МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ СОЦИАЛЬНО-ГУМАНИТАРНЫХ НАУК

Кафедра документоведения и документационного обеспечения управления

Заведующий кафедрой
канд. техн. наук
А.М. Петров

ВЫПУСКНАЯ КВАЛИФИКАЦИННАЯ РАБОТА
магистра

ПРОЕКТИРОВАНИЕ КОМПЛЕКСА ДОКУМЕНТАЦИИ ПО РЕГЛАМЕНТАЦИИ УПРАВЛЕНЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ ТЮМЕНСКОЙ ОБЛАСТИ «ГОСУДАРСТВЕННЫЙ АРХИВ ТЮМЕНСКОЙ ОБЛАСТИ»

46.04.02 Документоведение и архивоведение

Магистерская программа «Документационное обеспечение управления»

Выполнила работу
Студентка 3 курса
заочной формы обучения — Дроздова Екатерина Юрьевна

Научный руководитель
канд. ист. наук, доцент — Кондратьева Тамара Николаевна

Рецензент
Заместитель директора ГБУТО
«Государственный архив
Тюменской области» — Черепнева Ольга Владимировна

Тюмень
2021

ОГЛАВЛЕНИЕ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АРМ	–	автоматизированное рабочее место
ВНИИДАД	–	Всероссийский научно-исследовательский институт документоведения и архивного дела
г.	–	год
г.	–	город
ГАТО	–	Государственный архив Тюменской области
ГБУТО	–	Государственное бюджетное учреждение Тюменской области
госархив	–	государственный архив
ГОСТ	–	государственный стандарт
Гостехкомиссия	–	Государтвенная техническая комиссия
ГУТО	–	Государственное учреждение Тюменской области
ИСПДн	–	информационная система персональных данных
ЛВС	–	локальная вычислительная сеть
Минкомсвязь	–	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Минтруд	–	Министерство труда и социальной защиты Российской Федерации
НСД	–	несанкционированный доступ
облгосархив	–	областной государственный архив
ООО	–	Общество с ограниченной ответственностью
ОИПСиЗИ	–	Отдел информационно-поисковых систем и защиты информации
ПДн	–	персональные данные
ПК	–	персональный компьютер
ПО	–	программное обеспечение
пр.	–	проезд

ПЭМИН	–	побочные электромагнитные излучения и наводки
Рис.	–	рисунок
Росархив	–	Федеральное архивное агентство
Росздравнадзор	–	Федеральная служба по надзору в сфере здравоохранения
Росстат	–	Федеральная служба государственной статистики
Роструд	–	Федеральная служба по труду и занятости
РФ	–	Российская Федерация
с.	–	страница
СЗИ	–	средства защиты информации
СИБИД	–	Система стандартов по информации, библиотечному и издательскому делу
СКЗИ	–	средства криптографической защиты информации
СЭД	–	система электронного документооборота
т.е.	–	то есть
т.о.	–	таким образом
т.ч.	–	том числе
ФЗ	–	федеральный закон
ФМБА	–	Федеральное агентстве железнодорожного транспорта
ФСТЭК	–	Федеральная служба по техническому и экспортному контролю
ч.	–	час

ВВЕДЕНИЕ

В современном мире информационные потоки являются неотъемлемой частью жизни и деятельности каждого индивидуума. Они помогают дать оценку происходящим событиям, принять обдуманное решение, выбрать наиболее подходящий путь решения задач. С течением времени информация стала группироваться на виды, подразделяться на классы, выделялись характерные признаки каждого из них. Однако, вместе с этим возникла и потребность в обеспечении сохранности информационных массивов. Данная тенденция особенно стала актуальна для предприятий и учреждений, так как защита различного рода сведений для них является одним из внутренних направлений внутренней деятельности, ведь их разглашение или изменение может привести к значительному ущербу.

Несомненно, любая деятельность человека, в особенности трудовая, имеет документальное подтверждение. Исходя из статьи 2 ФЗ № 149 информацией можно назвать любые сведения, или же сообщения, данные – вне зависимости от формы их представления [Об информации…]. Согласно госстандарту на термины и определения информацию, которая была зафиксирована любым способом на каком-либо носителе и имеет реквизиты, что позволяют её идентифицировать, принято называть документом [ГОСТ Р 7.0.8-2013]. Таким образом, можно прийти к заключению о том, что объектом проводимого комплекса мероприятий по защите информации можно считать именно документ или же целый комплекс документов.

Как правило, практически любой вид документации, создаваемой в организации, а в особенности документы, содержащие сведения, охраняемые в соответствии с законодательством (персональные данные, переписка, различные виды тайн), требует защиты от внесения в неё изменений или ознакомления с ней третьих лиц. Деятельность по защите информации предполагает осуществление такой деятельности, которая была бы нацелена на предотвращение возможной утечки подлежащей защите информации, реализации несанкционированных, а

также предупреждению непреднамеренных воздействий на неё [ГОСТ Р 50922-2006]. Существующей практикой организации системы обеспечения безопасности данных в российских учреждениях и действующими нормативными актами Российской Федерации созданы предпосылки для внедрения на локальном уровне документального комплекса, закрепляющего основные направления такой защиты.

Объектом проводимого исследования является организационно-правовая документация ГБУТО ГАТО, регламентирующая отдельные направления деятельности госархива в области защиты информации, а также существующий порядок документирования процессов осуществления отдельных процедур в области обеспечения информационной безопасности в Государственном бюджетном учреждении Тюменской области «Государственный архив Тюменской области».

Под архивом понимается организация или выделенное в её структуре подразделение, в функционал которого входит осуществления хранения, организация комплектования, проведение учёта и обеспечение условий для использования архивных документов [Об архивном деле…]. ГБУТО «Государственный архив Тюменской области» (далее – Тюменский облгосархив, госархив, ГБУТО ГАТО) создано в целях обеспечения реализации продиктованных российским законодательством полномочий органов государственной власти Тюменской области в архивной сфере. Основными задачами деятельности госархива являются:

- формирование архивного фонда Тюменской области;
- обеспечение сохранности документов архивного фонда;
- оказание информационных услуг;
- обеспечение доступа пользователей к информации, содержащейся в архивных документах;
- эффективное использование имеющихся ресурсов и материальных средств [О создании…].

К основной деятельности этого областного архивного учреждения относятся также такие обязательные для всех организаций виды работ, как ведение кадрового и бухгалтерского учёта, контроль за охранным и пожарным состоянием помещений и др. В рамках реализации основных функций в ГБУТО «Государственный архив Тюменской области» их выполнение разделено между специалистами управленческого звена, условно выделенными в группу с названием «Администрация» и пятью отделами согласно утверждённому штатному расписанию [Штатное расписание ГБУТО ГАТО]. Структура организации представлена в рисунке 1.

Рисунок 1

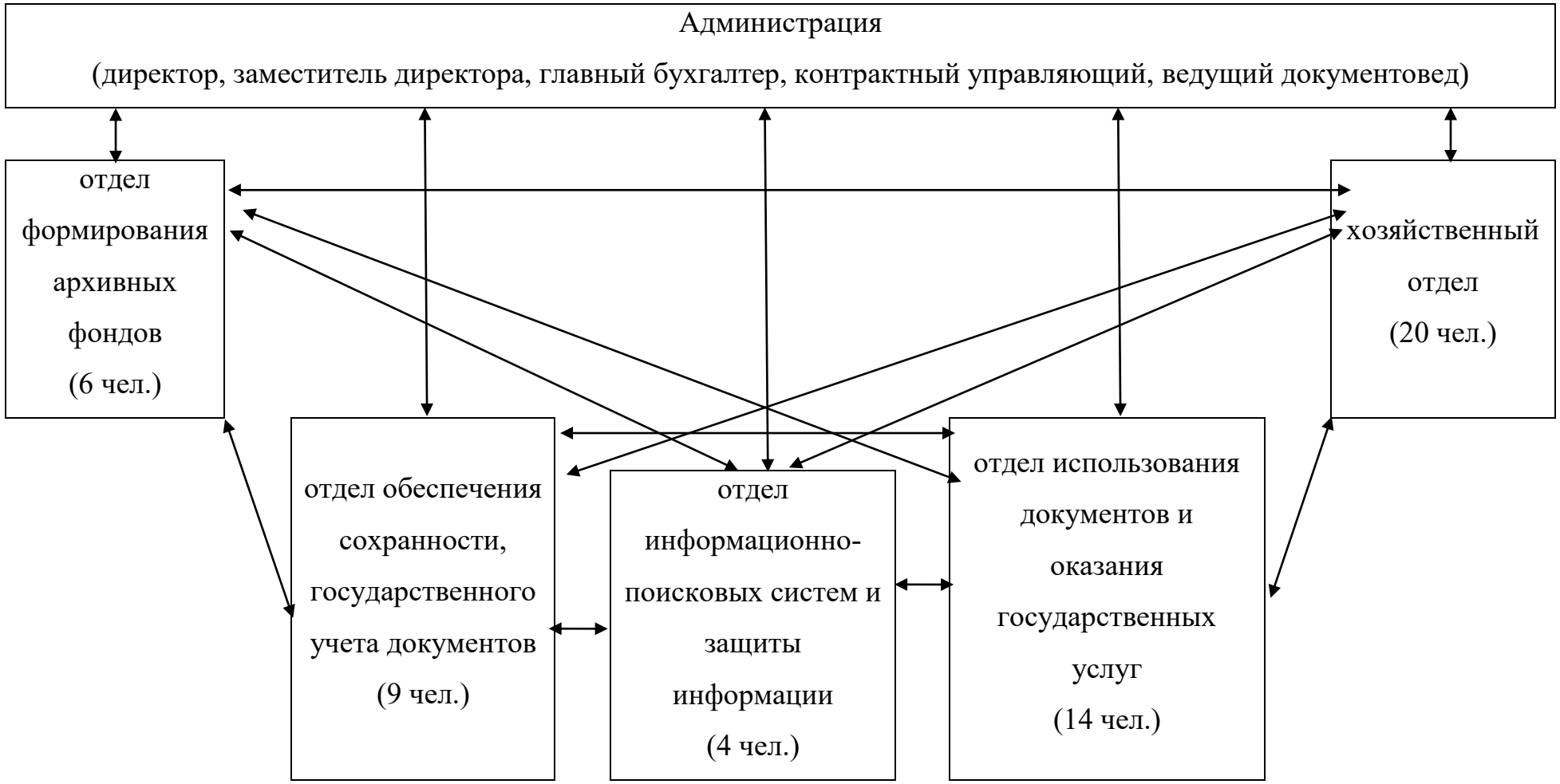


Рис. 1. Структура Государственного бюджетного учреждения Тюменской области «Государственный архив Тюменской области»

В связи с возложенными на учреждение функциями потребность в защите информации является первостепенной, причём вопросы безопасности данных касаются не только документов, являющихся частью Архивного фонда Тюменской области, но и тех, что создаются в текущей деятельности и касаются непосредственно внутренней работы ГБУТО ГАТО. Именно рассмотрению отдельных аспектов обеспечения информационной безопасности в процессе осуществления текущей деятельности госархива (кадровой, бухгалтерской работы, работы с аппаратным и программным обеспечением и др.) посвящена выпускная квалификационная работа, в связи с чем была выбрана следующая формулировка темы – «*Проектирование комплекса документации по регламентации управленческой деятельности в области защиты информации в Государственном бюджетном учреждении Тюменской области «Государственный архив Тюменской области*».

Стоит отметить, что такое направление деятельности, как защита информации в архивных учреждениях предполагает две области развития – внутреннюю, направленную на защиту служебной информации, данных о сотрудниках и обеспечение безопасной работы с документацией и при использовании программных и аппаратных средств в учреждении, а также внешнюю, ориентированную на регламентацию процесса обеспечения информационной безопасности заявителей, обратившихся в госархив с запросами, а также пользователей, осуществляющих работу в читальном зале ГБУТО ГАТО или в Программном комплексе автоматизированной информационной системы «Электронный архив Тюменской области». В данной работе акцент сделан на обеспечение внутренней безопасности, т.к. она представляет основополагающее значение в построении эффективной системы защиты информации организации и должна быть усовершенствована в первую очередь.

Непосредственное участие в решении вопросов защиты информации Тюменского облгосархива принимают заместитель директора ГБУТО ГАТО, системный администратор и администратор информационной безопасности

вычислительной сети отдела информационно-поисковых систем и защиты информации. Участие в разработке отдельных документов в области защиты сведений ограниченного доступа принимают также главный бухгалтер и ведущий документовед администрации – выступающие в качестве должностных лиц, назначенных ответственными за такие направления деятельности, как организация и обработка персональных данных в учреждении.

Однако осуществление всех основных видов работ в области защиты информации в соответствии с положением об отделе находятся в ведении отдела информационно-поисковых систем и защиты информации ГБУТО «Государственный архив Тюменской области», т.к. именно в нём осуществляет работу большинство занятых защитой информации сотрудников [Положение об ОИПСиЗИ…]. Штатная численность отдела определяется штатным расписанием архива в соответствии с задачами и объёмом выполняемых отделом работ. В настоящее время отдел состоит из четырёх сотрудников: структурное подразделение возглавляет начальник, в его подчинении находятся системный администратор, администратор информационной безопасности вычислительной сети и главный архивист [Штатное расписание…].

Администраторы в соответствии с возложенными на отдел задачами осуществляют следующие функции:

- проведение мероприятий по контролю за состоянием и обеспечением работоспособности работы аппаратного и программного обеспечения госархива;
- организация комплексной защиты информации, предупреждение несанкционированного доступа к информационным ресурсам ГБУТО ГАТО;
- контроль за использованием сетевых ресурсов, обеспечение сетевой безопасности и безопасности межсетевого взаимодействия;
- обеспечение безопасного доступа к внутренней локальной сети и глобальным сетям;
- своевременное копирование и резервирование данных;

- антивирусная защита внутренней локальной сети архива;
- регистрация идентификаторов (имён) и аутентификаторов (паролей) пользователей, обучение и консультации пользователей по вопросам работы в сети, программном и аппаратном обеспечении;
- обеспечение безопасности данных персонального характера при их обработке в информационных системах персональных данных архива;
- осуществление работ по реализации мероприятий по классификации и проведению аттестации объектов информационных систем персональных данных архива;
- регулярный периодический контроль за соблюдением правил использования средств защиты информации, предусмотренной технической
  и эксплуатационной документацией [Положение об ОИПСиЗИ…].

В связи с неукомплектованностью штата отдела и занятостью других сотрудников, отвечающих за различные направления защиты информации госархива, данный вид работы не проводился с 2016 г. – отсутствует какой-либо анализ существующей системы документации Тюменского облгосархива и принимаемых мер по защите сведений ограниченного доступа. За этот период изменились принципы выполнения отдельных видов работ, неоднократно обновлялось программное и аппаратное обеспечение, были внесены изменения в отечественном законодательные и нормативные акты в области защиты данных.

Таким образом, *актуальность* данной работы обуславливается сложившейся ситуацией недостаточности нормативной регламентации вопросов обеспечения информационной безопасности в документации госархива при осуществлении управленческой деятельности, т.е. потребностью в пересмотре ранее изданных локальных нормативных актов ГБУТО «Государственный архив Тюменской области», регламентирующих отдельные этапы работы по защите информации при работе с кадровыми и бухгалтерскими сведениями, использовании аппаратного и программного обеспечения. Поскольку большая часть локальных актов госархива по защите информации была утверждена

в 2014-2016 гг., актуальность темы исследования подтверждается также необходимостью дополнения положений утверждённых документов, внесением в них изменений с учётом современного практического опыта в рассматриваемой сфере и изменившихся с момента утверждения документации положений законодательства, а также издания новых регламентирующих документов.

Предмет исследования – направления деятельности и создаваемый в процессе их осуществления комплекс документации госархива по защите информации, которая регламентирует отдельные этапы и аспекты обеспечения информационной безопасности в процессе осуществления госархивом управленческой деятельности, а также организует этот процесс в целом. Наличие указанного комплекса организационно-правовой, распорядительной и учётной документации по защите информации в учреждении, отвечающего требованиям законодательства и актуальной практике работы, позволит говорить о том, что все процедуры защиты сведений ограниченного доступа описаны документально, а исполнение документально закреплённых процедур снизит вероятность угроз данных и минимизирует возможный ущерб информации от их реализации.

Исходя из темы выпускной квалификационной работы, а также установленных объекта и предмета, всю используемые в процессе исследования литературные ресурсы можно разделить по проблемно-хронологическому принципу на несколько групп в соответствии со следующими тематическими направлениями:

- работы, в которых с рассматривается порядок и особенности обеспечения защиты информации, в т.ч. при использовании информационных технологий;
- материалы по составлению и оформлению документации, а также описывающие процедуру документирования в целом;
- электронные ресурсы, использованные при изучении темы работы.

К первой группе относится учебное пособие Д.А. Скрипника, затрагивающее общие вопросы организации технической защиты информации, где рассматриваются такие направления, как определение целей, задач и

объектов защиты, категории защищаемой информации, информационных ресурсов, что было использовано при написании первой главы выпускной квалификационной работы. В четвёртом разделе пособия дана классификация угроз безопасности информации ограниченного доступа, которая была взята за основу при проведении анализа направлений деятельности Тюменского облгосархива в области защиты информации, результаты которого отражены в пункте 1.2 настоящей диссертации. Для проектирования документов, а именно Модели угроз, были применены положения разделов 7 и 8 – где отражаются такие вопросы, возникающие у составителей Модели угроз, как определение методов и проведение анализа угроз безопасности, а также уязвимостей программного обеспечения [Скрипник, с. 257-292].

Статья А.Е. Кириенко «Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения» разделена на следующие разделы: сначала даётся классификация возможных угроз безопасности информации, затем методов и средств защиты информации, после чего рассматривается вопрос обеспечения защиты информации, содержащейся в компьютерных системах, от несанкционированного доступа. Работа использовалась при рассмотрении отдельных видов угроз безопасности, в частности дана классификация и описание искусственных угроз в первой главе текста диссертации, при проектировании Модели угроз [Кириенко, с. 40-46].

Учебное пособие В. И. Завгороднего «Комплексная защита информации в компьютерных системах» предназначено для специалистов, занятых в области информационных технологий, и представляет интерес именно с точки зрения рассмотрения вопроса с технической точки зрения: здесь даны определение порядка защиты данных от угроз, шпионажа, диверсий, утраты данных от воздействия электромагнитных излучений и наводок и др. [Завгородний, 264 с.]. Именно этот документ стал основой для написания обоснования причин и важности проведения мероприятий по защите информации в организации с учётом применения комплексного подхода.

Решению технических задач при организации системы безопасности в учреждении посвящено и учебное пособие Д.В. Захарова – «Основные понятия информатики. Аппаратное обеспечение информационных технологий. Помимо ряда вопросов технического характера, здесь описан видовой состав средств компьютерной техники, дано описание их структуры, что было использовано при определении направлений технической защиты в качестве примеров возможных источников утечки данных» [Захаров, с. 15].

Работа «Информационная система учета уязвимостей оборудования и программного обеспечения автоматизированных систем управления технологическим процессом» группы авторов А.С. Пинус, И.А. Базаровой, Т.В. Хозяиновой поднимает вопросы учёта возможных уязвимостей оборудования и установленного в организации программного обеспечения [Пинус, Базарова, Хозяинова, 10 с.]. Статья представляет интерес с точки зрения изучения опыта применения в работе CVE (база данных общеизвестных уязвимостей информационной безопасности), используемой при проектировании Модели угроз.

Ко второй группе литературы, посвящённое вопросу документального закрепления процедур составления и оформления документов, относится учебно-методическое пособие Ивановой Н.Ю., Романовой Е.Б. [Составление и оформление…]. Указанное пособие рекомендовано к применению студентам и сотрудникам Санкт-Петербургского национальным исследовательским университетом информационных технологий, математики и оптики по направлению подготовки «Информационная безопасность». Текст пособия разделён на две части: в первой дана теория, а во второй предусмотрены практические задания. Теоретические разделы отражают выполнение таких делопроизводственных процессов как составление организационно-распорядительных, организационно-правовых документов, предусмотрен порядок оформления документов с трафаретным текстом. Отдельным подразделом первой главы выделен пункт, касающийся оформления научной и исследовательской документации.

Статья Е.М. Каменевой содержит рассмотрение отдельных аспектов составления проектов документов [Работа с проектами…]. Так здесь приведены возможные цели разработки проекта, подробно описывается, какие действия должны быть предприняты на каждом из этапов проектирования документа. Отражены и такие моменты, как использование текстовых редакторов, передача проекта для согласования в бумажном виде или через систему электронного документооборота. Вторая часть статьи детально описывает такой этап, как согласование, приводит правила и примеры оформления грифа согласования, перечисляет способы внутреннего согласования документа.

Руководство М. Рогожина по делопроизводству затрагивает все основные этапы работы с документами с учётом документоведческого подхода [Настольная книга ответственного...]. Теоретическая разделена на главы – в первой из них даётся характеристика сущности архивоведения и делопроизводства, далее кратко охарактеризованы нормативные акты в этой сфере. Процедуры, осуществляемые в процессе работы с документами, разделены на разделы: управление документами (рассмотрены вопросы организации документооборота, текущего и временного хранения документов, их передача на хранение в архив) и документирование (определены содержание и структура различных видов документов, освящены вопросы стиля изложения текстов и оформления актов учреждений). Такие особенности ведения делопроизводства учреждения как обеспечение сохранности коммерческой тайны, обеспечение безопасности персональных данные, причины и условия применения электронной подписи в работе специалистов, рассмотрены в шестой главе.

Руководство охватывает не только организационное регулирование отдельных процессов работы с документами, но и предлагает к ознакомлению образцы отдельных документов, которые составляют более половины листажа книги. Здесь представлены Примерное положение о службе документационного обеспечения управления, выдержки из квалификационных справочников, примерная инструкция по делопроизводству.

Учебное пособие В.П. Егорова, А.В. Слинькова раскрывает отдельные моменты, касающиеся создания и обработки документов, содержащих сведения конфиденциального характера [Конфиденциальное делопроизводство…]. Структура пособия выстроена в соответствии с этапами работы с такими документами, предусмотрено и описание ответственности за их нарушение. Помимо организации документооборота, подготовки и издания документов ограниченного доступа, рассмотрены вопросы формирования номенклатуры таких дел, составления заголовков, подготовка их и передача в архив либо для уничтожения. Отличительной особенностью пособия стало наличие отдельных пунктов, касающихся работы с носителями конфиденциальной информации, их учёту и безопасному использованию.

При закреплении результатов исследования в главах 2 и 3 настоящей диссертации, а именно при характеристике групп приказов ГБУТО «Государственный архив Тюменской области» и при проектировании инструкций использовались статьи, ранее опубликованные автором диссертации. Так в статье «Как приказы помогают обеспечить безопасность данных в учреждении» раскрыто назначение и место приказов в системе организационно-распорядительной документации учреждения по защите информации. Упоминаются в тексте статьи и отличительные характеристики Положения и Политики об обработке персональных данных [Дроздова. Как приказы помогают...., с. 83-90]. Статья «Инструкция по антивирусной защите организации: что нужно знать» посвящена установлению причин разработки, правовых оснований и рассмотрению этапов проектирования такой инструкции в организации, документационного закрепления этого процесса [Дроздова. Инструкция по антивирусной защите…, с. 46-48].

В процессе поиска материалов и законодательных актов использовался ряд самостоятельных Интернет-ресурсов. Основным источником изучения законодательной и нормативной базы в области защиты сведений, подлежащих ограничению в доступе, являлся официальный сайт Федеральной службы по техническому и экспортному контролю Российской Федерации. Информация

для пользователей в целях облегчения поиска разделена на несколько разделов, размещённых в верхней части любой страницы под названием учреждения:

- раздел «Контакты» предоставляет данные о месторасположении органа, его полном и сокращённом названии, почтовом адресе, официальном адресе электронной почты и др.;
- раздел «Информация» содержит сведения о структуре учреждения, его руководителях, официальной символике;
- раздел «Деятельность» перечисляет основные государственные функции и услуги, которые выполняет ФСТЭК, указывает государственные программы, в которых принимается участие. Здесь же размещены сведения о проведении официальных мероприятий и участии в международной деятельности;
- в разделе «Документы» представлены тексты актов, проектов документов, административных регламентов, докладов, судебных решений и других документов в области защиты информации;
- сведения в разделе «Техническая защита информации» структурированы по следующим подразделам: «Обеспечение безопасности критической информационной инфраструктуры», «Лицензирование», «Сертификация», «Обучение специалистов», «Укомплектование подразделений», «Банк данных угроз», «Часто задаваемые вопросы». Первые четыре подраздела также включают в себя электронные версии законов, указов, стандартов и иных документов по информационной безопасности, действующих на территории России, пятый и шестой подразделы содержат перечни и информационные сообщения ФСТЭК о программах профессиональной подготовки и повышения квалификации, порядке предоставления сведений о кадровом обеспечении подразделений учреждений специалистами, занятыми вопросами защиты информации. Подраздел «Банк данных угроз» является по своей сути базой данных, представляющей собой перечни кодов угроз и их наименований,

который применялся при написании третьей главы диссертации и выборке данных при проектировании Модели угроз;

– следующие разделы сайта – «Экспортный контроль», «Лицензирование», «Вакантные должности», «Противдействие коррупции», «Территориальные органы», «Государственный научно-исследовательский институт проблем технической защиты информации ФСТЭК России», «Технический комитет по стандартизации «Защита информации» – в работе не применялись.

Вторым источником получения доступа к документам в Интернет-пространстве являлась одна из крупнейших справочных правовых систем, функционирующих на территории Российской Федерации – «Консультант Плюс». Ресурс также состоит из разделов, куда входят «Законодательство», «Судебная практика», «Формы документов», «Проекты нормативных правовых актов» и др. Помимо того, что в системе размещаются только документы органов власти различного уровня и ведомственных учреждений, ресурс позволяет настраивать параметры отображения и осуществлять поиск по документу, что способствует оперативной работе с текстами актов. При формировании поискового запроса в «Консультант Плюс» отображаются все найденные соответствия: и сам искомый документ, и иные документы, тем или иным образом связанные с текстом запроса. Результаты поиска сразу включают в себя указание на статус документа – действующий он или уже утратил силу. К тому же в справочных данных к каждому документу содержится информация, был ли опубликован конкретный рассматриваемый акт и в каких источниках с указанием номера и даты публикации.

