	Оперативная память	2 Гб (Рекомендуется 4 Гб)
3	Жесткий диск (свободное пространство)	4 Гб

СЕРВЕР БЕЗОПАСНОСТИ

№	Аппаратный ресурс	Secret Net Studio
1	Процессор	В соответствии с требованиями ОС (Рекомендуется Intel Core i5 / Xeon E3 и выше)
2	Оперативная память	8 Гб (Рекомендуется 16 Гб)
3	Жесткий диск (свободное пространство)	150 Гб (Рекомендуется SSD-диск)

Рисунок 11 – Системные требования Secret Net Studio

Таким образом, при использовании имеющихся и рекомендованных мер по защите информации, будет усовершенствована система обеспечения информационной безопасности в рассматриваемой налоговой инспекции.

ЗАКЛЮЧЕНИЕ

В выпускной квалификационной работе исследована система обеспечения безопасности информации и даны рекомендации по её совершенствованию.

Практический материал по выпускной квалификационной работе был собран во время прохождения преддипломной практики в отделе информационных технологий в Межрайонной ИФНС России № 29 по РБ.

В ходе анализа объекта были изучены организационная структура организации, локальные нормативно-правовые документы в области защиты информации, рассмотрен комплекс применяемых организационных, инженерно-технических мер защиты информации, программно-аппаратные и криптографические средства защиты информации.

Основной государственной информационной системой в Инспекции является АИС Налог-3. Многие сотрудники отделов ведут работу в данной системе, с помощью которой происходит прием, обработка, предоставление данных и анализ информации. Система обеспечения безопасности информации включает организационную базу (должностные лица, пользователи АИС Налог-3); исполнительный механизм (встроенные в ПО АИС Налог-3 функции безопасности, технические СЗИ, средства мониторинга и аудита); механизм поддержки, включающий в себя комплекс организационных, инженерно-технических и технических мер по защите информации.

Установленные программно-аппаратные и криптографические СЗИ в Инспекции являются сертифицированными ФСТЭК и ФСБ России и отвечают требованиям безопасности, предъявляемым к государственным информационным системам 3-го класса.

Для усиления существующей системы защиты было предложено использование на рабочих станциях СЗИ Secret Net Studio, которое оснащено дополнительными механизмами защиты: антивирусная защита, межсетевое

экранирование, шифрование контейнеров, авторизация сетевых соединений, обнаружение и предотвращение вторжений.

Secret Net Studio имеет сертификат соответствия ФСТЭК России № 3745 от 16.05.2017 г., который действителен до 16.05.2020 г. и соответствует требованиям РД по 4 уровню контроля; 4 классу защиты САВЗ, СОВ, МЭ; 5 классу СВТ. Может применяться в автоматизированных системах до класса 1 включительно.

В рассматриваемой организации имеется большое количество информации конфиденциального характера, доступ к которой необходимо ограничивать, поэтому, основной целью специалиста по информационной безопасности является разработка и дальнейшее совершенствование такой системы по защите информации, при которой угрозы утечки конфиденциальной информации были бы минимальны.

Из вышеизложенного следует вывод о том, что необходимо уделить больше внимания к защите конфиденциальной информации налоговых органов, подбору компетентных специалистов в области информационной безопасности.

По результатам можно сказать, что защита информации в инспекции отвечает стандартам эффективности защиты информации. В каждой сфере, будь то конфиденциальная информация, документы для служебного пользования и другие, имеется ответственный отдел и закрепленный персонал.

Таким образом, был проведен анализ системы обеспечения информационной безопасности, результатом которого стали разработанные рекомендации, которые позволяют усовершенствовать имеющуюся систему защиты информации и повысить общий уровень обеспечения информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Нормативные акты

1. Конституция Российской Федерации от 12 декабря 1993 г. [ред. от 21.07.2014] // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 19.04.2019.

2. Налоговый кодекс Российской Федерации от 31 июля 1998 г. № 146-ФЗ [ред. от 01.05.2019] // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 07.05.2019.

3. Постановление Правительства РФ от 03 ноября 1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» [ред. от 18.03.2016] // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 19.04.2019.