При написании магистерской диссертации подвергалась анализу и официальная страница ГБУТО «Государственный архив Тюменской области» на Портале Управления по делам архивов Тюменской области, расположенном в сети Интернет по адресу: http://archiv.72to.ru/index.php/gosudarstvennyj-arkhiv-tyumenskoj-oblasti. Страница состоит из следующих разделов:

- «Главная», где содержится краткая информация об архиве, а также размещаются актуальные объявления о работе учреждения (например, о возобновлении работы читального зала);
- «Великая Отечественная война в документах», где отражаются основные результаты работы архива в этом направлении (перечни документов, электронные выставки), а также размещаются различные справочные материалы, печатные издания на указанную тему;
- Раздел «Новости» оповещает пользователей об изменениях в работе архива, появлении новых направлений работы, участии в различных конференциях и др.;
- в следующем разделе «Об архиве» содержится историческая справка о создании и работе этого архивного учреждения в различные годы;
- раздел «Нормативные документы» представлен двумя документами, регламентирующими работу ГБУТО ГАТО и подлежащими размещению в открытых источниках – это Устав и Политика обработки персональных данных;
- возможность просмотра электронных копий архивных дел возможно реализовать через раздел страницы Портала под названием «Электронный архив»;
- информация о порядке и графике работы читального зала Тюменского облгосархива включены в раздел «Работа в читальном зале»;
- в разделе «Электронная библиотека» содержатся электронные версии различных справочников, литературных изданий, касающихся отдельных событий или периодов истории;
- в разделах «Выставки», «Публикации», «Доклады, сообщения» размещаются работы сотрудников ГБУТО ГАТО, подготовленные в процессе осуществления основной деятельности, участия в конференциях и иных мероприятиях;

- обновления в справочно-поисковом аппарате архива можно посмотреть в одноимённом разделе. Здесь размещаются описи усовершенствованных и переработанных фондов, описанных аудиовизуальных документов, разработанные указатели, перечни и др. справочники к архивным документам;
- в 2018 г. на сайте был создан раздел «К 100-летию государственной архивной службы», где размещена видеопрезентация, описывающая рабочую деятельность госархива в настоящее время, а также размещены статьи и презентации, подготовленные сотрудникам к памятной дате;
- раздел «Инициативное документирование» предоставляет доступ о проводимых в городе мероприятиях (до 2015 г.), в ходе которых сотрудниками госархива производилась фото-, видео- и аудиосъёмка для включения созданных документов в состав архивного фонда области;
- раздел «Нормативно-методические документы по вопросам архивного дела» разделён на три части: документы ВНИИДАДа и Росархива, акты Управления по делам архивов Тюменской области, разработки ГБУТО ГАТО;
- информацию о перечне и стоимости оказываемых госархивом услуг можно посмотреть в разделе с аналогичным названием;
- в следующем разделе официальной Интернет-страницы ГБУТО «Государственный архив Тюменской области» нашёл отражение такой процесс, как рассекречивание документов;
- за ним располагаются сведения о заключённых контрактах учреждения – в разделе «Госзакупки»;
- раздел «Контакты» содержит информацию о местонахождении архива, его должностных лицах и их контактных номерах телефонов;
- обязательными элементами сайта любого учреждения в соответствии с законодательством являются разделы

«Противодействие коррупции» и «Специальная оценка условий труда». Указанные разделы пополняются в госархиве по мере утверждения новых актов – приказов, планов мероприятий и др.

По результатам анализа используемых в исследовании ресурсов, можно сделать следующий *вывод о степени изученности темы*: во-первых, наиболее часто в литературе и статьях рассматривается общий порядок защиты информации, причём освещённый преимущественно с теоретической точки зрения. Во-вторых, современная источниковая база, регламентирующая порядок защиты информации на локальном уровне – в отдельных учреждениях и организациях, затрагивает все основные направления этого процесса. Однако на основе произведённой оценки литературной базы в этой области можно говорить о нехватке информации о практическом подходе к данной теме, а также о типичности структуры и содержания текстов литературных работ. В-третьих, анализ источников позволяет сделать вывод о том, что большинство аспектов защиты информации в российских учреждениях рассматривается в общих чертах, в то время как некоторые другие, например, оформление Модели угроз, нашли более подробное отражение в публицистических материалах.

Таким образом, намечена следующая основная *цель* проведения исследования – осуществление всестороннего анализа процесса и организации документирования в ГБУТО ГАТО процессов по защите информации, позволяющего выявить сильные и слабые стороны названных процессов, определить пути и способы его совершенствования.

Для достижения поставленных целей необходимо выполнение следующих *задач*:

1. анализ законодательных, нормативных и иных актов, государственных стандартов Российской Федерации, нормативных и методических документов профильных органов в области защиты информации;
2. экспертиза текущего состояния комплекса документации по защите информации в ГБУТО «Государственный архив Тюменской области»: анализ полноты и качества существующего комплекса документации

госархива по защите информации, оценка правильности оформления документации ГБУТО ГАТО по защите информации;

3. выявление необходимости внесения изменений в существующие документы или разработки недостающих документов, определение направлений работы по совершенствованию ранее утверждённой документации по защите информации в госархиве;
4. изучение опыта ГБУТО ГАТО в части организации процессов по защите информации, в т.ч. по оформлению соответствующей документации;
5. подбор источниковой базы для разработки локальных нормативных и методических актов в сфере защиты информации;
6. уточнение этапов и сроков разработки недостающих локальных актов, доработки и переутверждения ранее существующих документов госархива в области защиты информации;
7. проектирование документации организационно-правового характера, изменение положений отдельных документов госархива по защите информации и/или разработка новых.
8. оформление и проверка проектов документов для передачи на согласование комиссии по защите информации госархива.

В соответствии с указанными задачами можно выделить следующие две большие группы источников, которые подлежат изучению в процессе написания работы:

- законодательные, нормативно-правовые акты Российской Федерации, акты ведомственных учреждений по защите информации;
- национальные стандарты и методические документы органов, регулирующие сферу защиты информации, определяющие порядок ведения документооборота организации, в том числе составления и оформления документации;
- организационно-правовые документы ГБУТО «Государственный архив Тюменской области», изданные с целью конкретизации обязанностей

должностных лиц и определению перечня функций по различным направлениям защиты информации в госархиве;

– материалы госархива по составлению и оформлению документации, в т.ч. по обеспечению информационной безопасности, а также описывающие процедуру документирования в целом.

По каждой группе источников проведён отбор с целью выявления материалов, наиболее соответствующих изучаемой теме, проанализирована их полнота, определено соответствие практике работы в госархиве, осуществлён сравнительный анализ внутри групп и определены возможности применения тезисов изученных источников на практике при составлении документации в области защиты информации для Государственного архива Тюменской области. Не были выделены в отдельную группу или включены в состав одной из указанных групп акты методического характера органа, в подчинении которого состоит ГБУТ ГАТО, – Управления по делам архивов Тюменской области, т.к. названый орган имеет в сфере защиты информации только документы, регламентирующие внутренние направления работы (Модель нарушителя [Модель нарушителя безопасности…], Технический паспорт на ИСПДн «Директум» [Технический паспорт…] и др.).

В таких общеобязательных актах государственного значения, как Конституция Российской Федерации, Трудовой и Уголовный кодексы содержатся только отдельные положения, обозначающие возникающие права и границы сферы распространения ответственности граждан в области защиты информации, однако именно они являются главной правовой основой осуществления этого процесса как на государственном, так и на корпоративном уровне.

Федеральный закон о гостайне устанавливает перечень сведений, которые могут к ней относиться, перечисляет принципы такого отнесения, даёт характеристику степеням секретности, определяет порядок их передачи, рассекречивания [О государственной тайне…]. Для проводимого в рамках темы выпускной квалификационной работы исследования закон интересен в части

изучения положений статьи 12 третьего раздела, где указаны реквизиты документов, составляющих государственную тайну, и раздела 6, где описывается порядок защиты сведений ограниченного доступа.

Что касается ФЗ № 98, то исходя из определения коммерческой тайны (а именно – присвоение информации такого режима конфиденциальности, который позволил бы увеличить доходы, избежать неоправданные расходы или получить иную выгоду, выражаемую в денежном эквиваленте, её обладателю) он может быть применён в рамках текущей работы только в части обоснования необходимости разработки локальных актов по защите информации – целью такой разработки является предупреждение и минимизация возможного понесённого ущерба, что как раз соответствует данному законом определению [О коммерческой тайне…].

ФЗ об архивном деле, являющийся основным для Тюменского облгосархива, освещает вопрос защиты информации только в части ограничения доступа к документам архивного фонда России и их использованию, что указано в главе 6 закона [Об архивном деле…]. Изучение закона было также полезно при определении основных направлений деятельности госархива, проводимое в целях определение места защиты информации в нём.

К числу наиболее часто использовавшихся в процессе магистерского исследования актов первой группы источников относится и Федеральный закон от 27 июля 2003 г., являющийся основополагающим актом в вопросах работы с персональной информацией [Об информации, информационных технологиях…]. Согласно третьей статье 149-ФЗ обработкой персональных данных принято считать осуществление любого действия (или совокупности таких действий) с персональными данными. К их числу относятся такие направления работы, как сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. На основе закона № 149 в работе и проектах применялись термины «информация», «идентификация» и

«аутентификация», «конфиденциальность», «доступ» и «распространение» информации.

Контроль в сфере защиты отдельных категорий информации на уровне государства реализуется путём определения конкретных требований о защите информации, а также установления ответственности за нарушение законодательства Российской Федерации о работе с информацией и её защите. Перечень мер, направленных на защиту сведений, согласно закону «Об информации…», предполагает проведение учреждениями работ в трёх направлениях: защита данных от неправомерного доступа, соблюдение такого свойства информации ограниченного доступа, как конфиденциальность, а также реализацию права гражданина на доступ к информации. При этом в соответствии с законом № 149 обладатели информации (в текущем случае – Тюменский облгосархив) должны обеспечить условия, при которых несанкционированный доступ к информации будет невозможен или его возможность минимизирована, факты возникновения такого доступа будут обнаружены своевременно. Также закон предполагает проведение организационных и технических мер по защите информации в учреждениях, непрерывный контроль за обеспечением соответствующего уровня защищённости.

Еще один документ, ставший основой не только для теоретической части работы, но и для разработки проектов документов для госархива, это Федеральный закон № 152 [О персональных данных…]. Он регламентирует те вопросы обработки персональных данных, которые связаны с использованием средств автоматизации, а также обрабатываемые без их использования, принципы и условия такой обработки. Здесь же рассмотрены основные права субъекта и обязанности оператора персональных данных, приведён перечень мер, соблюдение которых способствует обеспечению безопасности данных персонального характера в ходе их обработки.

Здесь стоит отметить, что положения российского законодательства затрагивают в основном вопросы защиты государственных информационных ресурсов и информацию конфиденциального характера, представленную в

основном персональными данными граждан. Однако положения законодательных и нормативных актов указанных направлений, в том числе и закон «О персональных данных» могут составлять методическую основу для разработки локальной документации организации, позволяющей учитывать специфику работы с более широким спектром данных, чем тот, что указан в законодательстве.

Указ Президента РФ № 188 был использован в работе в целях определения категорий данных сотрудников и пользователей архива, обработка которых осуществляется в ГБУТО «Государственный архив Тюменской области», подлежащих защите [Об утверждении Перечня…]. Исключая сведения «профильного» характера (судебная деятельность, различные виды тайн – адвокатская, врачебная и др., сведения о сущности изобретения), было выявлено, что на основании данного акта для госархива будет являться актуальной защита таких сведений, как информация персонального характера, позволяющая идентифицировать личность гражданина.

Постановление Правительства Российской Федерации № 1119 приводит перечень основных требований к защите персональных данных, возникающих в случае их обработки в информационных системах, однако именно здесь дана классификация видов мер, которые должна включать система защиты сведений ограниченного доступа учреждения [Об утверждении требований…]. В четвёртом пункте документа указано, что выбор применяемых средств защиты информации остаётся за организациями, т.е. зависит только от возможностей и нужд учреждения. Также в постановлении дано определение актуальных угроз безопасности, перечислены их виды, а также классификация уровней защищённости информационных систем, что было использовано при проектировании Модели угроз.

Говоря об обеспечении информационной безопасности, обеспечиваемой в процессе автоматизированной обработки сведений ограниченного доступа, стоит упомянуть Постановление Правительства РФ № 890 [О мерах по совершенствованию…]. Правительственный акт устанавливает требования к

обеспечению безопасности информации в процессе осуществления её обработки и передачи посредством информационно-телекоммуникационных сетей, в т.ч. тех, доступ к которым не ограничен.

Приказ Минкомсвязи № 221 регламентирует порядок осуществления работы предприятия с использованием электронного документооборота, в т.ч. при обработке служебной информации ограниченной сферы распространения в федеральных исполнительных органах. В третьем разделе приложения к названному приказу указано, что в целях обеспечения необходимой защиты информации ограниченного доступа следует применять технические или программные средства защиты информации [Об утверждении требований…]. В пункте 22 дано положение, устанавливающее обязательность определения класса защищённости информационной системы, в 26 – наличия политики безопасности учреждения. Далее дано ещё одно требование – о наличии в применяемой СЭД возможности резервного копирования данных с установленной периодичностью.

Для должности администратора информационной безопасности вычислительной сети, в ведение которой входят функции по обеспечению защиты информации в госархиве, существуют специальные профстандарты – 06.027 и 06.032 [Общероссийский классификатор должностей…]. Первый предназначен для специалистов, администрирующих сетевые устройства информационной системы, второй – для специалиста по безопасности компьютерных сетей и систем. Именно на их основе в должностную инструкцию администратора госархива были включены такие функции, как установка обслуживание аппаратных и программных средств защиты информации, осуществление анализа безопасности компьютерных систем и др.

В основу для разработки Модели угроз легли положения таких документов, как приказ Федеральной службы по техническому и экспортному контролю Российской Федерации № 21 [Об утверждении состава…], который даёт характеристику реализуемым в организации мерам, направленным на обеспечение безопасности персональных данных – по 4 уровням защищённости,

а также Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, описывающая порядок проведения таких работ, а также Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, также являющаяся методикой, но по своей сути представляющая из себя шаблон документа, на основе которого разрабатываются Модели угроз в российских учреждениях. Определение уязвимостей информационной системы для Модели угроз, а также их классификация осуществлялись на основе положений ГОСТ Р 56546-2015 [Защита информации…].

Правила делопроизводства, утверждённые Росархивом в 2019 г. [Правила делопроизводства…], не содержат конкретных положений о документальном закреплении защиты каких-либо категорий данных, однако даёт отсылки на федеральное законодательство, в соответствии с которым организуется обеспечение доступа к информации, отражающее вопросы деятельности госорганов и органов местного самоуправления [Федеральный закон № 8], а также о деятельности судов [Федеральный закон № 262].

Правила работы архивов 2020 г. уже включают в себя требования к обеспечению информационной безопасности в архиве [Правила организации хранения…]. Так в пункте 1.4 первого раздела указано, что в случае наличия в архивном учреждении соответствующей требованиям безопасности информационной системы, в ней может быть осуществлён учёт исполнения основных функции архива – т.е. учёт, использование и др. Новшеством в этой редакции Правил стало упоминание отдельных этапов работы с электронными документами. В седьмом разделе указаны, что хранение таких документов осуществляется только в случае соблюдения требований безопасности и защит информации.

При разработке проектов инструкций в качестве основы брались положения методического документа «Меры защиты информации в государственных информационных системах»: Федеральной службы по

техническому и экспортному контролю Российской Федерации: для инструкции по организации парольной защиты ГБУТО ГАТО изучался пункт 3.1 указанного документа, для инструкции по организации антивирусной защиты – пункт 3.6, а для инструкции по работе со съёмными носителями информации – пункт 3.4. Остальные части документа использовались при написании теоретической части диссертации.

Основные принципы разработки инструкций при написании пункта 3.2 настоящей выпускной квалификационной работы и проектировании приложений брались на основе Методических рекомендаций Росархива по разработке инструкции по делопроизводствуъ 2020 г. [Методические рекомендации…]. Однако, основным делопроизводственным актом, на котором базировалось проектирование, стала аналогичная инструкция госархива [Инструкция по делопроизводству…].

Все термины, встречавшииеся в процессе исследования, были истолкованы в соответствии с ГОСТ Р 50922-2006 и ГОСТ Р 53114-2008, а для толкования определений в области защиты информации от несанкционированного доступа применялся руководящий документ Гостехкомисии при Президенте Российской Федерации, изданный 30 марта 1992 г. [Защита от несанкционированного доступа…].

Для расчёта эффективности разрабатываемых в процессе написания настоящей магистерской диссертации использовалась формула, установленная нормативами 1994 г. на выполнение работ по документационному обеспечению [Нормы времени…]. Определение направлений работы, по которым мог осуществляться расчёт эффективности, был произведён на основе Норм времени федеральных органов исполнительной власти 2002 г., т.к. именно там содержится рассмотрение необходимых документоведческих процедур [Нормы времени…].

Анализ иных правовых и нормативных документов, являющихся основой для организации системы защиты информации в ГБУТО «Государственный архив Тюменской области», но в меньшей мере применяемых при написании

диссертации, приведён в пункте 1.1 настоящей работы. В ходе оценки источников был сделан вывод о том, что необходимость разработки некоторых документов по защите информации в организациях регламентирована отдельными положениями нормативных документов Российской Федерации, однако составление, например, инструктивных материалов по организации и проведению отдельных мероприятий в этой сфере передано на усмотрение самих организаций. Как для учреждений, чья деятельность связана с работой со сведениями ограниченного доступа или информацией, содержащей какую-либо из видов тайн, так и для тех, кого эти вопросы не затрагивают, необходимо самостоятельно определить требуемый перечень локальных актов по защите информации, который должен быть создан в организации в целях снижения рисков утечки и доступа к информации.

В рамках оценки источников были изучены состав и содержание утверждённых документов госархива по основной деятельности. Результаты проведённых исследований включены в текст второй главы выпускной квалификационной работы, они также нашли отражение в списке используемых при написании работы источников и литературы. Основополагающими локальными документами Государственного архива Тюменской области, используемыми в работе при определении её структуры, направлений исследования, стали приказы о назначении ответственных лиц – ответственных за обработку персональных данных сотрудников в бумажном и автоматизированном виде, инструкции должностным лицам, ответственным за различные направления работы по защите информации (например, Инструкция администратору безопасности в информационных системах персональных данных, Инструкция ответственного за организацию обработки персональных данных в ГБУТО ГАТО).

Положение об обработке и защите персональных данных утверждено приказом ГБУТО ГАТО № 26. Документ определяет порядок сбора, хранения, передачи и любого другого использования персональных данных работников в соответствии с законодательством Российской Федерации и гарантией

конфиденциальности сведений о субъекте персональных данных в ГБУТО ГАТО. Положение содержит обоснование причин обработки персональных данных сотрудников, принципы их получения, обработки, передачи и других выполняемых действий.

Отдельно стоит упомянуть документы, регламентирующие отдельные этапы деятельности госархива по защите информации, например, Перечень конфиденциальной информации ГБУТО «Государственный архив Тюменской области», в соответствии с которым были установлены актуальные направления проводимых работ по защите информации, Схема контролируемой зоны ГБУТО ГАТО, конкретизирующая расположение объектов, на которых осуществляется обработка сведений ограниченного доступа.

Последнюю группу источников представляют документы, в которых определяются последовательность и особенности документирования административных процедур учреждения на локальном уровне. Основным документом, используемым при оформлении проектов инструкций по организации антивирусной и парольной защиты, по работе со съёмными носителями информации в ГБУТО «Государственный архив Тюменской области» в рамках настоящей диссертации стала Инструкция по делопроизводству ГБУТО ГАТО [Инструкция по делопроизводству].

Действующая Инструкция по делопроизводству ГБУТО «Государственный архив Тюменской области» состоит из девяти разделов, разделённых на подпункты, а также семнадцати приложений к ним. Раздел «Общие положения» раскрывает цели и правовую основу разработки документа, сферу его деятельности. Обговариваются особенности работы с отдельными видами документации, например, в 6 пункте указано, что положения Инструкции не могут применяться при организации работы с документами, содержащими сведения, являющиеся гостайной [Инструкция по делопроизводству…]. Особенности работы с документами, содержащими информацию конфиденциального характера (любой из видов тайн, персональные данные), регулируются специальными нормативными актами (инструкциями,

положениями, правилами), утверждаемыми директором госархива, что указано в пунктах 7 и 8 соответственно. Однако двенадцатым пунктом предусматривается ответственность сотрудников за разглашение или передачу документов или копий документов ограниченного доступа, проектов сторонним организациям.

Второй раздел Инструкции состоит из перечня основных понятий, упоминаемых в тексте этого нормативного документа. В следующем разделе рассматриваются основные этапы подготовки и оформления документов, в том числе употребление определённых шрифтов, размеров текста, интервалов и отступов, границы полей документов, нумерации, использование бланков и оформление каждого из возможных реквизитов документов. Здесь же указано, что гриф согласования комиссионного органа оформляется под реквизитом «Подпись» от границы левого поля документа [Инструкция по делопроизводству…]. В четвёртом разделе Инструкции раскрываются особенности подготовки и оформления отдельных видов документов, в том числе и инструкций, что было использовано при разработке проектов документов в рамках написания данной работы.

Организация процесса работы с документами в отделах госархива осуществляется на основании указаний директора госархива, его заместителя, начальника этого структурного подразделения. Именно работе исполнителей с документами в госархиве посвящён восьмой раздел. Для удостоверения подлинности подписи на документах или соответствия копий документов подлинникам используется печать архива и гербовая печать. Вопросам их применения отведены положения девятого раздела.

Ещё одним локальным документом, определяющим порядок и правила оформления различных разработок, является Памятка по подготовке методических пособий сотрудниками ГУТО ГАТО [Памятка по подготовке…]. В документе рассмотрены основные виды методических пособий, разрабатываемых в госархиве – методические рекомендации, инструкции и памятки, указаны требования к их оформлению. В пункте 2.3 указано, что

инструкции могут разрабатываться для регламентации отдельных видов работ или же регламентировать какой-либо организационный процесс в целом. Этапы разработки проектов, в т.ч. их согласование, подробно рассмотрены в третьем разделе. Перечислению требований к оформлению документов отведён последний – четвёртый – раздел. Здесь указано, что методический документ обязательно должен иметь титульный лист, а в его структуру должны входить введение (или общие положения), основные разделы и приложения [Памятка по подготовке…]. Пункт 4.11 определяет, что текст инструкций располагается в логической последовательности по разделам, подразделам и пунктам. В приложениях к Памятке даны формы и образцы оформления отдельных элементов указанных документов, в т.ч. титульного листа, первой и последней страницы проекта документа.

Подробный анализ всех утверждённых локальных актов ГБУТО ГАТО с выводами о степени соответствия современной практике работы содержится в пунктах 1.2 и 2.1 выпускной квалификационной работы.

Методы научного исследования, используемые при написании данной выпускной квалификационной работы и проектировании документов для Тюменского облгосархива, условно можно разделить на 3 группы – эмпирические, общенаучные и частные (специальные) методы исследования. На этапе предпроектного обследования при рассмотрении теоретической базы, регламентирующей основные вопросы защиты информации в Российской Федерации и на локальном уровне непосредственно в ГБУТО ГАТО, применялись методы *системного анализа*, *классификации* источников информации – были выделены основные источники как среди отечественного законодательства и нормативных документов, так и в локальной документации Тюменского облгосархива, положения которых наиболее отвечали целям и задачам проведения исследования, осуществлён *отбор* и проведена классификация собранной информации для включения в текст работы. Метод *комплексного изучения* способствовал формированию целостного представления о системе защиты информации в госархиве, выделению в ней отдельных

элементов по основным направлениям работ. Определению взаимосвязей элементов комплекса мер, направленных на обеспечение информационной безопасности госархива, способствовал метод *дедукции*.

Целый комплекс методов (а именно метод *структуризации, аналогии и сравнения)* использовался при анализе результатов проведённого предпроектного обследования. Они выражаются в выделении информации в соответствии с определённой тематикой, определении наиболее значимых источников и сведений для проводимого исследования, их *группировке* в соответствии со структурой диссертации. Для представления анализа изученных источников в текстовом виде применены метод *описания*, *формализации* сведений. *Психолингвистический* метод применялся в целях выявления степени восприятия документированной информации – как для ранее утверждённых локальных актов ГБУТО ГАТО по защите информации, так и для разрабатываемых проектов документов. Метод *формулярного анализа* позволил дать оценку структуре указанных документов, определить правильность расположения отдельных элементов.

Установленные цели, определённые задачи и выявленные методы исследования определяют *структуру* выпускной квалификационной работы. В состав настоящей диссертации входят список сокращений и условных обозначений, необходимых для обеспечения верного восприятия информации, содержащейся в тексте диссертации и приложений к ней. Далее идёт введение и три тематические главы. В первой главе рассмотрено правовое, организационное и техническое обеспечение информационной безопасности в ГБУТО «Государственный архив Тюменской области»: в первом разделе даётся анализ правовой основы защиты информации в Российской Федерации, во втором и третьем описаны основные направления деятельности госархива по обеспечению информационной безопасности. Во второй главе диссертации проведён анализ текущего состояния комплекса действующей в госархиве документации по защите информации, в том числе подробно рассмотрены комплексы инструктивных документов и приказы, определены изменения и

дополнения, требующие внесения в Политику обработки персональных данных в ГБУТО «Государственный архив Тюменской области».

Третья глава полностью посвящена теме проектирования организационно-правовых документов по защите информации, разработка которых позволит говорить о совершенствовании текущего порядка защиты информации в госархиве. Первый раздел главы посвящён описанию порядка составления и оформления проекта Частной модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» в ГБУТО «Государственный архив Тюменской области». Во втором разделе описана методика проектирования инструкций по организации парольной и антивирусной защиты, а также по работе со съёмными носителями информации в ГБУТО «Государственный архив Тюменской области», в третьем приведены возможные направления дальнейшей работы в области документационного обеспечения процессов по защите информации в госархиве.

Завершает основную часть текста выпускной квалификационной работы заключение, где делаются выводы о результатах проведённого исследования, отмечаются наиболее важные моменты и заключения. Вся используемая в процессе написания работы и изучения темы исследования литература, статьи, Интернет-ресурсы включены в библиографический список. Завершают структуру диссертации пять приложений, расположенных в соответствии с порядком из разработки и описания в главах диссертации.

ГЛАВА 1. ПРАВОВОЕ, ОРГАНИЗАЦИОННОЕ И ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГБУТО «ГОСУДАРСТВЕННЫЙ АРХИВ ТЮМЕНСКОЙ ОБЛАСТИ»

Говоря о защите информации, необходимо понимать, что для обеспечения безопасности данных на любом уровне (будь то сведения государственной важности, корпоративная тайна или персональные сведения конкретного гражданина) необходима реализация целого комплекса мер, причём обязательность их выполнения должна исходить от органов законодательной власти страны, т.е. являться частью правовых отношений. При этом нельзя говорить о гарантии безопасности при соблюдении только одного из направлений защиты информации, например, при проведении законотворческой деятельности. Без дополнительных действий сами по себе законы «работать» не будут, они только установят рамки допустимых действий в отношении информации ограниченного доступа, но для обеспечения информационной безопасности необходимо одновременное применение и иных мер. С учётом существующей практики обеспечения информационной безопасности в российском информационном пространстве установлены следующие направления защиты информации:

- правовая защита состоит в регламентации вопросов защиты данных в законах, нормативно-правовых актах, правилах и других документах, которые обеспечивают защиту информации в Российской Федерации на общегосударственном уровне;
- организационная защита подразумевает регламентацию производственной деятельности и/или взаимных отношений исполнителей на нормативно-правовой основе, которая ослабляет или полностью исключает нанесение возможного ущерба исполнителям;
- инженерно-техническая защита включает использование различных технических средств, которые препятствуют нанесению ущерба деятельности [Скрипник, с. 12].

1.1. РЕГУЛИРОВАНИЕ ПРОЦЕССОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ЗАКОНОДАТЕЛЬНЫХ, НОРМАТИВНО-ПРАВОВЫХ И НОРМАТИВНО-МЕТОДИЧЕСКИХ АКТАХ РОССИЙСКОЙ ФЕДЕРАЦИИ

Любое направление деятельности, являющееся обязательным для большого числа учреждений, а также государственных органов, имеет в своей основе какой-то документный акт или целый комплекс документов, закрепляющих порядок выполнений действий в этой сфере. Такое направление, как обеспечение безопасности, всегда имело большое значение не только для государств, рядовых предприятий, но и для обычных людей. Охрана частной жизни, защита сведений о деятельности предприятий, автоматизированных систем являются в условиях тотальной информатизации одним из приоритетных направлений развития любого государства, поэтому неудивительно, что основы такой деятельности находят своё отражение в международных и общегосударственных документах, а их исполнение носит не только обязательный, но и рекомендательный характер. В России вопросы защиты информации затронуты как в отдельных пунктах разнопрофильных законодательных актов, так и выделены в самостоятельные правовые документы.

Общий перечень отечественных нормативных правовых документов в области информационной защиты включает в себя различные кодексы, федеральные законы, указы и распоряжения Президента России, Постановления Правительства РФ, государственные стандарты, нормативно-методические и руководящие документы уполномоченных федеральных органов (Федеральная служба безопасности, ФСТЭК, Роскомнадзор). Однако в рамках данной работы такие общие документы, как, например, Указ Президента Российской Федерации № 537 [О стратегии…] или Постановление Правительства Российской Федерации № 1236 [Об установлении запрета…] рассматриваться не будут. Полный перечень всех актуальных нормативных правовых актов, организационно-распорядительных документов, нормативных и методических разработок ведомств, а также проекты документов в области защиты

информации представлены на официальном сайте Федеральной службы по техническому и экспортному контролю Российской Федерации. В данном разделе анализ будет осуществляться только исходя из наличия практической пользы содержащейся в актах информации для написания данной работы и разработки проектов документов для ГБУТО ГАТО.

К непрофильным документам, но закладывающим основу для разработки других правовых актов в области защиты данных, относится документ, имеющий высшую юридическую силу на территории нашего государства, – Конституция Российской Федерации. В статье 23 указано гарантированное право каждого гражданина на неприкосновенность частной жизни и личную тайну, а 24 – подкрепляет эти положения, вводя обязательность наличия согласия гражданина на обработку такой информации [Конституция РФ…]. Трудовой кодекс в главе 14 рассматривает вопросы защиты персональных данных работников учреждений при их обработке, использовании и хранении как одного из обязательных условий функционирования современных учреждений, в штате которых числится хотя бы один сотрудник [Трудовой кодекс…].

Уголовный кодекс Российской Федерации в главе 28 «Преступления в сфере компьютерной информации» предусматривает ответственность за неправомерный доступ к информации, в т.ч. содержащейся в различных информационных системах, за создание, использование и распространение вредоносных программ, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей [Уголовный кодекс…]. Такая регламентация определяет и основные направления защиты информации, т.е. применение специальных мер на каждом этапе работы со сведениями ограниченного доступа.

Главным российским правовым актом, регламентирующим защиту сведений на государственном уровне, является ФЗ № 5485-1 [О государственной тайне…]. Документ интересен тем, что это первый подобный акт, где даётся определение средств защиты информации, а также описывается какого рода информация ограниченного доступа может содержаться на носителях

информации. Также во второй статье приводится классификация средств защиты информации: в документе сказано, что ими могут быть технические, криптографические или же программные средства, которые разработаны в целях защиты информации, составляющей государственную тайну, а также средства, в которых она содержится и средства контроля эффективности применяемых способов защиты информации.

Закон России «Об электронной подписи» содержит ряд конкретизирующих определений, используемых специалистами, занятыми в сфере защиты информации, а также подробную классификацию и порядок работы с главным криптографическим средством подтверждения личности в информационном пространстве [Об электронной подписи…]. Здесь можно найти толкование таких понятий, как электронная подпись, сертификаты ключей, аккредитация, информационные системы различных типов и др., используемых в работе специалистов, занятых не только защитой информации в учреждении, но и обработкой персональных данных в автоматизированном виде.

Основополагающим среди российских законов, посвящённых именно вопросам обеспечения информационной безопасности, является 149 закон [Об информации…]. Во второй статье содержатся следующие определения: информация, информационная система, доступ и распространение информации, конфиденциальность информации, идентификация и аутентификация. В статье 8 обосновывается порядок реализации права гражданина на доступ к информации, а в 9 указано, при каких условиях информация подлежит ограничению в доступе. Статья 16 рассматриваемого закона целиком посвящена только рассмотрению вопросов защиты информации. Согласно ей, защита информации представляет собой ничто иное, как принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от реализации неправомерных действий в отношении такой информации, на соблюдение конфиденциальности информации, имеющей ограничения по доступу, на реализацию права на доступ к информации.

Федеральный закон № 152 даёт гарантию на защиту прав и свобод любого гражданина России в случае осуществления обработки его персональных данных [О персональных данных…]. Положения закона распространяются на все виды отношений, связанных с обработкой персональных данных вне зависимости от использования средств автоматизации. Во второй статье представлены четыре исключения, куда включена организация хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации. Также в законе обосновываются принципы и обговариваются условия обработки данных персонального характера, обозначены права субъекта таких данных и обязанности оператора при обработке персональных сведений. В статье 9 указано на обязательность применения в работе согласия субъекта персональных данных на обработку его данных персонального характера.

Требования к обязательности обеспечения защиты персональных данных в случае их обработки в информационных системах продиктованы положениями Постановления российского Правительства № 1119 [Об утверждении требований…]. Здесь закладываются основные направления организации такой защиты, функции оператора в сфере соблюдения безопасности при обработке персональных данных. В пятой статье дан перечень отличительных признаков информационных систем, в которых обрабатываются специальные категории, биометрические и общедоступные персональные данные. В следующем пункте дано определение актуальных угроз, перечислены их типы. Рассмотрению уровней защищённости персональных данных при их обработке в информационных системах и требований к их обеспечению посвящены статьи с 8 по 16.

Вопросам защиты информации отведён целый комплекс государственных стандартов: в них можно найти требования к защите систем от несанкционированного доступа (например, ГОСТ Р 50739-95, ГОСТ Р 51188-98, ГОСТ Р 53115-2008), требования к созданию и использованию

автоматизированных систем (например, ГОСТ Р 51583-2014, ГОСТ Р 52863-2007), направления работы с биометрическими персональными данными (например, ГОСТ Р 52633.1-2009, ГОСТ Р 52633.2-2010), порядок аудита информационной безопасности (например, ГОСТ Р ИСО/МЭК 13335-1-2006, ГОСТ Р ИСО/МЭК 27003-2012), аспекты технической защиты данных (например, ГОСТ Р 52448-2005, ГОСТ Р 52633.6-2012) и др.

Однако большинство действующих стандартов в области защиты информации охватывают какую-то конкретную сферу деятельности, что объясняет использование при проектировании документов госстандартов общей направленности, т.е. содержащих основные положения в сфере информационной защиты: толкование основных терминов и определений в сфере защиты данных даётся на основе ГОСТ Р 50922-2006 и ГОСТ Р 53114-2008, основополагающим документом при составлении нескольких разделов Частной модели угроз является стандарт «Классификация уязвимостей информационных систем» [ГОСТ Р 56546-2015…].

Акты Федеральной службы по техническому и экспортному контролю Российской Федерации также использовались при написании магистерской диссертации, а именно приказы ФСТЭК № 17 [Об утверждении требований о защите информации…] и № 21 [Об утверждении состава и содержания организационных и технических мер…], которые описывают перечень мер, применение которых необходимо в информационных системах для обеспечения безопасности персональных данных. Здесь рассмотрены вопросы идентификации и аутентификации субъектов, настройки доступа к системам, защиты машинных носителей с содержащимися на них сведениями конфиденциального характера, технической защиты систем, использования антивирусных средств и систем обнаружения вторжений, определение класса защищённости информационной системы.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных разработана на основе действующего отечественного законодательства в целях

облегчения работы учреждений при организации безопасной работы со сведениями персонального характера в информационных системах. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, как и Методика утверждена заместителем директора Федеральной службы по техническому и экспортному контролю Российской Федерации, но представляет собой типовой образец, т.е. может являться основой для разработки собственного документа в организаций путём внесения изменений и дополнений в неё, что и было реализовано при определении структуры Частной модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» ГБУТО «Государственный архив Тюменской области».

Таким образом, проведя анализ источников, затрагивающих в том или ином объёме вопросы обеспечения информационной безопасности на различных уровнях, можно говорить о наличии в российском правовом пространстве множества актов, как государственного, так и ведомственного значения. Однако, несмотря на их большое количество, они затрагивают далеко не все необходимые направления защиты информации, вследствие чего возникают ситуации, в которых имеется необходимость разработки какого-то акта в сфере защиты информации, но соответствующие правовые основания такой разработки либо отсутствуют, либо затрагиваются в отдельных пунктах в нескольких актах, зачастую даже различного уровня.

1.2. НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ТЮМЕНСКОГО ОБЛГОСАРХИВА В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Защита информации предполагает системный подход, включающий в себя параллельную работу с комплексом взаимосвязанных элементов. Важнейшим из них является объект (или объекты) защиты информации, так как от их количества, состава и текущего состояния зависят не только применяемые в учреждении методы и средства защиты, но и состав проводимых мероприятий.

В соответствии со стандартом, дающим толкование основных определений и терминов, применяемых специалистами, занятыми решением вопросов обеспечения информационной безопасности, под объектом защиты информации понимается информация, её носитель или информационный процесс, которую (который) необходимо защищать в соответствии с поставленной целью защиты информации [ГОСТ Р 50922-2006].

К основным видам объектов защиты, утвержденным приказом Гостехкомиссии России № 282, относят:

- информацию, представленную на бумажном носителе, или в виде цифровых сигналов (электронная форма);
- ресурсы (программное и аппаратное обеспечение);
- физические объекты, для которых необходимо обеспечить защиту процесса обработки данных (конкретные территории, здания, помещения, техническое оборудование и каналы связи) [Специальные требования…].

Для ГБУТО ГАТО первый вид защищаемых объектов представлен в бумажном виде личными делами сотрудников ГБУТО ГАТО, в электронном виде – аналогичными данными, содержащимися в бухгалтерских и кадровых программах, а также служебными документами, передаваемыми по средствам электронного документооборота и иным каналам связи в информационных системах персональных данных «Бухгалтерия» и «Директум». Обеспечивается также защита рабочих мест, на которых осуществляется обработка персональных данных, – они находятся в отдельных помещениях, куда ограничен доступ других сотрудников, на самих компьютерах настроена парольная система входа не только в учётную запись, но и в каждую из программ.

Существует множество различных классификаций угроз безопасности данным, т.е. потенциально возможных направлений воздействий на информацию ограниченного доступа, которые могут прямо или косвенно нанести урон владельцам и пользователям. В классическом понимании угрозы информационной безопасности могут быть отнесены к одному из двух видов:

- естественные угрозы, которые реализуются в результате физических воздействий на информацию – в случае возникновения стихийных природных явлений (угрозы, не зависящие от деятельности человека);
- искусственные угрозы, которые вызваны результатами человеческой деятельности, которые могут являться следствием как умышленной деятельности против конкретного субъекта, так и случайной [Скрипник, с. 23].

Искусственные угрозы в зависимости от причин их возникновения могут подразделяться на непреднамеренные (случайные) и преднамеренные (умышленные). К первому виду угроз относятся: ошибки в проектировании компьютерных систем, ошибки в разработке программных продуктов, случайные сбои в работе аппаратных средств, линий связи, энергоснабжения, воздействие на аппаратные средства компьютерных систем физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др. [Киреенко, с. 40-46]. Решение таких проблем безопасности в госархиве происходит по мере их возникновения в рабочем порядке совместно со специалистами сторонних организаций, поскольку их возникновение является следствием сбоя в работе систем, разрабатываемых и обслуживаемых сотрудниками специализированных учреждений, а не ошибки, допущенной в работе сотрудником госархива, у которого к администрированию таких систем доступа нет.

Наибольшего внимания заслуживают именно искусственные и преднамеренные угрозы, т.к. вероятность этих угроз намного выше, а возможный ущерб организации или человеку – значительнее. Искусственные преднамеренные угрозы имеют своей целью нарушение таких свойств информации как:

- конфиденциальность информации (субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к информации);

- целостность (состояние информации, при котором она представлена в неискаженном виде по сравнению с каким-то начальным значением);
- доступность (беспрепятственный оперативный доступ субъектов к интересующей их информации).

Нарушение перечисленных свойств достигается действиями неблагонадежных сотрудников путём саботажа, организации внутренних утечек данных, а также при помощи таких технологических разработок, как, например, компьютерные вирусы, фишинг-атаки, шпионское программное обеспечение; программы-вымогатели, спам. При отсутствии регламентированного доступа и прав сотрудников организации в отношении информации ограниченного доступа возможны:

- свободный доступ большого количества рабочих мест учреждения к электронным документам, содержащим сведения ограниченного доступа, в т.ч. несанкционированный просмотр информации сотрудниками или третьими лицами, не имеющими необходимых прав доступа;
- бесконтрольное копирование и рассылка электронных документов.
- преднамеренное или случайное уничтожение документов;
- искажение информации или ошибки в работе вследствие использования неактуальной версии [Завгородний, с. 16-19].

Избежать реализацию указанных угроз возможно при проведении соответствующих организационных мероприятий, а также защитой аппаратного и использовании специализированного программного обеспечения. Все действия и мероприятия, ориентированные на обеспечение защиты информации Тюменского госархива, характеризуются рядом параметров.

Первый из них направлен на защиту персонала, обрабатывающего информацию, материальных ценностей, которые способствуют обработке информации и на саму информацию, то есть на объекты защиты. Второй классифицируется по характеру угроз и представлен тремя основными видами:

разглашение информации, её утечка и несанкционированный доступ к данным. Их реализация в ГБУТО ГАТО избегается путём:

- установления персональной ответственности должностных лиц за работу с персональными данными сотрудников архива. Например, в приказе, которым утверждается перечень сотрудников ГБУТО ГАТО, допущенных к обработке персональных данных сотрудников архива, перечислены конкретные должностные лица, на которые возлагаются функции по обработке персональных данных в автоматизированном виде в информационных системах персональных данных «Директум» и «Бухгалтерия», и работе с аналогичной информацией, только без использования средств автоматизации [Об утверждении списков…]. Допуск других сотрудников к этой категории данных в госархиве не допускается;
- установки специализированных средств защиты информации и индивидуальных идентификаторов и аутентификаторов на программы и персональные компьютеры, где осуществляется обработка конфиденциальной информации.

Третья классификация осуществляется по масштабу защитных действий и может быть направлена на защиту конкретных объектов или индивидуального объекта, группы объектов. Масштаб защитных действий в ГБУТО ГАТО ограничивается в учреждении конкретными объектами – рабочими местами специалистов, чья деятельность связана с обработкой сведений ограниченного доступа.

1.3. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕРЫ ГОСАРХИВА ПО ЗАЩИТЕ ИНФОРМАЦИИ

Основой проведения организационных мероприятий является исполнение положений законодательных актов Российской Федерации в сфере информационной безопасности и утверждённых локальных распорядительных и

нормативных документов в этой отрасли в госархиве. В целях организации всестороннего контроля за обеспечением защиты информации в ГБУТО ГАТО основные обязанности в этой области распределены между следующими должностными лицами госархива по направлениям:

- заместитель директора госархива является ответственным за контроль за обеспечение информационной безопасности в ГБУТО ГАТО, т.е. отвечает за определение направлений совершенствования и реализацию всех процедур, необходимых для поддержания достаточного уровня защищённости данных в госархиве [О назначении ответственных…];
- системный администратор отдела информационно-поисковых систем и защиты информации госархива является ответственным по контролю за информационной безопасностью и осуществляет техническую поддержку всего программного обеспечения, установленного в госархиве, в т.ч. применяемого и в целях защиты информации от различного рода технических угроз [О назначении ответственного…];
- администратор информационной безопасности вычислительной сети ОИПСиЗИ является ответственным за выполнение работ по обеспечению информационной безопасности в ГБУТО ГАТО и выполняет основные функции в этой области, в том числе:
    - администрирование подсистем, программно-аппаратных средств защиты информации в операционных системах, прикладного и системного программного обеспечения на предмет соответствия установленным нормам и правилам, в том числе получение сертификатов электронной подписи для сотрудников госархива;
    - проведение контрольных проверок работоспособности и эффективности применяемых в ГБУТО ГАТО программно-аппаратных средств защиты информации;

- разработка требований по защите данных в госархиве путём разработки методических, инструктивных и иных документов в области защиты информации.
- проведение анализа безопасности компьютерных систем [Должностная инструкция...].

В рамках исполнения своих должностных обязанностей указанные сотрудники реализуют комплексный подход к вопросам защиты информации в госархиве, в т.ч. путём использования специализированных программных средств и разработки локальных нормативных и методических актов, описывающих порядок и принципы работы по отдельным направлениям деятельности архивного учреждения с целью регламентации всех аспектов защиты и снижения вероятности нарушения такой защиты и минимизации возможного ущерба.

Организационная защита информации предусматривает регламентацию деятельности и действий ответственных за защиту информации сотрудников госархива на нормативно-правовом уровне, с целью затруднения и/или исключения неправомерного получения информации сторонними лицами, а также проявления внешних и внутренних угроз. Организационные меры ГБУТО ГАТО по защите информации предусматривают такие основные направления, как:

- организация режима пропускного режима в здание, охраны помещений с помощью охранно-пожарной и тревожной сигнализации;
- работа с сотрудниками госархива (объяснение правил безопасной работы в информационных системах, уведомление о возникновении возможных мер ответственности за нарушение правил работы с информацией ограниченного доступа, изменениях в законодательстве по защите информации и работе с персональными данными);
- работа с документацией (разработка документации, регламентирующей обязанности сотрудников при работе с информацией ограниченного доступа, определяющие порядок

использования специализированных информационных систем и носителей конфиденциальной информации и др., внесение изменений и дополнений в ранее утверждённые документы или их полное пересоставление);

- использование технических средств обеспечения безопасности информации (установка специализированных лицензионных программных средств на рабочие места, где осуществляется обработка персональных данных, с целью предупреждения вирусных атак и возможных вторжений в информационную среду госархива);
- периодическая информационно-аналитическая деятельность по выявлению внешних и внутренних угроз и планирование комплекса мероприятий по обеспечению защиты на конкретный период и др.

На сегодняшний день в Тюменском облгосархиве имеют документальное закрепление такие направления в области защиты информации, как определение ответственных за подписание электронной подписью служебных документов в различных программных комплексах, обработка персональных данных в бумажном и автоматизированном виде, определение перечней конфиденциальной информации и данных, обрабатываемых в информационных системах, работа с запросами субъектов персональных данных или уполномоченного органа по защите прав субъектов персональных данных и др. Подробный анализ организационных мер, регламентированных в локальных актах ГБУТО ГАТО, содержится во второй главе настоящей диссертации.

Организационные мероприятия имеют первостепенную роль в формировании эффективного механизма защиты данных госархива, так как появление угроз информации обуславливается в большинстве случаев не техническими аспектами, а злоумышленными действиями или допущенной небрежностью сотрудников. В случае использовании одних только технических средств практически невозможно избежать влияния этих аспектов. В целях минимизации возможности возникновения угроз безопасности данных необходимо применять целый комплекс организационно-правовых и

организационно-технических мероприятий, которые бы максимально снизили или даже исключили возможность возникновения угроз защищаемой информации, что и реализуется в ГБУТО ГАТО.

Техническая защита предусматривает использование комплекса технических средств при организации защиты данных. При этом применение конкретных средств должно обуславливаться реальными потребностями учреждения, а не являться типовым (пакетным) решением. Первый вариант такой защиты нацелен на дополнительное обеспечение безопасности аппаратного обеспечения – систему взаимосвязанных технических устройств, предназначенных для ввода, обработки, хранения и вывода информации [Захаров, с. 7]. Иными словами – на персональные компьютеры госархива и их комплектующие: системные блоки и мониторы или моноблоки, клавиатуры, компьютерные мыши, принтеры, сканеры и иные многофункциональные офисные устройства, установленные на рабочих местах сотрудников архива, осуществляющих обработку сведений ограниченного доступа. Применение таких мер характерно для тех учреждений, чьим основным направлением деятельности является обработка персональных данных или сведений ограниченного доступа, являющихся служебной тайной, например, для Центра занятости населения или государственных органов власти, для Тюменского облгосархива применение таких мер не предполагается.

Второй вариант технической защиты предполагает использование специализированного программного обеспечения – средств антивирусной защиты, средств криптографической защиты информации, различных утилит и расширений, обеспечивающих безопасность данных, установленные на конкретных рабочих местах. Данный вид защиты применяется в ГБУТО ГАТО путём установки на персональных компьютерах, где осуществляется обработка персональных данных сотрудников, средств антивирусной защиты (используется лицензионное программное обеспечение Dr.Web и антивирусный модуль в специализированной программе защиты), средств защиты информации (программный комплекс Secret Net), настройкой парольной системы входа не

только в учётную запись сотрудника на компьютере, но и в каждую из используемых программ.

Некоторые из названных направлений имеют документальное подтверждения осуществления таких действий. Например, контроль сроков применения электронных подписей осуществляется путём из учёта в соответствующем журнале, представленном в табличной форме, в которой указывается дата получения сертификата безопасности, срок его действия, фамилия и инициалы должностного лица, которое будет осуществлять работу с ЭП, а также название системы, для внесения сведений и их обработки в которой используется это криптографическое средство [Журнал учёта сроков…]. Основным документом, отражающим движение съёмных носителей с записанными на них сертификатами безопасности, является Журнал учета выдачи карт и флеш-накопителей с электронной подписью [Журнал учёта выдачи…]. Журнал состоит из следующих граф:

- № п/п;
- вид носителя;
- фамилия и инициалы владельца электронной подписи;
- фамилия и инициалы лица, которому выдан носитель в целях осуществления должностных полномочий;
- дата произведения такой выдачи;
- подпись сотрудника, принимающего носитель, содержащий электронную подпись;
- дата возврата носителя должностному лицу, ответственному за контроль обеспечения безопасности при проведении мероприятий этого направления (системный администратор или администратор информационной безопасности вычислительной сети);
- подпись сотрудника, передающего ЭП;
- примечания, в которых могут быть указаны такие обстоятельства, как цель получения электронной подписи.

Ещё одним учётным документом, отражающим проведение тех или иных мероприятий ГБУТО ГАТО в сфере информационной безопасности, можно назвать Журнал учёта проведения в госархиве антивирусных проверок. Помимо даты осуществления проверки в нём указываются название отдела и имя компьютера или сервера, на которых производится проверка. В следующей графе даётся название специализированного средства – программного продукта, с помощью которого выяснялось наличие угроз безопасности. В целях подтверждения факта проведения проверки в журнал была включена графа «Количество проверенный файлов», т.к. отображение таких сведений в отчёте антивирусного ПО подтверждает факт завершения антивирусного анализа [Журнал учёта проведения…].

Для отображения обнаруженных в процессе проведения проверки угроз предусмотрена графа 7 «Количество и наименования инфицированных файлов, источник поступления», а результаты устранения таких внештатных ситуаций фиксируются в графе примечания – применённые меры могут фиксироваться здесь при помощи формулировки «Удалено Dr.Web», т.е. даётся указание факта совершённого с заражёнными объектами действия и название программы, которая осуществила указанную процедуру. Последней графой журнала является отметка об исполнителе, где напротив каждой сделанной записи (каждого компьютера или сервера Тюменского облгосархива) указывается фамилия сотрудника, осуществившего антивирусную проверку и, в случае необходимости, обезвреживание вирусных файлов.