4. Приказ Госналогслужбы РФ от 26 апреля 1993 № ВГ-3-12/32 «Об образовании отделов информатизации в государственных налоговых инспекциях по республикам в составе Российской Федерации, краям, областям, автономным образованиям, городам Москве и Санкт-Петербургу» [ред. от 16.06.1999] // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 17.05.2019.

5. Приказ МНС РФ от 3 марта 2003 № БГ-3-28/96 «Об утверждении Порядка доступа к конфиденциальной информации налоговых органов» // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 17.05.2019.

6. Приказ от 11 декабря 2012 № ММВ-7-4/942@ «О переходе Удостоверяющего центра ФНС России на выпуск квалифицированных сертификатов ключей проверки электронной подписи» // справ.-правовая

система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 08.05.2019.

7. Приказ ФНС России от 13 января 2012 № ММВ-7-4/6@ «Об утверждении Концепции информационной безопасности Федеральной налоговой службы» // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 20.05.2019.

8. Приказ ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [ред. от 15.02.2017] // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 21.05.2019.

9. Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [ред. от 23.03.2017] // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 21.05.2019.

10. Закон РФ от 21 июля 1993 № 5485-1 «О государственной тайне» [ред. от 29.07.2018] // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 19.04.2019.

11. Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [ред. от 18.03.2019] // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 19.04.2019.

12. Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных» [ред. от 31.12.2017] // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 19.04.2019.

13. Федеральный закон от 29 июля 2004 № 98-ФЗ «О коммерческой тайне» [ред. от 18.04.2018] // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 19.04.2019.

14. Федеральный закон от 6 апреля 2011 № 63-ФЗ «Об электронной подписи» [ред. от 23.06.2016] // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 19.04.2019.

15. Указ Президента РФ от 5 декабря 2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 19.04.2019.

16. ГОСТ Р 50922-2006 от 27 декабря 2006 № 373-ст «Защита информации. Основные термины и определения» // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 18.04.2019.

17. ГОСТ Р ИСО/МЭК 15408-1-2012 от 15 ноября 2012 № 814-ст «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. – Послед. обновление 07.05.2019.

Книги

18. Аверченков, В.И. Аудит информационной безопасности органов исполнительной власти: учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. – 4 изд. – М.: Издательство «Флинта», 2016. – 100 с.

19. Громов, Ю.Ю. Программно-аппаратные средства защиты информационных систем: учебное пособие / Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков. – Тамбов.: Издательство ФГБОУ ВПО «ТГТУ», 2017. – 194 с.

20. Загинайлов, Ю.Н. Основы информационной безопасности: учебное пособие / Ю.Н. Загинайлов. – М.: Директ-Медиа, 2015. – 105 с.

21. Ковалев, Д.В. Информационная безопасность: учебное пособие / Д.В. Ковалев, Е.А. Богданова. – Ростов-на-Дону.: Издательство Южного федерального университета, 2016. – 74 с.

22. Петренко, В.И. Теоретические основы защиты информации / В.И. Петренко. – Ставрополь.: СКФУ, 2015. – 222 с.

23. Уткин, В.Б. Информационные системы и технологии в экономике / В.Б. Уткин, К.В. Балдин. – М.: Юнити-Дана, 2015. – 336 с.

Материалы из сети Интернет

24. Информационная безопасность в налоговых органах Российской Федерации [Электронный ресурс] / CYBERLENINKA.RU: Научная электронная библиотека КиберЛенинка. – Электрон. дан. URL: https://www.cyberleninka.ru/article/v/informatsionnaya-bezopasnost-v-nalogovyh-organah-rossiyskoy-federatsii (дата обращения 17.05.2019). – Загл. с экрана.

25. Комплексная защита информационных ресурсов рабочих станций и серверов «Блокхост-сеть 2.0» [Электронный ресурс] / GAZ-IS.RU: Официальный сайт Блокхост-сеть 2.0. – Электрон. дан. URL: https://www.gaz-is.ru/produkty/zashchita-rabochih-stancii-i-serverov/blockhost-set.html (дата обращения 21.05.2019). – Загл. с экрана.

26. Межрайонная инспекция ФНС России № 29 по РБ [Электронный ресурс] / NALOG.RU: Официальный сайт Федеральной налоговой службы. – Электрон. дан. URL: https://www.nalog.ru/rn02/ifns/imns02_29/ (дата обращения 03.05.2019). – Загл. с экрана.