ГЛАВА 2. АНАЛИЗ И МОДЕРНИЗАЦИЯ КОМПЛЕКСОВ ОРГАНИЗАЦИОННО-ПРАВОВОЙ И РАСПОРЯДИТЕЛЬНОЙ ДОКУМЕНТАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ГБУТО «ГОСУДАРСТВЕННЫЙ АРХИВ ТЮМЕНСКОЙ ОБЛАСТИ»

2.1. ТЕКУЩЕЕ СОСТОЯНИЕ ДЕЙСТВУЮЩЕЙ ОРГАНИЗАЦИОННО-ПРАВОВОЙ ДОКУМЕНТАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ГОСУДАРСТВЕННОМ АРХИВЕ ТЮМЕНСКОЙ ОБЛАСТИ

В ГБУТО «Государственный архив Тюменской области» имеется ряд самостоятельно разработанных и утверждённых документов по защите информации – в приказах в качестве приложений содержится ряд основных организационно-правовых документов в сфере защиты конфиденциальной информации, в том числе персональных данных при их обработке в госархиве. При этом документа, регламентирующего общий порядок работы в этой сфере, или определяющего направления такой работы, в ГБУТО ГАТО нет. Существующие документы по защите информации облгосархива можно условно разделить на следующие группы:

- инструкции для должностных лиц, осуществляющих те или иные полномочия по защите информации в соответствии с возложенными на них обязанностями (Инструкция администратору безопасности информации в информационных системах персональных данных, Инструкция ответственному за эксплуатацию информационных систем персональных данных, Инструкция работнику, ведущему обработку персональных данных без использования средств автоматизации);
- инструкции по выполнению отдельных видов работ в области защиты информации (Инструкция по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных, Инструкция по организации парольной защиты в информационных системах персональных данных, Инструкция по

организации антивирусной защиты в информационных системах персональных данных, Инструкция по организации резервирования и восстановления программного обеспечения и баз персональных данных информационных системах персональных данных, Инструкция о порядке работы пользователей информационных систем персональных данных в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, Инструкция о порядке проверки электронного журнала обращений к информационным системам персональных данных, Инструкция по использованию средств защиты информации в информационной системе персональных данных, Инструкция по обработке запросов субъектов персональных данных или уполномоченного органа по защите прав субъектов персональных данных, Инструкция о порядке учета, хранения, уничтожения носителей персональных данных);

- перечни информации ограниченного доступа (Перечень конфиденциальной информации, Перечень персональных данных, обрабатываемых в информационных системах персональных данных ГБУТО «Государственный архив Тюменской области»);
- схема контролируемой зоны;
- положение «Об обработке и защите персональных данных в ГБУТО «Государственный архив Тюменской области»».

Перечисленные локальные акты были внедрены в работу в целях исполнения требований федерального законодательства и постановлений Правительства Российской Федерации о работе с информационными технологиями и обеспечении защиты информации и персональных данных в процессе работы с ними [О персональных данных…]. В самих документах отсылки на отечественное законодательство, в рамках которого осуществляется тот или иной вид работ, не указаны. Все вышеуказанные инструкции являются приложениями к приказу ГБУТО ГАТО «Об утверждении инструкций по обеспечении безопасности персональных данных в информационных системах

персональных данных» от 27.07.2014 № 13 и оформлены в большинстве случаев однотипно: структура документов включает общие положения, тематические разделы и приложения.

Инструкция администратору безопасности в информационных системах персональных данных, Инструкция ответственному за эксплуатацию информационных систем персональных данных и *Инструкция работнику, ведущему обработку персональных данных без использования средств автоматизации*, *Инструкция ответственного за организацию обработки персональных данных в ГБУТО ГАТО* определяют основные обязанности, права и ответственность указанных лиц при работе с персональными данными с использованием средств автоматизации и без использования таковых, описывают особенности и порядок работы специалистов. Анализ содержания рассматриваемых инструкций приведён в таблице 1.

Таблица 1

Анализ содержаний инструкций должностных лиц,

ответственных за различные направления защиты информации в госархиве

Название документа	Инструкция администратору безопасности в информационных системах персональных данных	Инструкция ответственному за эксплуатацию информационных систем персональных данных	Инструкция работнику, ведущему обработку персональных данных без использования средств автоматизации	Инструкция ответственному за организацию обработки персональных данных в ГБУТО ГАТО
1	2	3	4	5
Кол-во листов документа	4,5	1	2,5	5,5
Структура текста	Документ имеет 4 раздела, разделённых на подпункты: – «Общие положения», где рассмотрены назначение документа, порядок назначения администратора безопасности в информационных системах персональных данных, функции администратора; – «Обязанности администратора безопасности информации информационных систем персональных данных», в числе которых перечислены 14 направлений защиты	Текст Инструкции разделён на 4 подпункта: – в первом указано назначение документа; – во втором пункте описаны основания для допуска и прекращения допуска работника к персональным данным, обрабатываемым в информационных системах персональных данных ГБУТО «Государственный архив Тюменской области»; – в 3 пункте указывается обязанность ведения Журнала	Инструкция разделена на 3 раздела, разбитых на подпункты: – «Общие положения» описывают назначение документа, возложение ответственности за соблюдение правил эксплуатации информационных систем, подчинённость ответственного за эксплуатацию этих систем; – «Обязанности ответственного за эксплуатацию ИСПДн»	Структура текста документа включает в себя следующие разделы: –«Список сокращений и определений»; –«Общие положения», где указано назначение документа, сфера его распространения, порядок назначения ответственного и его подчинённость, регламентируются требования к рабочему месту ответственного;

	информации в информационных системах персональных данных, например, осуществление контроля за соблюдением безопасности при работе с информацией ограниченного доступа, проведение инструктажей и др.; – «Права администратора безопасности информации в информационных системах персональных данных» – указаны 3 основных направления: право требовать от работников соблюдения установленной технологии обработки информации, инициировать проведение служебных расследований, обращаться к ответственным должностным лицам в сфере защиты информации при несоблюдении установленных технологий работы с персональными данными. – Ответственность администратора безопасности информации госархива рассмотрена в документе последней.	учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных; – в 4 пункте указано, каким образом учитывается вышеуказанный Журнал в номенклатуре дел госархива и на кого возлагается обязанность по его ведению.	состоят из 9 направлений, указанных во втором разделе Инструкции; – В разделе «Права ответственного» указаны такие права, как право инициировать проведение служебных расследований, подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты на своем участке работы.	–Во втором разделе «Должностные обязанности» перечислена 21 функция; –Третий разделе перечислены права ответственного за организацию обработки персональных данных в ГБУТО ГАТО, в т.ч. прописаны функции контроля за общим состоянием безопасности данных в учреждении; –Раздел «Ответственность» состоит из одного предложения, где делается отсылка на действующее отечественное законодательство; –Последний раздел – «Заключительные положения» – содержит условия пересмотра документа (изменение законодательства России о персональных данных).

В Инструкции работнику, ведущему обработку персональных данных без использования средств автоматизации, в ГБУТО ГАТО подробно описан порядок приёма запросов от субъектов персональных данных, а также перечень действий по предоставлению ответов на различные категории запросов касаемо обработки персональных данных в госархиве. В разделе «Общие положения» раскрыто понятие персональных данных, охарактеризованы такие термины, как «автоматизированная обработка персональных данных» и «неавтоматизированная обработка персональных данных», сделана отсылка на отечественное законодательство как дополнительный источник регламентации этого вида деятельности, однако перечисления конкретных названий законов или иных правовых актов в документе нет [Инструкция работнику…].

Особенности организации обработки персональных данных без средств автоматизации перечислены во втором разделе. Здесь приведены принципы раздельной обработки с другими документами, запрет фиксации на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы, отдельно перечислены условия использования типовых форм документов и др. Последний раздел Инструкции имеет название «Обеспечение безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации». Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы для каждой категории персональных данных можно было определить места хранения таких данных (материальных носителей), а также установить перечень должностных лиц организации, осуществляющих обработку персональных данных либо имеющих к ним доступ. В связи с этим положением в последнем разделе рассматриваемой Инструкции вновь ставится необходимость обеспечения возможности раздельного хранения материальных носителей ГБУТО ГАТО, содержащих персональные данные, отвечающих различным целям обработки.

С учётом наличия в ГБУТО ГАТО Инструкции работнику, ведущему обработку персональных данных без использования средств автоматизации

можно предположить наличие аналогичного документа, регламентирующего порядок осуществления сходного направления работы – обработку персональных данных с использованием средств автоматизации или хотя бы наличие в иных организационно-правовых документах госархива пункта с перечислением регламентирующих этот процесс локальных актов госархива. Однако данный процесс регулируется только должностной инструкцией сотрудника, отвечающего за работу с кадрами в госархиве.

Инструкция ГБУТО ГАТО по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных, определяет порядок учета лиц, чья основная деятельность связана именно с обработкой персональных данных при использовании информационных системах. В документе, состоящем из четырёх пунктов, указано, что для учёта лиц, допущенных к работе с персональными данными в информационных системах персональных данных, ведется «Журнал учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных». Отдельным пунктом в Инструкции дано уточнение оснований для допуска работника к обработке персональных данных и соответствующим информационным системам персональных данных, а также прекращения такого допуска [Инструкция по учёту…]. Иные сведения Инструкция не содержит.

Инструкция Тюменского облгосархива по организации парольной защиты в информационных системах персональных данных регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных, а также контроль за действиями пользователей при работе с паролями. Текст документа состоит из 8 пунктов, где рассматриваются такие вопросы, как возложение ответственности за проведение этого вида работ, порядок генерации и распределения паролей, требования к паролям, ответственность за разглашение парольной информации, порядок реагирования при возникновении нештатных ситуаций, периодичность смены паролей [Инструкция по организации…].

По своему содержанию документ охватывает практически все направления этого вида работы, при этом не оговорены порядок смены паролей при увольнении сотрудника, имеющего доступ к одной системе или же нескольким программным продуктам, в которых обрабатываются сведения ограниченного доступа. Действие инструкции распространяется только на работу с персональными данными, при этом целесообразно было бы расширить её регламентацию и на порядок работы с официальной электронной почтой госархива, и на работу с системами межведомственного электронного документооборота.

Инструкция ГБУТО ГАТО по организации антивирусной защиты в информационных системах персональных данных определяет требования к организации антивирусной защиты информационных систем персональных данных от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность работников структурных подразделений, осуществляющих эксплуатацию и сопровождающих информационные системы персональных данных, за их выполнение [Инструкция по организации…]. Текст документа состоит из трёх разделов, размещённый на 3,5 страницах, и включает в свой состав регламентацию таких направлений деятельности как:

- категории антивирусных средств для допуска к использованию в информационных системах персональных данных;
- определение ответственных за функционал по установке и настройке антивирусных программ;
- порядок применения средств антивируского контроля: указаны периодичность и порядок проведения такого контроля, основания признания обязательности такого контроля для отдельных рабочих мест;
- уведомление при возникновении подозрений на наличие угрозы информационной системе, последовательность реагирования на такие сообщения.

Более подробно недостатки документа и пути их устранения рассмотрены в пункте 3.3. настоящей диссертации.

Инструкция ГБУТО ГАТО по организации резервирования и восстановления программного обеспечения и баз персональных данных в информационных системах персональных данных определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных ГБУТО «Государственный архив Тюменской области» с целью обеспечения возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним. Документ состоит из четырёх разделов, разделённых на подпункты. В первом разделе «Общие положения» дано обоснование разработки и внедрения в работу инструкции, а также сфера её распространения [Инструкция по организации…].

Второй раздел имеет название «Резервируемое программное обеспечение и базы персональных данных» и состоит из одного подпункта. В нём рассматриваются категории данных информационных систем персональных данных госархива, подлежащих резервированию. Определению порядка резервирования и хранения резервных копий отведён третий раздел. Здесь указано, что резервирование общего и прикладного программного обеспечения, а также программного обеспечения и специализированных средств защиты информации обеспечивается путём организации хранения у администратора защиты информации машинных носителей информации, содержащих дистрибутивы данного программного обеспечения. При этом во втором подпункте даётся оговорка о том, что резервирование данных в информационной системе персональных данных «Бухгалтерия» осуществляется автоматически программными комплексами «Контур-экстерн» и «Парус». В четырёх пунктах рассматривается порядок работы с резервными носителями персональных данных, однако на практике в работе они не применяются. Последний, четвёртый раздел описывает порядок восстановления работоспособности информационной системы персональных данных – указаны возможные случаи, в которых может потребоваться выполнение этого вида работы, возлагается ответственность за его исполнение.

В данный момент большинство положений Инструкции являются неактуальными ввиду перехода на онлайн-формат работы ещё и информационной системы персональных данных «Директум», у которой также имеется своё сетевое хранилище данных, т.е. на настоящий момент времени в госархиве фактически отсутствуют системы, требующие резервного копирования и восстановления в случае утраты работоспособности – при работе с онлайн-платформами эти вопросы решают службы поддержки этих систем.

Инструкция ГБУТО ГАТО о порядке работы пользователей информационных систем персональных данных в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных определяет безопасный порядок действий пользователей информационных систем персональных данных, исключающий или минимизирующий вероятность возникновения угроз персональным данным при их обработке в информационных системах персональных данных. Инструкция состоит из 9 пунктов, в которых определяются, что допуск сотрудников к информационным системам персональных данных осуществляется только в соответствии с утверждёнными списком должностных лиц, допущенных к обработке персональных данных сотрудников Государственного бюджетного учреждения Тюменской области «Государственный архив Тюменской области» с использованием средств автоматизации [Инструкция о порядке…]. Далее возлагается ответственность на пользователей за правильность использования систем, конкретизируется порядок получения идентификатора (имени пользователя) и аутентификатора (пароля) к системе.

Отдельными пунктами вынесена информация о порядке записи информации, содержащей персональные данные, на съемные машинные носители информации, порядок работы с ними. В подпунктах 8.1-8.6 перечислена ответственность сотрудников, допущенных к обработке персональных данных сотрудников ГБУТО «Государственный архив Тюменской области» с использованием средств автоматизации. Отличительной

чертой рассматриваемой Инструкции от других документов госархива по защите информации является наличие вынесенных в отдельный пункт направлений деятельности, выполнение которых сотрудникам категорически запрещается. К ним относятся, например, осуществление обработки конфиденциальных данных в присутствии посторонних (не допущенных к данной информации) лиц, запись и хранение конфиденциальной информации на неучтенных машинных носителях информации (гибких магнитных дисках, флеш-накопителях и т.п.).

Инструкция ГБУТО ГАТО о порядке проверки электронного журнала обращений к информационным системам персональных данных в шести разделах на трех листах определяет задачи и порядок проведения такой проверки, описывает существующие штатные журналы операционной системы и последовательность работы с ними. В первый раздел вынесены задачи такого аудита, то есть отслеживания событий, происходивших на автоматизированных рабочих местах в течение определенного промежутка времени. Поскольку события, происходящие на автоматизированных рабочих местах, входящих в состав информационных систем персональных данных, регистрируются в системных журналах, общая информация о таких журналах включена в раздел 2, отдельно же рассмотрены штатные журналы операционной системы и журнал событий средств защиты информации – в 3 и 4 разделах соответственно [Инструкция о порядке…]. В то же время в документе дана только общая характеристика этих учётных документов, порядок работы с ними (например, выгрузка данных) в тексте инструкции не оговорены.

В разделе 5 «Аудит» в единственном входящем в его состав пункте сделана отсылка на руководства пользователей к используемым средствам защиты информации, без какой-либо конкретизации. Завершающим разделом для документа является «Просмотр событий электронных журналов», где возлагается ответственность за проверку электронных журналов на администратора защиты информации (в настоящий момент должность имеет другое название), определена периодичность такой проверки – 1 раз в месяц, а также обязанность доклада о фактах обнаружения нарушений ответственному за

выполнение работ по обеспечению безопасности персональных данных в информационных системах персональных данных (которым по функционалу также является сам администратор защиты информации, чего не должно быть).

Инструкция ГБУТО ГАТО по использованию средств защиты информации в информационной системе персональных данных указывает, какими методическими документами необходимо руководствоваться при работе со средством защиты информации от несанкционированного доступа «Secret Net» и программным комплексом VipNetClient [Инструкция по использованию…]. По своей сути документ инструктивной составляющей не имеет, т.к. является кратким перечнем, представленном на одном листе, разделённым на две части – по одному для каждого из средств.

Инструкция по обработке запросов субъектов персональных данных или уполномоченного органа по защите прав субъектов персональных данных в ГБУТО «Государственный архив Тюменской области» является самым развёрнутым в плане раскрытия содержания инструктивным документом архивного учреждения. Её структура состоит из четырёх разделов. В «Общих положениях» указана сфера распространения документа: данная инструкция регулирует отношения, возникающие при выполнении ГБУТО «Государственный архив Тюменской области» обязательств согласно требованиям статей 14, 20 и 21 Федерального закона «О персональных данных» 152-ФЗ от 27 июля 2006 года. Во втором разделе возложена ответственность за организацию и проведение работы по выдаче ответов на запросы и устранению выявленных нарушений на «администраторов защиты информации» - формулировка указана обобщённо, фактически в штате числится один специалист, занятый в этой сфере. Здесь же подразумевается вовлечение в работу еще и системного администратора госархива, чьи обязанности как раз «завязаны» на решение технических вопросов, например, устранение нарушений в программных продуктах. в т.ч. путём взаимодействия со службами поддержки различных систем [Инструкция по обработке…]. Следующие два раздела – «Действия в ответ на запросы по персональным данным» и «Прием запросов от

субъектов персональных данных или его законных представителей, а также от уполномоченного органа, по защите прав субъектов персональных данных» являются изложением принципов и последовательности действий по выполнению этих видов работ.

Инструкция содержит ряд приложений:

- в приложении № 1 к Инструкции приведена *Сводная таблица* действий в ответ на запросы по персональным данным с указанием тематики запроса, цепочки осуществляемых действий, сроков их реализации и вида предоставляемого ответа;
- в приложении № 2 содержится форма *Журнала обращений граждан* (субъектов персональных данных) по вопросам обработки персональных данных ГБУТО ГАТО;
- в приложение № 3 включена форма *Запроса субъекта* персональных данных о наличии и ознакомлении с персональными данными;
- в приложении № 4 приведена форма *Запроса субъекта* персональных данных на уточнение персональных данных, в приложении № 5 – на уничтожение, в приложении № 6 – на отзыв согласия на обработку персональных данных;
- в приложении № 7 содержится форма *Ответа на запрос* субъекта персональных данных о наличии и на ознакомление с персональными данными, в приложении № 8 – на уточнение персональных данных, в приложении № 9 – на уничтожение персональных данных, в приложении № 10 – на отзыв согласия на обработку персональных данных;
- в приложение № 11 включена форма *Уведомления* субъекта персональных данных, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных при выявлении недостоверности персональных данных;

– в приложении № 12 приведена форма *Уведомления* субъекта персональных данных, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных при выявлении неправомерности действий с персональными данными.

На практике каких-либо запросов сотрудников об изменении, уточнении или удалении их персональных данных не зафиксировано, *Журнал учёта обращений граждан* (субъектов персональных данных) по вопросам обработки персональных данных ГБУТО «Государственный архив Тюменской области» не ведётся.

Текст *Инструкции о порядке учета, хранения, уничтожения носителей персональных данных ГБУТО «Государственный архив Тюменской области»* разделён на 18 подпунктов. В первом из них дано определение персональных данных, дублирующее пункт 1 статьи 3 ФЗ «О персональных данных», дополненные при этом конкретизирующими положениями из отраслевых приказов по работе с информацией, содержащей персональные данные, таких учреждений, как Росстат [Об утверждении статистического…], Росжелдор [Об организации работы…], Росздравнадзор [О защите персональных данных…] и др. Работа с носителями персональными данных рассматривается в следующих аспектах:

– обязательность их учёта и выдачи рассмотрена в пунктах 2 и 3;
– срокам и порядку хранения отведены пункты с 4 по 6;
– в 7 пункте определён порядок отправки и передачи персональных данных сотрудников, причины таких действий в тексте Инструкции не оговорены;
– этапы работы при обнаружении фактов утраты съёмных носителей, содержащих персональные данные, кратко описаны в пункте 8;
– рекомендации по парольной защите данных на съёмных носителях даны в 9 пункте;

- меры, необходимые для обеспечения внешней защиты персональных данных заявителя, перечислены в 10 пункте Инструкции;
- в 11 пункте прописана обязанность должностных лиц, чья деятельность связана с получением, осуществлением обработки и защитой персональных данных, подписать обязательство о неразглашении персональных данных работников (актуальное название документа в настоящий момент времени – «Обязательство о неразглашении информации, содержащей персональные данные»);
- в следующих двух пунктах рассмотрена возможность передачи документов, содержащих персональные данные, по завершении работы с ними в архив;
- вопросам уничтожения персональных данных отведены последние 5 пунктов (с 14 по 18). В первом из них приведён термин «уничтожение персональных данных» в соответствии с профильным законодательством [О персональных данных…], далее даётся отсылка на законодательство при определении сроков хранения персональных данных. Уничтожение носителей, содержащих персональные данные рассмотрено в части порядка их уничтожения, составления акта по результатам проведения работы и уведомления о произведённых действиях субъекта персональных данных. Форма акта приведена в приложении 1 к Инструкции, при этом она предусматривает комиссионное рассмотрение вопроса, однако, единственной действующей комиссией на момент разработки Инструкции являлась комиссия по классификации информационных систем персональных данных. Положение о комиссии утверждено не было, но исходя из названия этого органа нельзя сделать вывод о том, что она занималась также согласованием уничтожения носителей персональных данных.

Более подробно недостатки документа и пути их устранения рассмотрены в пункте 3.3. настоящей диссертации.

На основании пункта 3 Перечня сведений конфиденциального характера,

утверждённого Указом Президента Российской Федерации от 06.03.1997 № 188, главы 14 Трудового кодекса Российской Федерации и федеральных законов составлен *Перечень конфиденциальной информации ГБУТО «Государственный архив Тюменской области»*. Документ является приложением к приказу от 27.07.2014 № 14 и содержит вводную текстовую часть, где указано, что поступающая конфиденциальная информация о юридических и физических лицах, находящихся в ведении ГБУТО «Государственный архив Тюменской области», подлежит ограничению в допуске. Отдельно прописано, что информация ограниченного доступа может быть представлена в электронном виде и на бумаге. Сам Перечень представлен в табличной форме и состоит из двух граф: «№ п/п» и «Сведения конфиденциального характера» [Перечень конфиденциальной информации…]. Всего в перечень включено 14 пунктов.

Перечень персональных данных, обрабатываемых в информационных системах персональных данных ГБУТО «Государственный архив Тюменской области» утврждён приказом госархива № 15 от 27.07.2014. Документ представлен в табличной форме и состоит из следующих граф: «№ п/п», «Информационная система персональных данных», «Название персональных данных», «Срок хранения». Включённые в Перечень данные разграничены в зависимости от информационной системы, в которой они обрабатываются – «Директум» или «Бухгалтерия» – на две части, расположенные друг за другом [Перечень персональных данных…].

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств [О перечне…]. В целях обеспечения безопасности при обработке сведений конфиденциального характера в госархиве была разработана *Схема контролируемой зоны ГБУТО ГАТО.* Документ представлен в графическом виде (рисунок) с указанием конкретных кабинетов здания Тюменского облгосархива, расположенного по адресу: г. Тюмень, пр. Геологоразведчиков, д. 21, в которых осуществляется обработка персональных данных сотрудников госархива. Схема

помещена в приложение № 1 к приказу ГБУТО ГАТО «Об определении границ контролируемой зоны» от 27.07.2014 № 17. В тексте приказа указан адрес помещения, которое изображено на схеме, а также даны уточнения, в каком из выделенных помещений ведётся работа с каждой из имеющихся систем.

Положение об обработке и защите персональных данных в Государственном бюджетном учреждении Тюменской области «Государственный архив Тюменской области» определяет порядок сбора, хранения, передачи и любого другого использования персональных данных работников госархива в соответствии с законодательством Российской Федерации. Целью разработки Положения стало закрепление механизмов обеспечения прав субъекта на сохранение конфиденциальности информации о фактах, событиях и обстоятельствах его жизни, что отражено в разделе «Общие положения». Здесь же обоснована цель издания документа, его назначение и правовые основы разработки. В отдельный элемент структуры документа выделен перечень понятий, упоминаемых в Положении.

Далее перечислены требования, обязательные для соблюдения на различных этапах работы с персональными данными, в том числе во время их получения, обработки, хранения, передачи и уничтожения. в этим же разделе приведён перечень сотрудников госархива, имеющих право доступа к персональным данным, который дублирует аналогичный по содержанию документ – *Список* должностных лиц ГБУТО ГАТО, обрабатывающих персональные данные в информационных системах персональных данных с использованием средств автоматизации, утверждённый приказом от 06.12.2016 № 19 [Положение об обработке…].

Также отдельно перечислены права и обязанности субъектов персональных данных и оператора, указана ответственность за нарушение норм, регулирующих процессы обработки и защиты персональных данных. Деления на разделы как такового в документе нет, различные по тематике элементы разделяются обобщёнными заголовками, вынесенными перед абзацем и выделенные полужирным начертанием. Приложением № 1 к Положению

является форма *Заявления-согласия* субъекта на обработку его персональных данных.

Положения большинства рассмотренных инструкций, касающихся обработки информации в автоматизированном виде, не отвечают современной практике работы в части выделенных этапов деятельности и полноты их содержания, в том числе потому, что их положения должны быть актуальны не только для рабочих мест, где обрабатываются персональные данные, но и для компьютеров других сотрудников, т.к. все компьютеры госархива связаны локальной сетью, а реализация угроз на одном из них может повлечь возникновение ущерба и на других.

В связи с этим указанные документы будут считаться утратившими силу, вместо них в рамках данной работы будут разработаны новые инструкции, утверждённые ранее инструкции за основу браться не будут, т.к. качество включённой в них информации и структура и содержание текста не соответствует требованиям, предъявляемым к этой категории документов госархива. О возможных дальнейших направлениях работы в области проектирования методических документов по защите информации в госархиве подробно сказано в п. 3.3 настоящей диссертации.

Что касается оформления рассмотренных документов, отклонений от установленных правил здесь практически не встречается, однако имеются многочисленные ошибки технического характера – опечатки, нарушение нумерации внутри разделов, отсутствие или указание излишних знаков препинания.

В утверждённых в госархиве документах по защите информации требования к оформлению (наличию реквизитов и их расположению) соблюдены в полной мере. Однако, изначально не было предусмотрено согласование разрабатываемых документов с коллегиальным органом госархива – например, с комиссией по защите информации, в состав которого были бы включены специалисты, ответственные за различные направления работ по защите информации, а также специалисты юридического направления. Возможными

причинами допущенного отклонения является отсутствие в рассматриваемый период чётко регламентированных правил к сотрудникам, занимающим должности ответственных за обеспечение информационной безопасности, а также недостаточностью практических материалов и опыта российских учреждений в разработке документации, что является типовой проблемой и касается не только Тюменский облгосархив.

2.2. ПОРЯДОК РАЗРАБОТКИ, СОДЕРЖАНИЕ И ОФОРМЛЕНИЕ ПРИКАЗОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ГОСАРХИВЕ

Основным видом документации в комплексе по защите информации является такой организационно-распорядительный документ как приказ. Это акт, носящий правовой характер, который издаётся непосредственно руководителем учреждения с целью решения возникающих в процессе деятельности как текущих (оперативных), так и перспективных задач, в том числе в области защиты информации [Дроздова. Как приказы помогают…, с. 83-90]. В госархиве приказ представляет собой правовой акт директора, содержащий обязательные поручения для подчиненных структурных подразделений, должностных лиц и рядовых работников.

Если этапы создания приказа аналогичны порядку разработки иных документов, то с осознанием того, какие приказы нужно издавать в учреждении, чтобы регламентировать вопросы защиты данных, дело обстоит сложнее. Прямых указаний или перечней в отечественном законодательстве на этот счёт не приведено, что, однако, позволяет учитывать интересы своей организации при проектировании комплекса документации по защите информации. Основной вид сведений, подлежащих защите в соответствии с законодательством Российской Федерации, помимо различных видов тайн – это персональные данные. За основу тут берутся ратифицированные документы Совета Европы, положения кодексов Российской Федерации, ряд федеральных законов, указы Президента России, постановления российского Правительства и распорядительные и методические

документы российской Федеральной службы по техническому и экспортному контролю. Указанные в названных актах требования к документам по регламентации защиты данных персонального характера могут быть использованы в качестве основы для собственных разработок, что как раз и позволяет пробел в законодательстве касаемо иных видов охраняемых данных, не относящихся к какому-то из видов тайн.

Для тех организаций, чья деятельность не требует специализированной технической защиты данных и отражения постоянных угроз информации, к числу которых относится и ГБУТО «Государственный архив Тюменской области», приказы по защите информации будут разрабатываться в соответствии с основными этапами работы в этой сфере:

- *приказ о назначении ответственных* за реализацию отдельных функций в сфере информационной безопасности. Тут спектр направлений весьма широк и зависит только от нужд организации в текущий момент – назначаются ответственные по каждому виду работ или только за обработку персональных данных или обеспечение безопасности при работе с информационными системами, резервное копирование данных, утверждаются составы комиссий и т.д.;
- *приказы о закреплении полномочий* – например, по использованию электронной подписи, закреплению права подписания определённых видов документов конкретными должностными лицами;
- *приказы, вводящие в действие другие документы*, – политики и положения обработки данных, списки лиц, инструкции и др. Ими могут быть регламентированы как должностные обязанности конкретного сотрудника, целого подразделения или же порядок выполнения конкретной функции или одной операции в учреждении;
- *приказы ограниченного срока действия* (разового характера) – например, об утверждении планов проведения мероприятий по защите информации, организации пропускного режима на период проведения работ и др.;

- *приказы постоянного (до изменения существенных условий) действия* – о вводе в эксплуатацию систем, об утверждении перечня автоматизированных мест, на которых обрабатываются данные ограниченного доступа и др.;
- *приказы об утверждении форм документов* – например, журналов учёта съёмных носителей данных, проведения инструктажей по вопросам защиты данных, или документов по работе с обращениями граждан (формы заявлений, ответов, согласия на обработку персональных данных) [Дроздова. Как приказы помогают…, с. 83-90].

За 2009-2020 гг. (с момента включения рассматриваемого вида работ в основную деятельность госархива по 25.12.2020) в госархиве было издано 57 приказов в области обеспечения информационной безопасности, из них 13 приказов содержат информацию о назначении ответственных лиц за организацию отдельных направлений деятельности в области работы с информацией ограниченного доступа (в т.ч. комиссии), их них в настоящее время 2 требуют замены. Перечень приказов ГБУТО ГАТО о назначении ответственных по защите информации представлен в таблице 2.

Таблица 2

Перечень приказов ГБУТО «Государственный архив Тюменской области» о назначении ответственных по защите информации

№ п/п	№ приказа	Дата приказа	Заголовок приказа
1	2	3	4
1.	30	23.12.2020	Об утверждении перечней должностей, допущенных к обработке персональных данных сотрудников Государственного бюджетного учреждения Тюменской области «Государственный архив Тюменской области»

2.	18	26.06.2020	О назначении ответственных за обеспечение информационной безопасности в Государственном бюджетном учреждении Тюменской области «Государственный архив Тюменской области»
3.	12	12.03.2020	О назначении ответственного за организацию обработки персональных данных
4.	10	21.03.2019	О назначении ответственного за организацию перехода на использование отечественного офисного программного обеспечения
5.	03	09.01.2017	О назначении ответственного за организацию обработки персональных данных
6.	19	06.12.2016	Об утверждении списка должностных лиц, обрабатывающих персональные данные
7.	17	05.12.2016	Об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Государственном бюджетном учреждении Тюменской области «Государственный архив Тюменской области»
8.	11	15.05.2015	О назначении ответственного за обеспечение информационной безопасности
9.	24	28.07.2014	О назначении ответственного за резервирование и восстановление баз персональных данных
10.	12	27.07.2014	Об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ГБУТО «Государственный архив Тюменской области»
11.	14	01.06.2011	Об организации работ по обеспечению безопасности персональных данных
12.	23	02.12.2010	Об организации работ по защите конфиденциальной информации
13.	18	27.07.2014	О постоянно действующей комиссии по классификации информационных систем персональных данных

Указанные приказы, которыми назначается один ответственный за какой-то из видов работ по защите информации госархива, имеют сходную структуру: в преамбуле текста приказа даются правовые основания и цели назначения ответственного сотрудника, а в распорядительной части – фамилия, имя, отчество, должность сотрудника, на которого возлагается функционал.

Приказы, в которых ответственность по выполнению ряда работ в области защиты данных распределяется между несколькими сотрудниками, в распорядительной части приказа даётся обобщённая формулировка, например, «Утвердить состав постоянно действующей комиссии… согласно приложению 1», а сам перечень уполномоченных сотрудников помещается в пришожение к приказу.

Вопросам предоставления права и закрепления полномочий по подписанию служебных документов электронной подписью в ГБУТО ГАТО посвящено 18 приказов. Из них 5 утратили силу в связи с увольнением сотрудника или сменой фамилии. Перечень приказов ГБУТО ГАТО о подписании служебных документов электронной подписью представлен в таблице 3.

Таблица 3

Перечень приказов ГБУТО «Государственный архив Тюменской области» о подписании служебных документов электронной подписью

№ п/п	№ приказа	Дата приказа	Заголовок приказа
1	2	3	4
1.	29	21.12.2020	О предоставлении права использования ключей электронной подписи
2.	04	11.03.2020	О предоставлении права использования ключей электронной подписи
3.	23	01.10.2019	О предоставлении права использования ключей электронной подписи

4.	13	14.05.2019	О возложении обязанностей по подписанию электронной подписью служебных документов
5.	26	13.11.2018	О предоставлении права использования ключей электронной подписи
6.	7-а	14.03.2017	О предоставлении права использования ключей электронной подписи
7.	15	18.11.2016	О предоставлении права использования ключей электронной подписи
8.	08	26.04.2016	О предоставлении права использования ключей электронной подписи
9.	05	25.02.2016	О предоставлении права использования ключей электронной подписи
10.	04	16.02.2016	О предоставлении права использования ключей электронной подписи
11.	03	02.02.2016	О закреплении полномочий использования средства криптографической защиты информации «Континент-АП»
12.	02	19.01.2016	О предоставлении права использования ключей электронной подписи
13.	15	31.08.2015	О предоставлении права использования ключей электронной подписи
14.	04	13.02.2015	О предоставлении права использования ключей электронной подписи
15.	03	05.02.2015	О предоставлении права использования ключей электронной подписи
16.	36	09.12.2014	О предоставлении права использования ключей электронной подписи
17.	7	10.03.2011	Об электронной цифровой подписи
18.	7	19.04.2012	О закреплении права подписания электронных документов электронной подписью в системе «АЦК-Госзаказ»

Рассматриваемая группа приказов характеризуется неизменностью текста: приказы о предоставлении права использования ключей электронной подписи оформляются однотипно за весь рассматриваемый период, единственными

переменными составляющими в них являются графа с указанием данных о лице, на которого возлагаются эти обязанности, и предпоследний пункт, в котором указываются ранее утверждённые документы, которые утратят силу в связи с изданием нового приказа. Этот вид приказов используется при передаче полномочий по работе с информационной системой (например, межведомственного электронного взаимодействия) при смене сотрудников.

Вторая группа приказов закрепляет права подписания служебных документах в информационных системах за конкретными должностными лицами. В этом случае приказ создаётся «с ноля», т.к. его содержание зависит от того, на специалиста какой должности накладывается функционал. Текст таких приказов в распорядительной его части может представлять собой краткую формулировку, например, «Оставить за собой полномочия на эксплуатацию средства криптографической эксплуатации «Континент-АП». В иных случаях может быть использована общая формулировка с отсылкой на приложение, а само приложение может представлять из себя перечень всех систем, с которыми работает должностной лицо.

Таким образом был оформлен приказ «О возложении обязанностей по подписанию электронной подписью служебных документов» № 13 от 14.05.2019. После перечисления законодательства, в соответствии с которым составлен документ, в распорядительной части текст разделён на три пункта: в первом приведена общая формулировка с отсылкой на приложение, в следующем пункте на сотрудника, ответственного за выполнение работ по защите информации в госархиве, возложены функции по ознакомлению с документом уполномоченных должностных лиц, в последнем пункте указано, что контроль за исполнением приказа останется за директором учреждения.

Приложение к приказу № 13 оформлено в табличном виде, где отражены такие графы как «№ п/п», «Должность работника, ответственного за составление служебных документов и их подписание электронной подписью», «Функциональные обязанности, выполняемые с использованием электронной подписи» и «Информационная система, в которой осуществляется подписание».

Информация в таблице разделена на две части: сначала идёт перечисление всех информационных систем, в которой осуществляет работу в соответствии с должностными обязанностями контрактный управляющий с указанием выполняемого функционала, затем по тому же принципу отражена информация по главному бухгалтеру.

В числе утверждённых документов по защите информации госархива числятся 18 приказов, которыми утверждаются методические документы – инструкции, положения и др., из них требует обновления – 1 (Политика обработки персональных данных). Перечень приказов ГБУТО ГАТО, которыми утверждаются методические документы в области защиты информации представлен в таблице 4.

Таблица 4

Перечень приказов ГБУТО «Государственный архив Тюменской области», которыми утверждаются методические документы в области защиты информации

№ п/п	№ приказа	Дата приказа	Заголовок приказа
1	2	3	4
1.	22	07.12.2016	Об обеспечении безопасности персональных данных (утверждена Политика обработки и защиты персональных данных)
2.	21	07.12.2016	Об определении уровня защищенности информационных систем персональных данных
3.	20	06.12.2016	Об утверждении матрицы доступа к информационным ресурсам и объектам доступа в информационной системе персональных данных «Бухгалтерия»
4.	26	27.07.2014	Об утверждении положения об обработке и защите персональных данных в ГБУТО «Государственный архив Тюменской области»
5.	25	29.07.2014	Об утверждении инструкций о пропускном и внутриобъектовых режимах

6.	23	28.07.2014	О утверждении инструкции о порядке учета, хранения, уничтожения носителей персональных данных
7.	22	28.07.2014	Об утверждении перечня должностей, обрабатывающих персональные данные с использованием средств информатизации
8.	21	28.07.2014	Об утверждении перечня должностей, обрабатывающих персональные данные без использования средств информатизации
9.	20	27.07.2014	Об утверждении матрицы доступа к информационным ресурсам и объектам доступа в информационной системе персональных данных
10.	19	27.07.2014	Об утверждении перечня автоматизированных рабочих мест, общесистемного и прикладного программного обеспечения
11.	17	27.07.2014	Об определении границ контролируемой зоны
12.	16	27.07.2014	Об утверждении перечня информационных систем персональных данных
13.	15	27.07.2014	Об утверждении перечня персональных данных
14.	14	27.07.2014	Об утверждении перечня конфиденциальной информации
15.	13	27.07.2014	Об утверждении инструкций по обеспечению безопасности персональных данных в информационных системах персональных данных
16.	16	25.07.2011	Об обеспечении сохранности персональных данных
17.	4	27.01.2009	Об определении границ контролируемой зоны объекта информатизации «АРМ РСП»
18.	3	27.01.2009	Об организации защиты информации на объекте информатизации «АРМ РСП»

В отдельный вид приказов по защите информации можно выделить 4 приказа, которые вносят изменения в ранее изданные приказы, другой информации или распорядительной составляющей эти правовые акты не имеют. Перечень приказов ГБУТО ГАТО о внесении изменений в ранее изданные приказы представлен в таблице 5.

Таблица 5

Перечень приказов ГБУТО «Государственный архив Тюменской области» о внесении изменений в ранее изданные приказы

№ п/п	№ приказа	Дата приказа	Заголовок приказа
1	2	3	4
1.	18	05.12.2016	О внесении изменений в приказы и признании утратившими силу отдельных пунктов приказов
2.	6	02.04.2012	О внесении изменений в перечень программных средств
3.	5	24.02.2012	О внесении изменений в перечень программных средств
4.	25	24.11.2011	О внесении изменений в перечень программных средств

По организации текущей работы госархива по защите информации за весь рассматриваемый период было издано 4 приказа. Все они имеют разовый характер, т.к. связаны с организацией деятельности в текущий момент времени. Перечень приказов ГБУТО ГАТО, которые регламентируют выполнение текущих работ по защите информации, представлен в таблице 6.

Таблица 6

Перечень приказов ГБУТО «Государственный архив Тюменской области», регламентирующих выполнение текущих работ по защите информации

№ п/п	№ приказа	Дата приказа	Заголовок приказа
1	2	3	4
1.	16	05.12.2016	Об утверждении плана мероприятий по защите персональных данных
2.	27	29.07.2014	О вводе в эксплуатацию автоматизированных рабочих мест для обработки персональных данных
3.	11	26.07.2014	Об утверждении плана мероприятий по защите персональных данных
4.	14	18.10.2012	Об организации пропускного режима в здании по ул. Воровского, 35

Таким образом в связи с обновлением законодательства, сменой сотрудников госархива, установкой новых лицензий программного обеспечения требуют замены следующие локальные акты:

- приказ от 07.12.2016 № 22 «*Об обеспечении безопасности персональных данных*» (необходимо обновление приложения – Политики обработки и защиты персональных данных в соответствии с актуальным законодательством);
- приказ от 06.12.2016 № 20 «*Об утверждении матрицы доступа к информационным ресурсам и объектам доступа в информационную систему персональных данных «Бухгалтерия*» (в тексте приказа перечислены уволенные сотрудники);
- приказ от 06.12.2016 № 19 «*Об утверждении списка должностных лиц, обрабатывающих персональные данные*» (указаны старые наименования должностей и уволенный сотрудник);
- приказ от 05.12.2016 № 17 «*Об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ГБУТО ГАТО*» (в п. 8 в числе ответственных за эксплуатацию информационных систем персональных данных «Бухгалтерия» и в приложении 5 в составе комиссии по классификации информационных систем персональных данных указаны уволенные сотрудники);
- приказ от 27.07.2014 № 19 «*Об утверждении перечня автоматизированных рабочих мест, общесистемного и прикладного программного обеспечения*» (требуется обновление перечня установленного программного обеспечения);
- приказ от 27.07.2014 № 16 «*Об утверждении перечня информационных систем персональных данных*» (необходимо убрать фамилии сотрудников, обновить инвентарные номера техники).

Принципы и правила оформления документов в учреждениях Российской Федерации регулируются рядом государственных стандартов, по большей части

имеющих рекомендательный характер, на их основе, а также с учётом правовой базы в сфере архивного дела, а также положений локальных актов госархива, разработана инструкция по делопроизводству, исходя из положений которой разрабатываются все локальные акты архива. Инструкция по делопроизводству ГБУТО «Государственный архив Тюменской области» разработана в соответствии со следующими документами:

- Федеральным законом № 125 [Об архивном деле …];
- Правилами 2020 г. [Правила организации хранения…];
- Правилами 2015 г. [Правила организации хранения…];
- Инструкцией Росархива по делопроизводству [Примерная инструкция…];
- госстандартом, посвящённом рассмотрению порядка оформления организационно-распорядительной документации [ГОСТ Р 7.0.97-2016];
- госстандартом, устанавливающим основные определения и термины в архивной сфере и делопроизводстве [Р 7.0.8-2013];
- рекомендациями по применению госстандарта «Организационно-распорядительная документация. Требования к оформлению документов» [Р 7.0.97-2016];
- Методическими рекомендациями по применению Правил 2015 г. [Правила организации хранения…];
- Уставом ГБУТО ГАТО.

Разработка любого приказа госархива, в том числе и по защите информации, включает в себя следующие этапы:

- сбор необходимой информации – для приказа, который создаётся впервые, на этом этапе необходимо уточнить цели его создания, определить, какие функции он должен регламентировать и для кого. Если ранее документация по защите информации в учреждении уже разрабатывалась, осуществляется анализ полноты и качества текста ранее утверждённых документов, определяются направления их

совершенствования, уточняются сведения, выявляются группы локальных нормативных актов, регулирующих смежные вопросы, которые может быть целесообразно объединить в один документ;

- подготовка проекта документа – создание документа в электронном виде с указанием всех необходимых реквизитов, проверка соответствия полученного приказа заявленным целям его создания, правильности оформления, а также вывод полученного приказа на печать;
- согласование нового приказа с ответственными в области защиты информации госархива должностными лицами;
- внесение изменений в проект документа, повторный вывод на печать (при необходимости);
- подписание документа директором госархива;
- доведение приказа до исполнителей [Дроздова. Как приказы помогают…, с. 83-90].

В соответствии с положениями Инструкции по делопроизводству ГБУТО ГАТО внесение изменений в подписанный приказ не допускается. При возникновении необходимости внести изменения в приказ, создается новый приказ – о внесении изменений в необходимый приказ. Приказы госархива оформляются на бланке приказа с использованием следующих реквизитов: дата документа и регистрационный номер документа, располагаемые на одном уровне, заголовок к тексту, текст, подпись. Дата и регистрационный номер приказа проставляются на основании занесения информации о приказе в Журнал регистрации приказов госархива по основной деятельности после подписания приказа директором [Номенклатура дел ГБУТО ГАТО…].

Заголовок к приказу печатается через 1 межстрочный интервал под реквизитами бланка слева от границы левого поля. Точка в конце заголовка не ставится. Заголовок к приказу формулируется с предлогом «О» («Об»), кратко и точно отражая содержание текста приказа, например:

О возложении обязанностей по подписанию электронной подписью служебных документов

Текст приказа отделяется 2-3 межстрочными интервалами от его заголовка и печатается шрифтом размером № 14 и выравнивается по ширине текстового поля. Первая строка абзаца начинается на расстоянии 1,25 см от левой границы текстового поля. Текст приказа состоит из двух частей: обоснования (преамбулы) и распорядительной части. В первой части текста документа кратко излагаются цели и задачи, факты и события, послужившие основанием для издания приказа. Она может начинаться словами «в целях», «во исполнение», «в соответствии» и др. Если приказ издается на основании другого документа, то в данной части указываются наименование вида этого документа, наименование органа, издавшего документ, дата, регистрационный номер и заголовок к тексту [Инструкция по делопроизводству ГБУТО ГАТО…]. Для приказов по защите информации здесь обычно указываются ссылки на нормативно-правовые акты, на основании положений которых осуществляется работа, например, Федеральный закон «О персональных данных». Преамбула в проектах приказов завершается словом «п р и к а з ы в а ю:», которое печатается строчными буквами вразрядку.

Распорядительная часть приказа по защите информации содержит:

- решения организационного характера (утвердить, признать утратившим силу и др.);
- конкретные поручения с указанием исполнителя (исполнителей) и сроков их выполнения [Инструкция по делопроизводству ГБУТО ГАТО].

Каждое решение или поручение оформляется в приказе отдельным пунктом. Пункты приказа располагаются в логико-временной последовательности и нумеруются арабскими цифрами. Действия однородного характера могут быть перечислены в одном пункте. В качестве исполнителей в приказах по защите информации может быть указан ответственный за это

направление отдел информационно-поисковых систем и защиты информации, но на практике чаще называются конкретные должностные лица, ответственные за то или иное направление работы по обеспечению защиты данных. Когда поручение дается подразделению, его наименование пишется полностью, в скобках указываются фамилия и инициалы начальника отдела в именительном падеже. Если поручение дается конкретному исполнителю, указывается его должность в дательном падеже, затем в скобках называется фамилия.

Предписываемое действие выражается глаголом в неопределенной форме. В приказах госархива по защите информации не употребляются неконкретные обобщённые выражения («усилить», «ускорить» и т.п.), а даются точные формулировки, например, «разработать инструкцию ответственного по обеспечению антивирусной защиты госархива», которые подкрепляются указанием конкретных сроков исполнения. Если одному исполнителю поручается несколько различных заданий с одинаковым сроком исполнения, в таком случае ответственный исполнитель и срок исполнения указываются один раз в основном пункте, а поручения выделяются в отдельные подпункты. Если у поручений сроки исполнения различаются, то они указываются не в основном пункте, а в каждом подпункте [Инструкция по делопроизводству ГБУТО ГАТО].

Срок исполнения, указанный в приказе, должен быть реальным, соответствовать объему предполагаемых работ, поэтому при составлении приказов с указанием сроков при необходимости их временные рамки заранее согласовываются с исполнителем. Срок исполнения в пунктах распорядительной части приказа не указывается в случаях, если действия носят регулярный характер и их выполнение предписывается на весь период действия приказа (например, в приказах о предоставлении права подписания электронной подписью служебных документов). Количество исполнителей по каждому пункту (подпункту) не ограничивается. Ответственный исполнитель указывается первым. Если приказ отменяет полностью или частично ранее изданные документы по тому же вопросу, то в предпоследнем пункте приказа перечисляются все утратившие силу приказы с указанием их наименований, дат,

номеров и заголовков.

Последний пункт приказа – пункт о контроле, в котором указываются должность лица, ответственного за исполнение документа в целом, его фамилия и инициалы. В отдельных случаях директор может оставить контроль за собой, например, в приказах, регламентирующих разработку положения о комиссии по защите информации в ограниченные сроки. Подразделения и должностные лица, до сведения которых необходимо довести приказ, перечисляются в отдельном листе или списке, который может оформляться на оборотной стороне последнего листа приказа. Визы (при их наличии) включают должности визирующих, личные подписи, расшифровки подписей и даты. Визы проставляются на обороте последнего листа приказа или на отдельном листе визирования. При наличии приложений в тексте приказа в соответствующих пунктах распорядительной части даются отсылки: ... (приложение № 1); ... (приложение № 2), либо приложения могут упоминаться в тексте («…согласно приложению 3»…). Издание вместе с приказом приложений, не упомянутых в тексте документа, не допускается. Все приказы подписывает директор [Инструкция по делопроизводству…].

Изданный приказ подлежит обязательной регистрации в Журнале регистрации приказов госархива по основной деятельности по порядку номеров в пределах календарного года, с присвоением индивидуального уникального регистрационного номера [Номенклатура дел ГБУТО ГАТО]. Приказы по защите информации относятся к числу приказов по основной деятельности, поэтому их регистрационный номер указывается без присваивания литеры.

Поскольку каждый из издаваемых документов по защите информации учреждения должен утверждаться приказом, целесообразно вести отдельный учёт всех издаваемых документов с указанием ответственных лиц для оперативного их изменения в случае возникновения необходимости, т.к. одной из отличительных черт приказов этого направления деятельности учреждения является конкретика, т.е. отсутствие «размытых» формулировок и указание должностей и фамилий. Но для тюменского госархива, организация защиты

информации для которого не является профильным видом деятельности, а «текучка» специалистов рассматриваемого направления достигает высоких значений, есть лазейка – для приказов, содержание которых предполагает возложение обязанностей, возможно указание должности с отсылкой на лист ознакомления, где уполномоченные лица указывают свои фамилию, имя и отчество, ставят подпись и дату ознакомления.

Ещё один вариант предусматривает включение соответствующих пунктов приказов (или приложений к ним) в трудовой договор или должностную инструкцию специалиста соответствующей должности, в этом случае при каждой смене сотрудника у учреждения будет документальное подтверждение того, что сотрудник был ознакомлен с возложенным на него функционалом. На данный момент в госархиве практикуется первый вариант, т.е. создание листов ознакомления. Помимо этого, при приёме на работу каждый новый сотрудник расписывается в листе ознакомления с локальными нормативными актами госархива, который помещается в личное дело сотрудника. Для тех должностей, в чей функционал входит исполнение тех или иных обязанностей в области защиты информации, в лист ознакомления будут включены соответствующие локальные акты, возлагающие на сотрудника эти обязанности и конкретизирующие порядок их выполнения.

2.3. ВНЕСЕНИЕ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ В ОРГАНИЗАЦИОННО-ПРАВОВОЙ ДОКУМЕНТ «ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГБУТО «ГОСУДАРСТВЕННЫЙ АРХИВ ТЮМЕНСКОЙ ОБЛАСТИ»»

Каждый оператор персональных данных, то есть каждая организация, в штате которой числится хотя бы один сотрудник, обязан издать документ, определяющий его политику в отношении обработки персональных данных. Соблюдение положений Политики должно обеспечить конфиденциальность и безопасность обрабатываемых персональных данных. Данное положение

подкреплено законодательно – согласно ч. 1 ст. 18 Федерального закона № 152 [О персональных данных…] организация обязана предоставить всем желающим неограниченный доступ к Политике. Это требование исполняется ГБУТО ГАТО путём размещения Политики в разделе «Нормативные документы» страницы «Государственный архив Тюменской области» портала Управления по делам архивов Тюменской области (http://archiv.72to.ru/index.php/gosudarstvennyj-arkhiv-tyumenskoj-oblasti).

Действующая Политика обработки персональных данных ГБУТО ГАТО была разработана в 2016 г., однако её содержание и название не соответствуют целям издания документа – в тексте смешаны требования к обработке персональных данных как пользователей, так и сотрудников, хотя основное назначение Политики – регламентация работы с персональными данными именно пользователей архива. Работа с персональными данными сотрудников регулируется Положением об обработке и защите персональных данных.

Наличие Политики предполагается статьёй 18 Закона 152, а Положения – статьями 68 и 87 Трудового кодекса РФ [Трудовой кодекс РФ…], статьёй 5.27 Кодекса об административных правонарушениях Российской Федерации [Кодекс об административных…]. При этом указанные акты только обязывают иметь этот документ в организации, но не предписывают, что должно быть в него включено. По сути принципиальной разницы между Политикой и Положением нет, структура документов предполагает рассмотрение аналогичных вопросов: должны быть указаны цели обработки данных, основания такой обработки, категории, принципы и условия обрабатываемых данных, права субъекта и обязанности оператора, сроки хранения персональных данных. Однако наличие Политики предполагается в случае обработки персональных данных на сайте, а Положение является внутренним документом организации [Дроздова. Как приказы помогают…, с. 83-90].

В утверждённую Политику обработки персональных данных ГБУТО ГАТО вошло 11 разделов:

1. Общие положения;

2. Категории субъектов персональных данных;
3. Цели обработки персональных данных;
4. Основание обработки персональных данных;
5. Категории обрабатываемых персональных данных;
6. Принципы обработки персональных данных;
7. Условия обработки и передачи персональных данных третьим лицам;
8. Права субъекта персональных данных;
9. Приём обращений субъектов персональных данных;
10. Срок хранения персональных данных работников учреждения;
11. Перечень терминов [Об обеспечении безопасности…].

В первом разделе «Общие положения» указаны правовые основания разработки Политики, основные сведения об операторе персональных данных, определяется цель обработки персональных данных, порядок предоставления неограниченного доступа к документу, случаях пересмотра Политики и внесения в неё изменений и дополнений.

Раздел «Категории субъектов персональных данных» представляет собой список из двух пунктов – это работники и пользователи архива. Третий раздел – «Цели обработки персональных данных» – также является списком причин, состоящем из двух пунктов. В разделе «Основание обработки персональных данных» перечислены действующий на момент разработки Политики законодательные и нормативные акты Российской Федерации по защите информации, а также изданные локальные акты госархива.

Далее в отдельном разделе перечислены категории обрабатываемых персональных данных: это паспортные и контактные данные, сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе, страховом свидетельстве обязательного пенсионного страхования, военном билете, пенсионном удостоверении, сведения об образовании, трудовой деятельности. В шестом разделе оговорено пять принципов обработки персональных данных.

В разделе 7 «Условия обработки и передачи персональных данных третьим лицам» оговорён перечень действий, осуществляемых с персональными данными, основания и порядок их обработки в облгосархиве. В следующем разделе оговорены права субъекта персональных данных, в том числе приведён перечень сведений, право получения от оператора которых законодательно закреплено за субъектом.

Раздел «Приём обращений субъектов персональных данных» состоит из одного предложения с указанием адреса, по которому осуществляется приём заявлений от субъектов персональных данных. Сроки и формы хранения персональных данных работников учреждения оговорены в десятом разделе с отсылкой на положения законодательных актов. Документ завершается разделом «Перечень терминов». Общий объём Политики составил 12 листов.

В настоящий момент в Политику обработки персональных данных ГБУТО ГАТО требуется внесение следующих изменений:

- обновление законодательной базы;
- в разделе «Общие положения» необходимо добавить адрес второго здания госархива, расположенного по ул. Воровского, либо изменить формулировку «Архив расположен по адресу» на «Обработка персональных данных пользователей осуществляется по адресу 625035, г. Тюмень, пр. Геологоразведчиков, д. 21»;
- категории субъектов персональных данных, обрабатываемых в госархиве, целесообразно исключить из раздела 2 и поместить в раздел 1;
- адрес, по которому осуществляется приём заявлений от субъектов персональных данных, также необходимо перенести в раздел «Общие положения»;
- перечень терминов необходимо поместить перед основным текстом документа, исключив из последнего 11 раздела;
- расширение описание целей, порядка и принципов обработки персональных данных пользователей;

- исключение из целей обработки персональных данных положений, описывающих обработку персональных данных сотрудников госархива с целью ведения бухгалтерского и кадрового учёта, т.к. эти вопросы регламентируются Положением об обработке персональных данных, а не Политикой;
- требуют актуализации категории и объёмы обрабатываемых персональных данных субъектов в соответствии с существующей практикой работы;
- разделы «Принципы обработки персональных данных» и «Условия обработки и передачи персональных данных третьим лицам» целесообразнее объединить в новый раздел «Порядок и принципы обработки персональных данных»;
- перенести из 10 раздела в вышеуказанный образованный раздел информацию о сроках хранения персональных данных;
- в рамках разделов «Права субъекта персональных данных» и «Приём обращений субъектов персональных данных» либо путём выделения нового раздела необходимо также рассмотреть порядок актуализации, исправления, удаления и уничтожения персональных данных, ответов на запросы субъектов на доступ к персональным данным.

К тексту действующей Политики обработки персональных данных в ГБУТО ГАТО требуется внесение следующих дополнений:

- необходимо конкретизировать сферу действия документа – Политика составляется в случае обработки персональных данных в открытых информационных системах, размещённых в сети Интернет;
- указание адреса, по которому осуществляется приём заявлений от субъектов персональных данных, необходимо дополнить указанием адреса официальной электронной почты госархива;
- добавление положений, касающихся конкретизации содержания и объёмов обрабатываемых персональных данных субъектов;

- указать возможные причины и условия передачи персональных данных пользователей;
- помимо прав субъектов персональных данных в текст документа должен быть внесён перечень обязанностей оператора, возникающий при осуществлении обработки персональных данных пользователей, определении порядка допуска сотрудников госархива к обработке персональных данных, порядка хранения персональных данных, порядок организации защиты таких сведений.

Изменённая версия Политики обработки персональных данных в ГБУТО ГАТО с внесёнными в неё дополнениями и изменениями, представлена в приложении 1 к тексту выпускной квалификационной работы. Курсивом в документе выделены моменты, которые были конкретизированы, либо ранее вообще не были предусмотрены. Часть положений из текста документа была исключена, что прослеживается только при сравнении прежней версии с новой редакцией Политики. Так из раздела 2 «Правовые основания обработки персональных данных» были исключены Трудовой кодекс РФ, Федеральный закон № 27 [Об индивидуальном (персонифицированном) учете…], Федеральный закон № 4023 [О бухгалтерском учете…], Приказ Управления по делам архивов Тюменской области № 18 [Об утверждении Положения…] и другие акты, касающиеся бухгалтерского и кадрового учета, относящегося к внутренней деятельности ГБУТО ГАТО. Из категорий обрабатываемых персональных данных по тому же принципу были убраны такие пункты, как паспортные данные, сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе, страховом свидетельстве обязательного пенсионного страхования, военном билете; пенсионном удостоверении и сведения о трудовой деятельности.

Что касается вопроса оформления Политики, то тут предъявляются стандартные требования, как и при оформлении иных организационно-правовых документов: на документе должны быть указаны наименование организации, наименование вида документа, гриф утверждения, после текста документа

должна стоять подпись лица или лиц, ответственных за разработку документа [Дроздова. Как приказы помогают…, с. 83-90]. В действующей Политике эти требования соблюдены. В случае внесения всех указанных изменений и дополнений обновлённая Политика подлежит согласованию и утверждению, предыдущий вариант Политики признаётся утратившим силу. На странице ГБУТО «Государственный архив Тюменской области» следует удалить старую редакцию документа и разместить скан-копию новой утверждённой Политики обработки персональных данных в ГБУТО ГАТО.

Проект дополнений и изменений в документ «Политика обработки персональных данных в ГБУТО «Государственный архив Тюменской области»» содержится в приложении 1 к настоящей диссертации. Курсивом в тексте документа выделены положения, изменённые (дополненные, уточнённые, исправленные) в процессе проектирования, а также положения, ранее Политику не включённые, но которые должны быть в ней отражены. Такие изменения, как смена формулировки или изменения последовательности слов в проекте документа не учитывались.

ГЛАВА 3. ПРОЕКТИРОВАНИЕ ОРГАНИЗАЦИОННО-ПРАВОВЫХ ДОКУМЕНТОВ С ЦЕЛЬЮ СОВЕРШЕНСТВОВАНИЯ ПОРЯДКА ЗАЩИТЫ ИНФОРМАЦИИ В ГБУТО «ГОСУДАРСТВЕННЫЙ АРХИВ ТЮМЕНСКОЙ ОБЛАСТИ»

Определить типовые направления в области защиты данных учреждения можно исходя из текста приказа Федеральной службы по техническому и экспортному контролю Российской Федерации № 21, положения которого применимы не только к работе с персональными данными, о чём можно сделать вывод исходя из названия документа [Об утверждении состава…]. То есть к направлениям деятельности организаций в сфере защиты информации относятся: вопросы разграничения доступа к системам, защита машинных носителей информации, антивирусная защита, защита технических средств, управление конфигурацией информационных систем, распределение обязанностей и ответственности между должностными лицами, порядок работы с электронной почтой, система генерации паролей и др. Отсутствие чёткой регламентации этих направлений в отечественном законодательстве позволяет организациям самостоятельно определять, какие процессы нужно отражать в локальной документации.

Этапы работы над внедрением в работу госархива нового документа в области обеспечения защиты сведений ограниченного доступа состоят из следующих пунктов:

- подготовка проекта документа;
- составление заключения на проект документа;
- согласование проекта документа с комиссией госархива по защите информации;
- внесение правок и повторное согласование (при необходимости);
- подписание;
- регистрация и утверждение документа;
- внедрение документа в делопроизводственную практику.

Создание проектов документов для ГБУТО ГАТО, то есть методика проектирования, состоит из пяти одинаковых этапов деятельности, которые проводились раздельно при подготовке каждого из проектируемых документов – для Частной модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» в ГБУТО «Государственный архив Тюменской области», Инструкций ГБУТО ГАТО по организации антивирусной и парольной защиты, работе со съёмными носителями информации.

Работа производилась на трёх площадках: непосредственно в Государственном архиве Тюменской области, в информационно-библиотечном центре Тюменского государственного университета и за личным персональным компьютером по адресу проживания автора работы. Выбор мест обуславливается разделением информации, необходимой для изучения, на две категории: в первую входит так, которую можно получить дистанционно, а ко второй относятся сведения, которые требуют изучения сложившейся практики и уточнения сведений у соответствующих специалистов учреждения, что обуславливаем использование и методов *опроса* и *интервьюирования*.

Первый из этапов научного исследования представляет собой **предпроектное обследование** – на данной стадии осуществлялся сбор материалов и информации по теме исследования: для проектируемых документов для госархива был произведён поиск и анализ законодательной базы, регламентирующей выполнение таких действий в российских органах и учреждениях, как проведение антивирусной и парольной защиты, обеспечение безопасности при работе со съёмными носителями данных.

В рамках предпроектного обследования было проведено интервьюирование сотрудников госархива (заместителя директора, системного администратора, главного бухгалтера, ведущего документоведа) и изучение сложившихся традиций и особенностей организации работы с персональными данными в информационной системе персональных данных «Бухгалтерия», правил осуществления антивирусной и парольной защиты данных и порядка

работы со съёмными носителями. Основной задачей на этом этапе исследования являлось формирование представления об этапах проведения рассматриваемых видов работ в Тюменском облгосархиве, а также определение полноты и качества существующей документальной регламентации процесса.

На данной стадии был применён ряд методик, служащих для проведения изучения и исследования предметной области. Например, были использованы методы *наблюдения* и *опроса*, которые позволяют собрать необходимый материал, обобщить его и выделить основные смысловые единицы для отражения их в проектируемых документах. Разделению информации на отдельные логически связанные части способствовало и применение методов *классификации* и *аналогии*. Поскольку сбор и обработка информации в рамках определения основ законодательного и нормативного правового закрепления изучаемых процедур были произведены без привязки к конкретной территории Российской Федерации, то нельзя не упомянуть и методы *абстрагирования* и *дедукции*, т.е. процесс формирования логических выводов исходя из изучения общих положений и применения их к частной практике – организации рассматриваемых направлений работы в ГБУТО ГАТО.

Следующим шагом научного исследования является **проведение анализа результатов предпроектного обследования**. На данном этапе осуществляется интерпретация массива собранных данных, происходит их обобщение и/или разделение в соответствии с тематической принадлежностью к определённым частям проектируемых документов, а также актуальностью и важностью для исследуемой темы – по каждому из проектируемых документов. На этом этапе использовался метод *формализации*, заключающийся в представлении полученных сведений в символьно-знаковом выражении. Например, это перенос используемых в работе частей интервью с сотрудниками госархива из аудиоформата в печатный вид. Метод *сравнения* был актуален при изучении опыта разработки аналогичных документов (Частной модели угроз, инструкций по антивирусной и парольной защите, инструкции по работе со съёмными носителями информации). Задачей проведения указанных мероприятий стало

определение порядка проведения такой деятельности, обобщения сведений различных информационных ресурсов, *обобщение* и подготовка материалов к проведению следующей стадии исследования.

Третий этап методики исследования представляет собой **проектирование документов** и состоит из таких процедур, как составление и оформление документов, их согласование и утверждение. Проектирование представляет собой процесс, в рамках которого определяется структура документа, конкретизируется смысловое содержание каждой его текстовой части. Результатом проектирования является готовый для введения в действие в госархиве документ.

Инструкции ГБУТО ГАТО по организации антивирусной и парольной защиты, работе со съёмными носителями информации являются документами, информация в которых представляется особым структурированным способом – исходя из основных этапов работы в каждой из рассматриваемых областей, что помогают определить результаты интервью с сотрудниками облгосархива, проведённого в рамках предпроектрого исследования.

Исходя из назначения для каждого проекта документа определяется используемая терминология, определяется стиль написания, объём текста. Структура методических документов, к которым относятся и разрабатываемые в рамках написания настоящей диссертации проекты, традиционно состоит из следующих элементов: титульный лист; пояснительная записка; содержание; текст; список рекомендуемой в рамках данной тематики литературы; приложения [Разработка нормативных документов…].

Дадим характеристику каждому из них. Титульный лист должен включать такие элементы, как наименование организации (в нашем случае – Государственное бюджетное учреждение Тюменской области «Государственный архив Тюменской области»), указание структурного подразделения, разработавшего документ (отдел информационно-поисковых систем и защиты информации, т.к. разработка документов в области защиты информации относится к прямым обязанностям администратора

информационной безопасности вычислительной сети, относящегося в структуре госархива именно к этому отделу). Дальше идёт наименование вида документа, указание места и года разработки.

Содержание проектов документов включает наименование всех элементов текста, а также номера страниц, к которым относится начало каждого отдельного элемента структуры разрабатываемого документа. В соответствии со спецификой изложения сведений в проектируемых инструкциях информация будет разбивается на части и рубрицироваться в соответствии с принятом порядком проведения работ. Подробное описание структуры Частной модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» в ГБУТО «Государственный архив Тюменской области» содержится в пункте 3.1 настоящей диссертации, а в пункте 3.2 – для Инструкций ГБУТО ГАТО по организации антивирусной и парольной защиты, работе со съёмными носителями информации.

Приложения к разрабатываемым инструкциям могут включать материалы, которые играют немаловажную роль при организации и проведении рассматриваемых видов работ, в настоящем случае – это журнальные формы. Для Частной модели угроз наличие приложений не предусмотрено. Каждое приложение у инструкций начинается с новой страницы, а в верхнем правом углу проставляется слово «Приложение» и его порядковый номер, затем указывается название приложения без знаков препинания в конце [Инструкция по делопроизводству…]. Например:

Приложение 3 Проект Инструкции по организации антивирусной защиты в Государственном бюджетном учреждении Тюменской области «Государственный архив Тюменской области»

Последним этапом процедуры проектирования является оформление проектов разрабатываемых документов, которое включает форматирование текстовой составляющей проектов на основе собранных данных, а также работу

по выполнению предъявляемых технических требований – расстановке размеров полей, абзацных отступов, межстрочного интервала и др. Необходимо определить и технические требования, применяемые к оформлению документов. Их текст печатается на листе формата А4 белого цвета с выбором книжной ориентации страниц. Используются следующие поля документа: верхнее и нижнее – 20 мм, левое – 30 мм, правое – 10 мм. Текст печатается на компьютере через полтора межстрочных интервала с применением 14 кегля шрифта Times New Roman, выравнивается по ширине. Абзацный отступ первой строки составляет 1,25 см и применяется ко всему тексту разрабатываемых документов [Инструкция по делопроизводству…].

Приложения выполняются тем же шрифтом и межстрочным интервалом, но в случае необходимости помещения текста на один лист могут печататься 12 кеглем через один межстрочный интервал. Нумерация страниц осуществляется арабскими цифрами без использования каких-либо дополнительных знаков или символов 12 кеглем шрифта Times New Roman. Для основного текста и приложений используется сквозная нумерация, однако номер на титульном листе и содержании не проставляются, хотя оба документа учитываются в общем объёме. Сноски печатаются 10 кеглем шрифта Times New Roman.

Разделы текста Частной модели угроз и инструкций нумеруются арабскими цифрами в порядковой последовательности с применением абзацного отступа. Пункты нумеруются в пределах раздела, включая его номер, разделяются точкой – например, «1.1.» или «5.3.». Заголовки разделов нумеруются и в отличие от названий подразделов печатаются прописными буквами и в содержании, и в основном тексте. Точка в конце названия раздела или подраздела не ставится. Названия подразделов отделяются от наименования главы и основного текста 1 межстрочным интервалом [Памятка по подготовке…].

Основные разделы текста начинаются с новой страницы. Перенос слов не применяется. Сам заголовок формулируется кратко, информационно ёмко – не более чем в одно предложение. Проекты документов оформляются в соответствии с ГОСТ Р 6.30-2003 «Унифицированные системы документации.

Унифицированная система организационно-распорядительной документации. Требования к оформлению документов».

Все разрабатываемые в рамках настоящей диссертации документы включены в приложения и оформляются каждый с новой страницы с применением всех необходимых реквизитов. В правом верхнем углу проектируемого документа располагается слово «ПРОЕКТ», напечатанное прописными буквами. Все графические элементы, включённые в текст проектов, имеют одинаковое оформление в соответствии с Памяткой по подготовке методических пособий сотрудниками ГУТО ГАТО. Ссылки в списке литературы оформляются в соответствии со стандартом на оформление библиографических ссылок [ГОСТ Р 7.05-2008…].

Последним этапом работы над проектами документов для ГБУТО ГАТО будет являться их передача комиссии госархива по защите информации для согласования, что оформляется протоколом заседания этого органа. При необходимости на этом этапе присутствует стадия внесения изменений, повторного оформления и согласования проекта документа. Документы вступают в силу с момента утверждения, то есть становятся полноценными обладающими юридической силой актами после подписания соответствующим должностным лицом – директором Тюменского облгосархива. Завершающим этапом работы станет доведение документов до сведения лиц, работу которых они регламентируют, – путём осуществления тиражирования подписанных документов, их передача всем заинтересованным лицам.

3.1. РАЗРАБОТКА ПРОЕКТА ДОКУМЕНТА «ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ «БУХГАЛТЕРИЯ» В ГБУТО «ГОСУДАРСТВЕННЫЙ АРХИВ ТЮМЕНСКОЙ ОБЛАСТИ»»

В инфраструктуре госархива выделяются две информационные системы персональных данных – это ИСПДн «Директум» и ИСПДн «Бухгалтерия». Для

системы «Директум» в 2014 г. по договору на оказание услуг с госархивом ООО «Коминтек» было проведено обследование на предмет соответствия требованиям соблюдения безопасности данных персонального характера при их обработке в системе (в т.ч. проанализирован состав технических и программных средств, применяемых в архивном учреждении, организационно-распорядительной документации ГБУТО ГАТО на предмет соответствия установленным законодательством требованиям к гарантии безопасности сведений, составляющих персональные данные [Об утверждении требований…].

В результате проведённых в Государственном бюджетном учреждении Тюменской области «Государственный архив Тюменской области» работ специалистами ООО «Коминтек» был разработан и передан Тюменскому облгосархиву Аттестат соответствия требованиям безопасности информации при её обработке в информационной системе персональных данных «Директум» ГБУТО ГАТО № 002/14, все сопровождающие обследование документы, а также разработанная Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Директум» ГБУТО ГАТО.

Для второй ИСПДн госархива – «Бухгалтерия» – проводились аттестационные испытания. В рамках заключенного договора об оказании услуг ООО «КБ-Информ» по итогам проведения испытаний в 2016 г. были сформированы и переданы в госархив только следующие документы:

- *протокол* аттестационных испытаний информационной системы персональных данных «Бухгалтерия»;
- *программа-методика* аттестационных испытаний информационной системы персональных данных «Бухгалтерия»;
- *технический паспорт* информационной системы персональных данных «Бухгалтерия»;
- *заключение* по результатам аттестационных испытаний информационной системы персональных данных «Бухгалтерия»;

– *аттестат соответствия* информационной системы персональных данных «Бухгалтерия» требованиям по обеспечению безопасности персональных данных.

Обязательный характер разработки Частной модели угроз регламентирован положениями закона «О персональных данных…». В названном законе указано, что «обеспечение безопасности персональных данных достигается определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Указанное положение подкрепляется и иными актами, в т.ч. рядом приказов ФСТЭК, Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных и Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных Указанные акты указывают на то, что формирование необходимых к соблюдению требований к защите данных должно базироваться на определении угроз безопасности. Это значит, что для любых информационных систем персональных данных, которые подлежат защите, в соответствии с законодательством необходимо разработать модель угроз. При этом в правовых актах нет прямого указания на то, кто должен заниматься такой разработкой, что позволяет организациям привлекать к выполнению данного вида работ сторонние учреждения, что и было сделано при оценке информационной системы персональных данных «Директум».

Для ИСПДн «Бухгалтерия» частная модель угроз будет разрабатываться самостоятельно ответственными должностными лицами за защиту информации госархива. Из всех вышеперечисленных актов именно последний будет являться основой для разработки собственного документа путём внесения в него изменений и дополнений в соответствии со спецификой деятельности архивного учреждения и существующей практикой работы. Важность документа обусловлена тем, что на его основе формируются требования к защите информации, исходя из которых создается система защиты данных Тюменского облгосархива. Именно в Частной модели угроз безопасности персональных

данных при их обработке в информационной системе персональных данных «Бухгалтерия» определяются организационные меры, соблюдение которых позволяет избежать или минимизировать урон от реализации различных угроз.

Модель угроз облегчает решение следующих задач:

- определение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия»;
- определение требуемого уровня защищенности информации;
- анализ защищенности от угроз безопасности на момент составления Модели угроз;
- разработка и применение на практике таких принципов защиты данных, которые бы обеспечивали невосприимчивость ИСПДн к угрозам при использовании определённых организационных и технических мер;
- предотвращение фактов несанкционированного доступа к сведениям ограниченного доступа и/или передачи её третьим лицам, не имеющим права доступа к такой информации, путём проведения специальных мероприятий;
- организация защиты технических средств, при которой будет отсутствовать или максимально минимизирована возможность воздействия или нарушения их функционирования [Методика определения…].

Целесообразно изначально продумать и прописать в документе все возможные вопросы, касающиеся защиты данных, содержащихся в информационной системе учреждения, так как Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» документ хоть и подлежащий изменениям, но при этом относительно статичный – без существенных инфраструктурных изменений в системе переутверждению обычно не подлежит.

Содержание модели угроз продиктовано приказом ФСТЭК № 17: «Модель угроз безопасности информации должна содержать описание информационной

системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации» [Об утверждении требований…].

Что же касается порядка оформления модели угроз, по аналогии с оформлением других методических разработок, к документу обязательно составляется титульный лист, список сокращений и перечень используемых в документе терминов [Памятка по подготовке…]. Первым составляется раздел «Общие положения», где даётся обоснование, в какой организации и для каких целей и систем создаётся модель угроз, перечисляются актуальные нормативно-методические документы, положения которых посвящены вопросам защиты информации, то есть прямо или косвенно являются основанием составления модели угроз. Здесь же указывается, какие виды информации ограниченного доступа госархива подлежит защите и в какой информационной системе они содержатся.

После определения основных направлений защиты указываются основные сведения об информационной системе – её месторасположение, название, характеристика обрабатываемых данных и общее описание самой системы (подробное описание информационной системы персональных данных «Бухгалтерия» содержится в разделе 4.1 разработанной Модели угроз). Указанная информация должна позволять составить общее представление о защищаемой системе и том, как она функционирует. Далее идёт описание применяемых способов охраны помещений, в которых находится подлежащая защите информационная система, в том числе организации охранного контроля, видеонаблюдения, наличия сигнализации и т.п. Завершается первый раздел уточняющими положениями – в каких случаях документ может изменяться или пересматриваться.

Далее идут разделы «Классификация угроз безопасности» и «Характеристика угроз безопасности персональных данных, обрабатываемых в информационной системе персональных данных «Бухгалтерия» (рассматриваются по основным способам реализации – угрозы утечки информации по техническим каналам и угрозы несанкционированного доступа) [Бондарь, с. 8]. Текст указанных разделов является обобщённым теоретическим материалом, позволяющим на его основе осуществить анализ и расчёты актуальных для госархива угроз в целях дальнейшей корректировки и контроля проводимых действий по защите информации.

Описаниям возможных уязвимостей системы в модели угроз госархива отводится третий раздел – «Общая характеристика уязвимостей информационной системы персональных данных «Бухгалтерия». Поскольку называть в модели угроз конкретные уязвимости с указанием идентификатора CVE (база данных общеизвестных уязвимостей информационной безопасности) [Пинус, Безарова, Хозяинова, с. 32] и рейтинга CVSS (сравнение уязвимостей программного обеспечения с точки зрения их опасности) [Банк данных угроз…] нецелесообразно ввиду динамичности (изменчивости) как самой системы, так и возможных угроз безопасности, в текст документа включена градация возможных классов уязвимостей для информационной системы на основе положений стандарта «Классификация уязвимостей информационных систем» [ГОСТ Р 56546-2015…].

После определения возможных угроз расположены тематические разделы, информация которых посвящена подробному описанию конкретной информационной системы персональных данных госархива – «Бухгалтерия», в целях обеспечения защиты данных которой и разрабатывается модель угроз. Так в первом подразделе четвёртого раздела даётся обобщённая характеристика самой информационной системы персональных данных «Бухгалтерия», в том числе перечисляются средства защиты информации, которые входят в неё, а также указываются должностные лица ГБУТО ГАТО, имеющие доступ к

информационной системе персональных данных «Бухгалтерия» в связи с выполнением должностных обязанностей.

Во втором подпункте определяется уровень исходной защищённости ИСПДн «Бухгалтерия» даётся характеристика актуальной угрозы, описание последовательности определения её оценки и сами расчёты в табличной форме. В следующем подпункте осуществляется определение вероятности реализации угроз в информационной системе персональных данных «Бухгалтерия»: указываются существующие категории информационных систем, даётся характеристика этой информационной системы ГБУТО ГАТО, проводятся расчеты уровня защищённости и исходя из результатов определяются требования к защите системы на основе положений законодательства. Вероятность возникновения угроз, оценка такой вероятности и расчёты вероятности представлены в табличной форме. При составлении этого раздела используется Банк данных угроз безопасности информации ФСТЭК России, который представляет собой перечень описаний характеристик нарушителей с различными уровнями потенциала.

Поскольку законодательно какие-либо методики работы с Банком данных угроз не регламентированы, выборка актуальных для госархива угроз происходит «экспертным» путём – то есть ответственный за разработку Модели угроз сотрудник осуществляет самостоятельную выборку посредством просмотра существующих и внесённых в Банк данных угроз и определяет возможность их применения на информационную систему госархива. Завершается четвёртый раздел пунктом «Оценка опасности угроз информационной системы персональных данных «Бухгалтерия», в котором приведены характеристики актуальных для этой информационной системы госархива угроз с делением на виды, а также определяется возможный ущерб от реализации угроз для госархива, виды такого ущерба и степень его возмещения: опасность угроз может являться низкой, иметь средний или высокий уровень, в зависимости от того последствия наступают при реализации угрозы (незначительные негативные, просто негативные или же значительные

негативные соответственно). При этом в отечественных нормативных и методических документах нет конкретизации, должна ли опасность угроз определяться единожды и быть постоянной для всех возникающих угроз. В следствие этого при разработке Модели угроз в зависимости от нарушения конфиденциальности, целостности или доступности при реализации конкретной угрозы определяется и опасность угроз.

Далее пятом разделе Модели угроз включается описание угроз, актуальных для информационной системы, которая заполняется на основании данных из Банка данных угроз безопасности информации ФСТЭК России. Этот раздел полностью представлен в табличной форме, которая состоит из следующих столбцов:

- номер по порядку;
- название угрозы безопасности персональных данных;
- уровень возможности реализации названной угрозы;
- показатель опасности угрозы;
- показатель актуальности угрозы.

В последнем разделе документа рассматриваются «Используемые средства защиты данных персонального характера при их обработке в ИСПДн «Бухгалтерия», где перечислены предпринимаемые госархивом меры по противодействию угрозе (как технические, так и организационные). Завершается Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» заключительными положениями, где указывается, что построенная Модель угроз применима к существующему состоянию информационной системы персональных данных «Бухгалтерия» при условии соблюдения основных (базовых) исходных данных:

- технические средства находятся в пределах контролируемой зоны;

- информационная система не подключалась к новым сетям частного и общего пользования (по сравнению с состоянием на момент проведения оценки и разработки Модели угроз;
- гарантируется отсутствие возможности неконтролируемого пребывания сторонних лиц (посетителей, иных сотрудников) в служебных помещениях госархива, где осуществляется работа в информационной системе персональных данных «Бухгалтерия» [Кобышева, Федотов, Кобышев, с. 79].

По итогам разработки Модели угроз на проект документа составляется заключение, в котором обосновываются причины разработки, особенности составления и иные аспекты, касающиеся уточнения порядка работы с Частной моделью угроз безопасности персональных данных при их обработке в ИСПДн «Бухгалтерия». Заключение и проект документа направляются на согласование комиссии госархива по защите информации. После доработки документа и устранения полученных замечаний он предоставляется на утверждение директору госархива, после чего подлежит внедрению в работу. В случае несоблюдения и/или изменения названных условий Модель угроз подлежит пересмотру.

Проект документа «Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» в ГБУТО «Государственный архив Тюменской области» включён в приложение 2 к тексту выпускной квалификационной работы.

3.2. ПОДГОТОВКА КОМПЛЕКСА ИНСТРУКТИВНЫХ МАТЕРИАЛОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ГОСАРХИВЕ

Одним из самых распространённых направлений деятельности любого учреждения в области защиты информации является организация и проведение антивирусной защиты персональных компьютеров и серверов учреждения.

Порядок решения этого вопроса решается сугубо индивидуально для каждой организации: ряд учреждений предпочитает не расходовать средства и покупать системы защиты только для конкретных рабочих мест, определяемых как наиболее значимые в инфраструктуре учреждения (руководители, бухгалтерия, службы охраны и др.), другие пользуются «свободным», т.е. бесплатным софтом, третьи устанавливают антивирусные программы на все имеющиеся в учреждении компьютеры. В каждом случае соблюдается какая-то установленная для конкретной организации цепочка действий, которые осуществляют уполномоченные на проведение этой работы сотрудники. Наличие инструкций по различным направлениям одного вида деятельности позволяет эффективно организовать деятельность в этой области, конкретизировать функции по каждому виду действий для исполнителей и ответственных лиц, исключить дублетность и излишние трудозатраты на исполнение работ сотрудниками, облегчить процесс обучения новых сотрудников.

Общие требования, применяемые к антивирусному программному обеспечению и принципам его использования, значатся в следующих документах:

- Приказ ФСТЭК № 28 [Требования к средствам …];
- Информационное сообщение ФСТЭК России «Об утверждении требований к средствам антивирусной защиты»;
- Приказ ФСТЭК № 21 [Состав и содержание …];
- Приказ Минкомсвязи № 104 [Об утверждении требований…];
- Приказ Россвязькомнадзора № 104 [Об утверждении требований…].

Однако указанные акты затрагивают техническую сторону процесса антивирусной защиты, организационные моменты упоминаются вскользь в единичных случаях и не несут в себе положений, регламентирующих отдельные этапы организации и проведения работ по этому направлению защиты информации. Вследствие этого можно говорить о том, что при создании инструкций по защите информации, в том числе по антивирусной защите, следует руководствоваться теми же требованиями, что предъявляются к

разработке иных локальных актов.

Инструкция разрабатывается в случае, если имеется участок работы (узкое направление какого-то вида деятельности), нуждающийся в нормативном закреплении порядка его осуществления, либо требуется внесение значительного количества дополнений или изменений в ранее принятый локальный нормативный акт. Наличие инструкций по различным направлениям одного вида деятельности госархива (в настоящем случае – защиты информации) позволяет эффективно организовать деятельность в этой области, конкретизировать функции для исполнителей и ответственных лиц, исключить дублетность и излишние трудозатраты на исполнение работ сотрудниками, облегчить процесс обучения новых сотрудников. В зависимости от срока действия инструкции могут быть:

- постоянно действующими, т.е. без ограничения срока их применения;
- временными, т.е. действующими в течение указанного в них срока или до наступления определенного события [Дроздова. Инструкция по антивирусной защите…, с.46-48].

Инструкции, разрабатываемые для ГБУТО ГАТО (по антивирусной и парольной защите, работе со съёмными носителями информации), будут являться постоянно действующими, т.к. издаются в целях установления правил, регулирующих направления деятельности госархива по защите информации, работа по которым осуществляется на регулярной основе без каких-либо существенных изменений в порядке и принципах работы. При этом положения разработанных инструкций будут распространяться не только на работу с персональными данными, как было ранее, а для каждого из названных направлений в целом: т.е. антивирусную защиту всех персональных компьютеров, серверов и съёмных носителей информации госархива, выданных в служебное пользование, любая информация на которых приравнивается к служебной информации и подлежит ограничению доступа к ней третьих лиц.

Порядок разработки инструкций включает в себя следующие типовые этапы:

- инициирование издания инструкции – определение причин, побуждающих к созданию нового документа. В рассматриваемом случае это несоответствие положений утверждённых документов существующей в настоящее время практике работы;
- сбор необходимой информации для включения в текст документа с учётом актуальной законодательной и нормативной базы, а также действующей практики работы госархива;
- подготовка проекта документа – создание инструкции в электронном виде с размещением на нём всех необходимых реквизитов, проверка соответствия полученного документа заявленным целям его создания, проверка правильности оформления, а также вывод Инструкции на печать;
- согласование проекта Инструкции с ответственными в области защиты информации организации лицами;
- при необходимости – внесение изменения в проект документа, повторный вывод на печать;
- подписание документа у руководителя организации;
- доведение инструкции до исполнителей (возможно применение листа ознакомления с документом) [Дроздова. Инструкция по антивирусной защите…, с.46-48].

Так как разрабатываемые инструкции являются самостоятельными методическими документами, к ним оформляются титульные листы. Для оперативного поиска информации составляется оглавление [Памятка по подготовке…]. Начинает каждый документ раздел «Общие положения». В нём приводятся правовые основания разработки инструкции, указывается цель проектирования и утверждения документа, определяется область его распространения. Заключительным пунктом рассматриваемого раздела будет являться положение, разъясняющее при возникновении каких обстоятельств

возможно осуществить пересоставление инструкции.

Основной текст инструкций был разделён на главы, каждая из которых состоит из нескольких пунктов, разбитых в свою очередь на подпункты. Предшествовать ему в случае необходимости их выделения в отдельные элементы структуры документа могут такие разделы как «Термины и определения» и «Сокращения». Текст каждой из проектируемых в рамках написания диссертации инструкций излагается от третьего лица единственного или множественного числа. В тексте используются слова в повелительном наклонении: «обязан», «следует», «не допускается» и др. [Быкова, с. 6]. Констатирующую часть инструкции составляет раздел «Общие положения», в нём перечисляются основания разработки, назначение разрабатываемого документа и сфера его распространения, ответственность за нарушение установленных правил и технологий. Каждая глава каждой инструкции имеет самостоятельное название. Главы, пункты и подпункты нумеруются арабскими цифрами [Делопроизводство. Образцы, документы…]. Типовые разделы для каждой инструкции определяются исходя из основных этапов работы.

В первом разделе («Общие положения») проекта *Инструкции по организации антивирусной защиты в ГБУТО ГАТО* указываются цель и правовые основания разработки документа, возлагается ответственность за осуществление отдельных направлений работы по антивирусной защите госархива на конкретных должностных лиц. Далее закрепляется требование о регулярности проведения периодического антивирусного контроля. В пункте 1.4 проекта указано, что действие Инструкции будет распространяться на всех сотрудников архива, а в пункте 1.8 – что доведение положений Инструкции до сотрудников архива будет осуществляться под подпись в Листе ознакомления с локальными актами госархива, являющимися частью личных дел сотрудников. Ознакомление должно осуществляться при приёме на работу сотрудниками, ответственными за организацию антивирусной защиты в ГБУТО ГАТО.

В разделе 2 ставятся задачи обеспечения антивирусной защиты в госархиве, перечисляются меры, которые направлены на её соблюдение. В

рассматриваемом разделе уделяется внимание также определению порядка установки дат и сроков проведения антивирусных проверок в госархиве, причины проведения служебных расследований (по фактам появления и проникновения вредоносных программ, повлекших неустойчивую работу и (или) вывод из строя оборудования, локально-вычислительной сети и информационных массивов архива). Завершает первый раздел Инструкции пункт о возможности пересмотра документа.

Раздел 3 «Требования, предъявляемые к антивирусному программному обеспечению госархива» устанавливает, в каких случаях допускается применение лицензионного и нелицензионного антивирусного программного обеспечения. После этого перечисляются требования к средствам антивирусного контроля – порядок обновления баз, наличие документации, необходимой для установки и эксплуатации антивирусного программного обеспечения, на русском языке, соответствие системным требованиям, характеристикам и комплектации персональных компьютеров и серверов госархива и др.

В четвёртом разделе проекта документа («Порядок осуществления антивирусного контроля») указывается, какого рода информация подлежит антивирусной проверке, а также описываются этапы проведения такой проверки. В отдельный (пятый) раздел выделено определение вредоносной программы, признаки заражения такой программой офисного оборудования.

В разделе «Мероприятия по уничтожению вредоносных программ» описано, в каких случаях работники госархива обязаны самостоятельно обратиться к ответственным должностным лицам ГБУТО ГАТО за организацию антивирусной защиты – например, в случае обнаружения нетипичной работы программ, появления различного рода графических и звуковых эффектов, искажений данных, пропадания папок или отдельных файлов, возникновение сообщений о системных сбоях и ошибках и т.п. Мероприятия по штатному управлению средствами антивирусного контроля в рамках проведения мероприятий по уничтожению вредоносных программ также рассматриваются в шестом разделе текста проекта Инструкции по организации антивирусной

защиты в ГБУТО ГАТО. Здесь регламентирован порядок действий, предпринимаемым в целях уничтожения вредоносных программ ответственным за организацию антивирусной защиты в архиве. Он предусматривает отражение таких событий, как обновление антивирусных баз объектов антивирусной защиты Тюменского облгосархива, проверка их состояния, приводит порядок работы с подвергнутыми вирусным атакам рабочими местами, принятие конкретного перечня мер по предотвращению распространения заражения вредоносными программами, либо ликвидации его последствий и др.

Отдельным элементом текста проектируемого документа выделены положения, касающиеся обязанностей и ответственности лиц, ответственных за организацию антивирусной защиты в архиве: системного администратора и администратора информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации. В числе обязанностей ответственных сотрудников числится пункт «ведение Журнала учёта проведения в Государственном бюджетном учреждении Тюменской области «Государственный архив Тюменской области» антивирусных проверок». Указанный Журнал представляет собой таблицу, состоящую из следующих столбцов:

1. № п/п;
2. дата проведения проверки;
3. отдел;
4. имя компьютера;
5. наименование антивирусной программы;
6. результаты проверки:
   - количество проверенных файлов:
   - количество и наименования инфицированных файлов, источник поступления (при наличии).
7. примечания (принятые меры);
8. исполнитель.

Форма Журнала приведена в приложении 1 к Инструкции по организации антивирусной защиты в ГБУТО ГАТО. Также в последнем разделе Инструкции рассматривается основания и порядок составления ежегодных отчётов о состоянии антивирусной защиты в госархиве и проведению служебных расследований, в т.ч. по фактам обнаружения вредоносных программ, повлекших неустойчивую работу и (или) возникновение ущерба.

Что касается проекта *Инструкции по работе со съёмными носителями информации в ГБУТО ГАТО,* то разделы тут также определяются исходя из этапов работы: регламентируется порядок учёта, выдачи, использования съёмных носителей информации. Из трёх разрабатываемых для госархива в рамках написания настоящей диссертации инструкций данный документ является наиболее структурированным, т.к. представляет из себя описание последовательности действий и не предполагает вариативности таких действий.

В разделе «Общие положения», как и в проекте Инструкции по организации антивирусной защиты в ГБУТО ГАТО, содержатся отсылки на правовые акты Российской Федерации, послужившие основанием для разработки документа. Далее указана сфера распространения действия документа и конкретизация видов съёмных носителей информации с указанием целей их применения. Завершает первый раздел и этого проекта пункт о возможности пересмотра документа.

Во втором разделе рассмотрены цели и условия использования съёмных носителей информации: поясняется, что подразумевается под их использованием, указываются требования, соблюдение которых разрешает использовать носители в информационной системе госархива. В том числе, указано, что допускается применение в работе только учтённых носителей данных, которые должны являться собственностью архива и быть подвергнуты регулярной ревизии и контролю, а также прошедшим антивирусный контроль носителями информации иных организаций, чьё применение необходимо для реализации функций архива.

Порядок учёта и выдачи съёмных носителей информации в госархиве определяется в третьем разделе проекта Инструкции. Положения, регламентированные пунктом 3.4., подразумевают ведение Журнала учёта съёмных носителей информации, форма которого представлена в приложении 1 к Инструкции. Указанный Журнал является таблицей, состоящей из одиннадцати столбцов:

1. № п/п;
2. учётный номер носителя;
3. вид и описание носителя;
4. кому произведена выдача;
5. дата выдачи;
6. подпись получателя;
7. дата возврата носителя
8. подпись сдатчика;
9. подпись получателя;
10. № и дата уничтожения информации, содержащейся на носителе (полное форматирование);
11. примечания.

Также в третьем разделе проекта рассматриваются такие вопросы, как определение ответственного за учёт и выдачу съёмных носителей информации в госархиве, условия хранения носителей у сотрудников ГБУТО ГАТО, возврата носителей после завершения работы с ними. Подробно порядок использования съёмных носителей информации регламентирован положениями четвёртого раздела проекта Инструкции по работе со съёмными носителями информации в ГБУТО ГАТО. Здесь перечислено, какие действия запрещается осуществлять при использовании в работе съёмных носителей информации, а также обосновывается необходимость проведения служебных проверок, вызванных нарушением установленного порядка использования. Порядок выноса съёмных носителей информации госархива описан в пункте 4.9, а форма Журнала учёта вноса/выноса съёмных носителей информации ГБУТО ГАТО помещена во

второе приложение к Инструкции. Журнал состоит из десяти столбцов:

1. № п/п;
2. дата выноса съёмного носителя информации из рабочего помещения госархива;
3. цель выноса съёмного носителя информации;
4. наименование и адрес учреждения, в которое осуществляется вынос;
5. наименование структурного подразделения и ФИО должностного лица, которому передаётся съёмный носитель информации;
6. ФИО сотрудника, ответственного за использование съёмного носителя информации, осуществляющего его вынос;
7. подпись сотрудника, осуществляющего вынос съёмного носителя информации;
8. дата возврата съёмного носителя информации в рабочее помещение госархива;
9. подпись сотрудника, ответственного за использование съёмного носителя информации, в его возврате;
10. примечания.

Вопросам проведения мероприятий в случае обнаружения утраты съёмного носителя информации, отведён пункт 4.10. следом за ним расписан порядок уничтожения данных со съёмных носителей информации, которые были возвращены после работы с ними. Форма акта об уничтожении съёмных носителей информации представлена в приложении 3 к Инструкции.

Ответственность за нарушение определённых в учреждении правил и технологий работы по рассматриваемым видам работ может быть прописана как в отдельном разделе документа, так и в «Общих положениях». В данном случае указанная информация помещена в раздел 5 «Ответственность». Здесь прописаны зоны ответственности сотрудников, которым в служебное пользование предоставлены съёмные носители информации, ответственность за доведение положений Инструкции до сотрудников архива разделена между начальником Хозяйственного отдела госархива и администратором

информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации.

Третьей разработкой инструктивных материалов, которые были подготовлены в рамках написания настоящей диссертации, стал проект *Инструкции по организации парольной защиты в ГБУТО «Государственный архив Тюменской области»*. Отличительной особенностью проекта этого документа стало выделение в отдельный раздел терминов и определений, без объяснения которых восприятие инструкции становится затруднительным. Значение терминов было определено в соответствии с Базовой моделью угроз и Руководящим документом «Защита от несанкционированного доступа к информации. Термины и определения».

Инструкция регламентирует такое направление, как организационно-техническое обеспечение генерации, порядка смены и подтверждения прекращения действия паролей в информационных системах персональных данных, а также контроль за действиями сотрудников архива при работе с паролями, что указано в «Общих положениях». Здесь же указано, на какого сотрудника Тюменского облгосархива возлагается ответственность за организационное и техническое обеспечение вышеуказанных процессов, а также контроль за реализацией требований по обеспечению безопасности при использовании паролей, а также за общий контроль за соблюдением требований парольной защиты в архиве.

Функции здесь также, как и в предыдущих разработках, распределены между системным администратором (отвечает за «техническую» составляющую) и администратором информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации (отвечает за решение организационных вопросов и документационное сопровождение). Как и в случае с проектом Инструкции по работе со съёмными носителями информации в ГБУТО ГАТО документ предполагает постоянный срок действия, поэтому завершает текст первого раздела документа общая формулировка: «Настоящая Инструкция подлежит пересмотру в случае существенного изменения условий

или порядка работы с парольной информацией в архиве».

В разделе «Требования к генерации паролей» прописаны такие условия, как длина пароля для учётной записи, наличие буквенных, символьных и цифровых знаков в значении пароля. Нормативных документов, регламентирующих процесс генерации паролей для иных систем, кроме государственных и завязанных на обработке персональных данных, не утверждено. Вследствие этого для определения требований к паролям сотрудников госархива был взят за основу и применён с учётом реальной практики работы госархива методический документ ФСТЭК – «Меры защиты информации в государственных информационных системах»: из пункта «Требования к усилению идентификации и аутентификации» третьего раздела документа были взяты основные тезисы. Требования ФСТЭК были упрощены – не взяты во внимание при разработке проекта Инструкции положения, касающиеся количества неуспешних попыток авторизации, блокировка учётной записи и др. параметры, которые изначально закладываются разработчиками программных комплексов [Меры защиты информации…]. Указаны в разделе и те сведения, которые включать в пароль нельзя, например, номера телефонов, автомобилей, общепринятые сокращения и др. Для сотрудников госархива, не имеющих доступа к обработке персональных данных в автоматизированном виде или полномочий администратора системы, допускается использование одного (одинакового) пароля для доступа субъекта доступа к различным информационным ресурсам.

Цепочка предпринимаемых действий по смене пароля определена в третьем разделе проекта Инструкции. Рассмотрены такие варианты, как смена паролей при увольнении сотрудников, отвечающих за обработку персональных данных в автоматизированном виде, либо имевших доступ к официальным профилям госархива, например, к официальной электронной почте. Указаны причины внеплановой смены личных паролей и порядок восстановления пароля в случае его утраты.

Отдельно – в четвёртом разделе – прописаны и обязанности пользователей при работе с паролями: дан перечень запрещенных действий (например, предоставлять доступ от своей учетной записи посторонним лицам), указан порядок уведомления о возникающих случаях компрометации паролей. Исходя из этих положений выделен пятый раздел – «Мероприятия, проводимые в случаях компрометации паролей», где указаны признаки компрометации, перечень действий, которые необходимо принять для предотвращения и/или снижения ущерба.

Как и в двух предыдущих случаях в проекте Инструкции по организации парольной защиты в ГБУТО «Государственный архив Тюменской области» положения об ответственности выделены в отдельный раздел. В пункте 6.3 указывается, что все создаваемые пароли заносятся системным администратором в Журнал учёта логинов и паролей, ведение которого осуществляется в электронном виде в защищённом файле по форме, установленной приложением 1 к Инструкции. Форма Журнала предполагает занесение следующей информации:

- фамилия и инициалы сотрудника;
- занимаемая должность с указанием отдела;
- сведения о названии программного комплекса, к которому создаётся учётная запись;
- логин и пароль к системе;
- дата присвоения идентификаторов;
- примечания.

Проекты Инструкции по организации антивирусной защиты в ГБУТО ГАТО, Инструкции по работе со съёмными носителями информации в ГБУТО ГАТО, Инструкции по организации парольной защиты в ГБУТО «Государственный архив Тюменской области» оформлены в соответствии с требованиями, указанными в начале настоящего раздела: документы имеют титульные листы, содержание, их тексты разделены на пункты и подпункты, в

приложения помещены журнальные формы, ведение предусматривается регламентируется положениями разработанных проектов инструкций.

Поскольку российским законодательством не предполагается обязательность разработки этих инструкций в учреждениях, те организации, у которых названные инструкции утверждены, не размещают их в свободном доступе (например, на официальном сайте) справедливо считая их документом внутреннего пользования. Исключение составляют органы муниципальной власти, однако их инструкции при разработке проектов документов за основу не брались, т.к. изложенный в них порядок действий отличается от существующей практики работы госархива. Вследствие этого текст инструкций по организации парольной и антивирусной защиты, по работе со съёмными носителями информации в госархиве составлялся исходя из собственного опыта составителя и учётом методических документов ФСТЭК.

Работа над каждой из инструкций будет завершена по итогам согласования с комиссией госархива по защите информации и утверждения директором путём издания распорядительного документа (приказа госархива) об утверждении инструкции, сама инструкция будет сформирована в качестве приложения к приказу ГБУТО ГАТО.

В ходе наблюдения за порядком разработки в госархиве инструктивных материалов в рамках обеспечения защиты информации, можно выявить наиболее часто совершаемые действия, а также рассчитать затраты времени сотрудника на выполнение каждой процедуры. При этом при проведении анализа не могут быть использованы Нормы времени на работы и услуги, выполняемые государственными архивами, изданные Всероссийским научно-исследовательским институтом документоведения и архивного дела [Нормы времени…] или разработанный на их основе аналогичный документ ГБУТО ГАТО [Нормы времени…], применены не были ввиду того, что раздел «Научно-методическая работа» не отражает все проводимые при проектировании документов делопроизводственные процедуры, а также не имеет отдельно выделенных норм для работы над инструкциями.

Для каждой разрабатываемой Инструкции по защите информации выполнен отдельный расчёт, после чего происходит суммирование результатов. В целях определения временных затрат применяется следующая формула [Об утверждении межотраслевых…]:

$T_н = V_З * H_{ВРJ}$, где $T_н$ – трудоёмкость нормируемых работ за период,

$V_З$ – объём работ J вида,

$H_{ВРJ}$ – норма времени на выполнение J-работы.

В рамках написания настоящей диссертации при подготовке Инструкции по организации парольной защиты в ГБУТО ГАТО были фактически выполнены следующие технологические процедуры, представленные в таблице 7.

Таблица 7

Расчёт трудоёмкости разработки
Инструкции по организации парольной защиты в ГБУТО ГАТО

Направление деятельности	Кол-во листов в Инструкции	Объём фактически затраченного на разработку Инструкции времени, ч
Изучение нормативных и методических документов	-	197
Подготовка проекта инструкции	12	52
Корректировка	12	3
Печатание через 1,5 интервала	12	4
Таким образом общая трудоёмкость нормируемых работ на разработку Инструкции по организации парольной защиты в ГБУТО ГАТО составляет		256 часов.

Внедрение в работу Инструкции по организации парольной защиты в ГБУТО ГАТО позволит сократить временные затраты на выполнение следующих технологических процедур, представленных в таблице 8 [Нормы времени…].

Таблица 8

Расчёт внедрения в работу разработанной
Инструкции по организации парольной защиты в ГБУТО ГАТО

Направление	Нормируемая единица измерения, л	Кол-во листов в Инструкции	Норма времени, ч	Итого, ч
Изучение нормативных и методических документов	-	-	150	150
Подготовка проекта инструкции	5	12	20	20*(12/5)=48
Корректировка	5	12	0,7	0,7*(12/5)=1,68
Печатание через 1,5 интервала	5	12	1,47	1,47*(12/5)=3,528
Общая трудоёмкость нормируемых работ на внедрение в работу разработанной Инструкции по организации парольной защиты в ГБУТО ГАТО будет составлять				203,208 часа.

При сравнении с трудоёмкостью работ за текущий период и показателей после внедрения Инструкции по организации парольной защиты в госархиве разница будет составлять 256-203,208=52,792 часа.

Расчёты для Инструкции по организации антивирусной защиты в ГБУТО ГАТО представлены в таблице 9.

Таблица 9

Расчёт трудоёмкости разработки

Инструкции по организации антивирусной защиты в ГБУТО ГАТО

Направление деятельности	Кол-во листов в Инструкции	Объём фактически затраченного на разработку Инструкции времени, ч
Изучение нормативных и методических документов	-	169
Подготовка проекта инструкции	15	75
Корректировка	15	5,5
Печатание через 1,5 интервала	15	6
Таким образом общая трудоёмкость нормируемых работ на разработку Инструкции по организации антивирусной защиты в ГБУТО ГАТО составляет		255,5 часов.

Внедрение в работу Инструкции по организации антивирусной защиты в ГБУТО ГАТО позволит сократить временные затраты на выполнение следующих технологических процедур, представленных в таблице 10.

Таблица 10

Расчёт внедрения в работу разработанной
Инструкции по организации антивирусной защиты в ГБУТО ГАТО

Направление	Нормируемая единица измерения, л	Кол-во листов в Инструкции	Норма времени, ч	Итого, ч
Изучение нормативных и методических документов	-	-	150	150
Подготовка проекта инструкции	5	15	20	20*(15/5)=60
Корректировка	5	15	0,7	0,7*(15/5)=2,1
Печатание через 1,5 интервала	5	15	1,47	1,47*(15/5)=4,41
Общая трудоёмкость нормируемых работ за год после внедрения в практику работы разработанной Инструкции по организации парольной защиты в ГБУТО ГАТО будет составлять				216,51 часов.

При сравнении с трудоёмкостью работ за текущий период и показателей после внедрения Инструкции по организации парольной защиты в госархиве разница будет составлять 255,5-216,51=38,99 часов.

Расчёты для Инструкции по работе со съёмными носителями информации в ГБУТО ГАТО представлены в таблице 11.

Таблица 11

Расчёт трудоёмкости разработки
Инструкции по работе со съёмными носителями информации
в ГБУТО ГАТО

Направление деятельности	Кол-во листов в Инструкции	Объём фактически затраченного на разработку Инструкции времени, ч
Изучение нормативных и методических документов	-	179
Подготовка проекта инструкции	13	42
Корректировка	13	3
Печатание через 1,5 интервала	13	3
Таким образом общая трудоёмкость нормируемых работ на разработку Инструкции по работе со съёмными носителями информации в ГБУТО ГАТО составляет		227 часов.

Внедрение в работу Инструкции по работе со съёмными носителями информации в ГБУТО ГАТО позволит сократить временные затраты на выполнение следующих технологических процедур, представленных в таблице 12.

Таблица 12

Расчёт внедрения в работу разработанной
Инструкции по работе со съёмными носителями информации
в ГБУТО ГАТО

Направление	Нормируемая единица измерения, л	Кол-во листов в Инструкции	Норма времени, ч	Итого, ч
Изучение нормативных и методических документов	-	-	150	150
Подготовка проекта инструкции	5	13	20	20*(13/5)=52
Корректировка	5	13	0,7	0,7*(13/5)=1,82
Печатание через 1,5 интервала	5	13	1,47	1,47*(13/5)=3,822
Общая трудоёмкость нормируемых работ за год после внедрения в практику работы разработанной Инструкции по работе со съёмными носителями информации в ГБУТО ГАТО будет составлять				207,642 часов.

При сравнении с трудоёмкостью работ за текущий период и показателей после внедрения Инструкции по работе со съёмными носителями информации в ГБУТО ГАТО разница будет составлять 227-207,642=19,358 часов.

Таким образом, исходя из вышеизложенных расчётов, можно определить разницу между фактической трудоёмкостью работ и трудоёмкостью, определяемой исходя из установленных Норм времени:

738,5-627,36=111,14 часов.

Расчёт фактической и нормируемой трудоёмкостей работ на разработку инструкций в госархиве представлен в таблице 13.

Таблица 13

Расчёт фактической и нормируемой трудоёмкостей работ на разработку инструкций в госархиве

Название разработанного документа	Фактически затраченный на разработку инструкций объём времени, ч	Нормы времени на разработку инструкций, ч
Инструкции по организации парольной защиты в ГБУТО ГАТО	256	203,208
Инструкции по организации антивирусной защиты в ГБУТО ГАТО	255,5	216,51
Инструкции по работе со съёмными носителями информации в ГБУТО ГАТО	227	207,642
Итого:	738,5	627,36

Такое отклонение от Норм времени при разработке документов объясняется, во-первых, отсутствием чётко закреплённых российским законодательством требований к документам по защите информации касаемо, во-вторых, нетипичностью разрабатываемых инструкций – образцов, отвечающих требованиям полноты и качества структуры, в свободном доступе не представлено, что стало причиной разработки документов «с ноля», т.е. только исходя из практического опыта госархива. Вследствие этого затрачиваемое на подготовку инструкций время было увеличено за счёт проведения таких мероприятий, как интервьюирование сотрудников госархива, отвечающих за рассматриваемые процессы, самостоятельное проведение отдельных этапов работы с целью более детальной оценки процедур и описания их в текстах инструкций, а также апробирования на практике внесённых в тексты инструкций теоретических пунктов.

Для дальнейшего расчёта эффективности следует вычислить стоимость часа работы администратора информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации. Исходя

из того, что оклад специалиста с учётом надбавок за интенсивность для должности и районного коэффициента, равен ≈22 000 рублей, а среднее количество рабочих часов при 40-часовой рабочей неделе в 2021 г. составит ≈164 часа, то стоимость часа работы сотрудника будет равняться 22000/164 ≈134 рубля.

Таким образом, разовая экономическая эффективность от разработки и внедрении в работу госархива Инструкций по организации антивирусной и парольной защиты, Инструкции по работе со съёмными носителями информации в ГБУТО ГАТО будет составлять 111,14*134≈14892,76 рублей.

Разработанные проекты документов включены в приложения к диссертации: проект Инструкции по организации антивирусной защиты в ГБУТО «Государственный архив Тюменской области» Проект Инструкции по организации антивирусной защиты в ГБУТО «Государственный архив Тюменской области» - в приложение 3, проект Инструкции по работе со съёмными носителями информации в ГБУТО «Государственный архив Тюменской области» - в приложение 4, а проект Инструкции по организации парольной защиты в ГБУТО «Государственный архив Тюменской области» – в приложение 5.

3.3. ПЕРСПЕКТИВЫ РАЗВИТИЯ РЕГЛАМЕНТАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ ДОКУМЕНТАЦИИ ГОСАРХИВА

Поскольку ввиду изменчивости способов и технологий нарушения информационной безопасности вероятность возникновения угроз безопасности данных никогда не будет являться нулевой, необходим постоянный анализ существующего уровня и обеспечения порядка защиты и применения дополнительных мер. Перечень таких мер определяется исходя из текущих потребностей госархива в настоящий момент времени и может включать в себя, например:

- контроль за изменениями в законодательной и нормативной базе, регламентирующей отдельные и общие вопросы защиты информации на территории Российской Федерации;
- документальное закрепление периодичности проведения регулярного контроля за актуальным состоянием средств защиты информации госархива;
- своевременное обновление лицензий программного обеспечения и возможная смена таких средств в госархиве на более действенные и результативные в настоящий момент;
- мониторинг и контрольные проверки существующего состояния защиты информационных систем госархива с определённой периодичностью;
- проведение обучающих семинаров и техучёб для сотрудников госархива, в ходе которых всем сотрудникам, в т.ч. не занятым обработкой персональных данных, будут объяснены причины возникновения угроз безопасности, описан возможный ущерб от их реализации и разъяснены требования, соблюдение которых поможет этого избежать.

Все указанные действия носят организационный характер, однако в рамках соблюдения регулярности и гарантии их выполнения они могут быть регламентированы отдельным локальным актом, например, планом мероприятий ГБУТО ГАТО по контролю за состоянием и обеспечению защиты информации на следующий год, или иметь документальную основу в виде, например, журнала учёта средств защиты информации, в котором были бы указаны сроки действия лицензий соответствующего программного обеспечения.

Помимо проведения различного рода мероприятий в рамках обновления комплекса документации Тюменского облгосархива по защите информации должно быть осуществлено закрепление в инструктивных и иных методических материалах (памятки, инструкции, рекомендации и др.) порядка выполнения отдельных видов работ по обеспечению защиты информации в госархиве, ещё не нашедших отражение в документальном виде. Так ещё не разработаны акты, которые регламентировали бы основные правила и принципы безопасной работы

с официальной электронной почтой ГБУТО ГАТО, эксплуатации рабочих компьютеров, отражали этапы и особенности порядка получения электронных подписей для различных систем и т.д.

В текст проектируемых в рамках написания настоящей диссертации инструкций были включены пункты, касающиеся взаимодействия с комиссией госархива по защите информации, однако в настоящее время состав комиссии и положение о ней не утверждены, их разработка запланирована на 1 квартал 2021 г. Нарушение такой логической последовательности в разработке документов было допущено сознательно, т.к. работа над положением о комиссии требует учёта большего количества факторов – по каждому из выполняемых действий в области обеспечения защиты информации в госархиве, а предусмотреть их без первоначального обследования основных процессов по защите информации представляется затруднительным.

Так в госархиве в 2014 г. была создана комиссия, в функционал которой входила всего одна функция, не требующая регулярного осуществления – классификация информационных систем персональных данных госархива. При этом в изданных в то же время и позднее инструкциях были отсылки с указанием полномочий безымянной комиссии. Т.к. для комиссии по классификации информационных систем персональных данных госархива её функционал был определён только в названии, а других комиссий в области информационной безопасности в ГБУТО ГАТО не существовало, а также ввиду того, что разработка документов осуществлялась в рамках написания магистерской диссертации, т.е. без ущерба рабочему процессу и потери временных ресурсов от применения такой последовательности, был сделан вывод о том, что подобный подход к организации работы нецелесообразен.

Поэтому первоначальным этапом разработки стала регламентация отдельных работ в области защиты информации, в процессе проектирования определены отдельные функции, которые должны находиться в ведении комиссии госархива по защите информации. Утверждаться же будет изначально приказ о создании такой комиссии, определении её состава и утверждении

инструкции для комиссии (которую также необходимо разработать). Разработанные в процессе написания выпускной квалификационной работы инструкции, а также Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия», будут переданы для согласования уже после создания комиссии. В текст положения о комиссии будут включены абзацы из проектов разработанных инструкций по организации антивирусной защиты, обновлённых инструкций ответственных за защиту информации в ГБУТО «Государственный архив Тюменской области» лиц, по безопасной работе с офисным оборудованием и др., в том числе касающиеся рассмотрения результатов расследования причин появления и последствий от воздействия вредоносных программ, ежегодного отчёта о состоянии антивирусной защиты в архиве и др.

К утверждаемым в госархиве документам в качестве приложений могут быть помещены отдельные журнальные формы, например, форма журнала учёта проведённых инструктажей по отдельным вопросам информационной безопасности, форма журнала проведённых в госархиве мероприятий по контролю обеспечения защиты информации в госархиве, форма журнала учёта лицензий средств защиты информации.

Отдельными приказами могут быть утверждены различные документы, конкретизирующие отдельные вопросы организации процессов по защите информации (например, схема расположения персональных компьютеров и серверов госархива, подлежащих регулярным антивирусным проверкам), перечни сотрудников, допущенных к определённому виду работ с доступом к документам, содержащими сведения ограниченного доступа.

В качестве справочных материалов могут быть разработаны перечни или списки официальных интернет-источников профильных учреждений в области защиты данных и литературных или иных материалов, содержащих полезные сведения для сотрудников, ответственных за защиту информации в госархиве, актуальные перечни правовых актов, которыми необходимо руководствоваться при осуществлении работ по защите информации и др.

Таким образом, подводя итог проведённому исследованию, можно сделать о том, что комплекс организационно-распорядительной документации такого направления деятельности Государственного бюджетного учреждения Тюменской области «Государственный архив Тюменской области» как защита информации находится в данный момент в удовлетворительном состоянии, а комплекс методической документации – в неудовлетворительном, и требует доработки. Если основополагающие документы в сфере информационной безопасности в ГБУТО ГАТО разработаны и утверждены, пусть некоторые из них и требуют внесения изменений и дополнений, то ряд других узкоспециальных направлений работы в настоящее время ничем не регламентирован и будет подлежать разработке в будущем.

ЗАКЛЮЧЕНИЕ

Вопросы защиты информации в современном мире приобретают всё более важное значение, в связи с чем одним из направлений основной деятельности практически каждого учреждения стал такой вид работы, как обеспечение защиты сведений, носящих конфиденциальный характер. Служебная и профессиональная тайна, сведения, связанные с коммерческой деятельностью, персональные данные сотрудников и клиентов подлежат защите, что закреплено в Российской Федерации на законодательном уровне. В рамках реализации данного направления деятельности в Государственном бюджетном учреждении Тюменской области «Государственный архив Тюменской области» был утверждён комплекс документации по защите информации. Однако, большинство актов издавались до 2017 г., а за время, прошедшее с этого момента, изменилась практика работы, появились новые направления деятельности в сфере информационной безопасности, в связи с чем возникла необходимость в пересмотре ранее утверждённых документов, разработке новых актов, регламентирующих выполнение отдельных процедур, обеспечивающих соответствующий уровень защиты данных.

При изучении темы и написании выпускной квалификационной работы работа была построена в соответствии с установленными задачами, их решение осуществлялось поэтапно. На первом этапе работы был проведён анализ действующих законодательных актов Российской Федерации, постановлений российского Правительства в области защиты информации, изучены государственные стандарты, дана характеристика тем из них, которые имели практическую пользу для работы. Отдельно проанализированы акты Федеральной службы по техническому и экспортному контролю Российской Федерации методического характера, т.к. именно этот орган является профильным в вопросах обеспечения безопасности информации на территории России. Результат проведённой работы был изложен в пункте 1.1 диссертации.

Для достижения поставленной цели была изучена структура ГБУТО ГАТО, цели его деятельности, рассмотрено место и роль отдела информационно-поисковых систем и защиты информации, структура отдела, его функции в рамках обеспечения информационной безопасности. Основное внимание уделялось сбору и рассмотрению локальных документов, отражающих вопросы проведения отдельных организационных процедур. Также документация Тюменского облгосархива по защите информации, возникающей в процессе осуществления текущей управленческой деятельности, изучалась на предмет выявления особенностей оформления и определения значения документа и отдельных его частей для делопроизводственных процессов этого вида деятельности. Все полученные данные были проанализированы, наиболее соответствующие тематике работы положения включены в пункты 1.2-1.3 и 2.1-2.2 настоящей выпускной квалификационной работы.

Следующие задачи заключались в установлении направлений дальнейшего совершенствования существующего комплекса документации госархива по обеспечению информационной безопасности. Её осуществление основывалось на информации, полученной на предыдущем этапе работы, т.е. изучении локальных нормативных актов ГБУТО ГАТО, а также изучении практического опыта госархива в организации и проведении работ по защите информации, документальном регламентировании отдельных этапов работы. Сбор и анализ основного массива документации ГБУТО ГАТО по защите информации позволил также сделать ряд выводов, на основании которых была выявлена необходимость внесения изменений и дополнений в ранее утверждённую Политику обработки персональных данных в ГБУТО «Государственный архив Тюменской области», разработки Частной модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия», инструкций по организации парольной и антивирусной защиты, инструкции по работе со съёмными носителями информации.

Также был осуществлён анализ иных источников информации – методических документов, документов других учреждений, статей и научных работ – с целью подбора источников для разработки локальных нормативных актов в Тюменском облгосархиве. На основе проведённого исследования был сделан вывод, помещённый в третью главу работы – на данный момент в отечественном законодательстве и публицистических материалах отсутствует чёткая регламентация нужных для разработки проектов документов для ГБУТО ГАТО направлений работы. Организации и учреждения по большей части утверждают типовые тексты документов (например, инструкции по антивирусной защите), при этом мало кто размещает такие документы у себя на официальных сайтах. Статьи в области защиты информации тоже представляют собой либо обобщённый теоретический материал, написанный на основе учебных пособий и законодательных актов, либо рассматривают только техническую сторону вопроса, которая в данной работе не затрагивается. Определение сроков и непосредственно проектирование документов стало последним этапом проводимых работ при написании магистерской диссертации.

Итогом исследовательской деятельности в соответствии с поставленными на стадии планирования работы задачами о разработке документации, способствующей совершенствованию комплексу документации ГБУТО ГАТО по защите информации и, как следствие, повышению уровня защищённости данных в госархиве, стала разработка Частной модели угроз безопасности персональных данных при их обработке в ИСПДн «Бухгалтерия» в ГБУТО «Государственный архив Тюменской области», а также Инструкции по организации парольной защиты в ГБУТО «Государственный архив Тюменской области», Инструкции по организации антивирусной защиты в ГБУТО «Государственный архив Тюменской области», Инструкции по работе со съёмными носителями информации в ГБУТО «Государственный архив Тюменской области». Таким образом, можно прийти к выводу о том, что все поставленные задачи были решены в полном объеме.

Выпускная квалификационная работа содержит подробное описание каждого разработанного документа как в части его структуры и содержания, так и с точки зрения его оформления. Также в работе проанализированы недостатки утверждённых в госархиве документов по защите информации, а в пункте 3.3 перечислены возможные направления дальнейшего совершенствования комплекса документации Тюменского облгосархива в области защиты информации.

Изучение темы исследования и написание выпускной квалификационной работы осуществлялось поэтапно в течение года. За этот период был собран весь необходимый материал для всестороннего рассмотрения темы. Сбор информации в ГБУТО ГАТО предполагал работу с документами, взаимодействие с уполномоченными в сфере информационной безопасности должностными лицами организации, наблюдение за рабочим процессом проведения отдельных процедур по защите информации, принималось участие в осуществлении некоторых из них (например, проведении антивирусной проверки рабочих персональных компьютеров сотрудников госархива). Временные ресурсы были распределены таким образом, чтобы выполнение каждого из направлений работ на всех этапах соответствовало отведенному для него промежутку времени. Таким образом, процедуру написания магистерской диссертации можно охарактеризовать как имеющую высокую степень самоорганизации, у автора работы отметить наличие умения грамотно управлять имеющимися ресурсами, а также осуществлять полноценную социальную и профессиональную деятельность.

Соблюдённая структура диссертации даёт возможность говорить о том, что рассматриваемый вопрос был изучен со всех необходимых для проектирования документов сторон, описаны все основные организационные меры госархива, предпринимаемые в сфере информационной безопасности, нашедшие документальное закрепление в различных локальных документах. Для обеспечения более удобного восприятия в тексте диссертации применялось использование графических элементов – таблиц, схем, а в проекте Частной

модели угроз безопасности персональных данных при их обработке в ИСПДн «Бухгалтерия» в ГБУТО «Государственный архив Тюменской области» использовались ещё и рисунки.

При написании третей главы в текст диссертации было включено описание методики проектирования. Она описана для разрабатываемых инструкция, т.к. по разработке Модели угроз имеются соответствующие рекомендации ФСТЭК и представлен Типовой документ, а для Политики данная в диссертации методике не применима ввиду того, что документ не разрабатывался, а дополнялся и уточнялся путём внесения соответствующих положений в ранее утверждённый акт ГБУТО ГАТО.

В ходе разработки проектов документов был выполнен расчёт эффективности внедрения разработанных инструкций, выявлена возможная экономия временных затрат на выполнение основных технологических операций в процессе организации и проведения защиты информации в ГБУТО «Государственный архив Тюменской области». Трудоёмкость нормируемых работ, вычисленная с учётом применения в текущем делопроизводстве разработанных методических документов, была также переведена в денежный формат. Все расчёты содержатся в пункте 3.2 настоящей выпускной квалификационной работы.

Говоря о практической пользе материалов, разработанных в ходе написания настоящей выпускной квалификационной работы, нельзя не отметить, что при проектировании в качестве основы был использован изученный практический опыт в проведении таких мероприятий по обеспечению защиты информации в госархиве, как организация антивирусной проверки, работа со съёмными носителями информации, установление парольной системы для входа в информационные системы и их отдельные компоненты, что делает разработанные проекты документов более жизнеспособными, т.е. соответствующими целям и задачам проведения указанных видов работ именно для Тюменского облгосархива.

На основании изложенного в работе материала, можно сделать следующий вывод: цель проведения магистерского исследования была достигнута, поставленные задачи – достигнуты, а результаты научной деятельности подробно изложены в тексте диссертации. Однако, объективно оценивая проделанную работу, учитывая тот факт, что для темы работы была выбрана только организационная часть процесса защиты информации, затрагивающая только внутреннюю, управленческую деятельность ГБУТО «Государственный архив Тюменской области», можно прийти к следующему выводу о том, что исследования в данном направлении могут быть продолжены, а всё возрастающая роль защиты данных позволяет говорить о сохранении актуальности такой работы в будущем.

Проведённое исследование и полученные знания позволяют выделить проблемные моменты в организации системы защиты информации госархива на документном уровне. Например, вследствие разделения способов обработки персональных данных как основного вида защищаемой информации ГБУТО ГАТО на автоматизированный и неавтоматизированный, а также ввиду необходимости защиты сведений не только о собственных сотрудниках, но и о пользователях государственных услуг, процедура документирования оказалась весьма усложнена. В настоящее время действующие локальные акты не затрагивают весь спектр необходимых вопросов обеспечения безопасности. Ряд моментов, например, разработка документов, регламентирующих безопасную работу с входящими электронными документами, эксплуатации рабочего аппаратного и программного обеспечения и иные остались незатронутыми, что позволяет продолжать исследовательскую работу в данном направлении, а также разрабатывать и предлагать к внедрению в ГБУТО «Государственный архив Тюменской области» различные проекты, в различной степени позволяющие минимизировать трудовые и денежные затраты на их выполнение, а также повышать уровень защищённости информации в учреждении.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

ИСТОЧНИКИ

1. Конституция Российской Федерации: от 12 декабря 1993 г.: по состоянию на 01.07.2020 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.04.2020).

2. Уголовный кодекс Российской Федерации: от 13 июня 1996 г.: по состоянию на 08.12.2020 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.04.2020).

3. Трудовой кодекс Российской Федерации: от 30 декабря 2002 г.: по состоянию на 29.12.2020 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.04.2020).

4. О государственной тайне: Федеральный закон № 5485-1: от 21 июля 1993 г.: по состоянию на 06.01.2021 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 17.09.2020).

5. О коммерческой тайне: Федеральный закон № 98: от 29 июля 2004 г.: по состоянию на 18.04.2018 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.04.2020).

6. Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ: от 27 июля 2003 г.: по состоянию на 08.06.2020 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 17.09.2020).

7. О персональных данных: Федеральный закон № 152-ФЗ: от 27 июля 2006 г.: по состоянию на 08.12.2020 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 18.01.2021).

8. Об электронной подписи: Федеральный закон № 63: от 06 апреля 2011 г.: по состоянию на 06.01.2021 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.11.2020).

9. О стратегии национальной безопасности Российской Федерации до 2020 г.: указ Президента Российской Федерации: от 31 декабря 2015 г. // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 17.09.2020).

10. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства Российской Федерации от 01 ноября 2012 г., № 1119 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 12.12.2020).

11. Об установлении запрета на допуск программного обеспечения происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд: Постановление Правительства Российской Федерации от 16 ноября 2014 г., № 1236 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 12.12.2020).

12. Об утверждении Межотраслевых укрупнённых нормативов времени на работы по документационному обеспечению управления: Постановление Минтруда России от 25 ноября 1994 г., № 72 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.01.2021).

13. Нормы времени на работы по документационному обеспечению управленческих структур федеральных органов исполнительной власти. Утв. Постановлением Минтруда России от 26 марта 2002 г., № 23 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.01.2021).

14. Нормы времени на работы и услуги, выполняемые государственными архивами. Утв. Росархивом 01 марта 2007 г. // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.01.2021).

15. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11 февраля 2013 г., № 17 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 12.12.2020).

16. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК от 18 февраля 2013 г., № 21 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 26.12.2020).

17. Об утверждении статистического инструментария для организации федерального статистического наблюдения за потребительскими ожиданиями населения на 2009 год: приказ Росстата от 26 ноября 2008 г., № 288 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 20.11.2020).

18. О защите персональных данных государственных гражданских служащих центрального аппарата и заместителей руководителей территориальных органов Федеральной службы по надзору в сфере здравоохранения и социального развития: приказ Росздравнадзора от 12 мая 2009 г., № 3500-Пр/09 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 21.09.2020).

19. Об утверждении Положения о работе с персональными данными государственного гражданского служащего Федерального медико-биологического агентства и ведении его личного дела: приказ ФМБА РФ от 08 июля 2009 г., № 501 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 24.10.2020).

20. Об организации работы с персональными данными государственного гражданского служащего центрального аппарата Федерального агентства железнодорожного транспорта и ведении его личного дела: приказ Росжелдора

от 07 апреля 2010 г., № 137: ред. от 28.09.2015 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 31.10.2020).

21. Защита от несанкционированного доступа к информации. Термины и определения: руководящий документ. Утв. Гостехкомиссией при Президенте Российской Федерации 30 марта 1992 г. // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 17.11.2020).

22. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утв. приказом Председателя Гостехкомиссии России от 30.08.2002 № 282 // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 26.10.2020).

23. Разработка нормативных документов по документационному обеспечению организаций. Рекомендации. М., ВНИИДАД, 2007. 101 с.

24. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утв. зам.директора ФСТЭК России 14 февраля 2008 г. // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.01.2021).

25. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утв. Заместителем директора ФСТЭК России 15 февраля 2008 г. // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.01.2021).

26. Меры защиты информации в государственных информационных системах: методический документ. Утв. ФСТЭК России 11 февраля 2014 г. // Консультант

Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.01.2021).

27. О перечне законодательных актов и нормативных документов по защите конфиденциальной информации и персональных данных: письмо Роструда от 12 мая 2010 г., № 2198-ТЗ // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.01.2021).

28. ГОСТ Р ИСО/МЭК 13335-1-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий: дата введения 2006-12-19. Москва, Стандартинформ, 2007. 19 с.

29. ГОСТ Р ИСО/МЭК 27003-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасаности. Руководство по реализации системы менеджмента информационной безопасности: дата введения 2013-12-01. Москва, Стандартинформ, 2014. 57 с.

30. ГОСТ Р 50739-95. Национальный стандарт Российской Федерации. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования: дата введения 1995-02-09. Москва, Стандартинформ, 1995. 11 с.

31. ГОСТ Р 51188-98. Национальный стандарт Российской Федерации. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство: дата введения 2003-08-01. Москва, Стандартинформ, 1998. 9 с.

32. ГОСТ Р 52448-2005. Национальный стандарт Российской Федерации. Защита информации. Обеспечение безопасности сетей электросвязи. Общи е положения: дата введения 2007-01-01. Москва, Стандартинорм, 2019. 23 с.

33. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения: дата введения 2008-02-01. Москва, Стандартинформ, 2008. 17 с.

34. ГОСТ Р 52863-2007. Национальный стандарт Российской Федерации. Защита информации. Автоматизированные системы в защищённом исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования (переиздание): дата введения 2008-07-01. Москва, Стандартинформ, 2020. 66 с.

35. ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения: дата введения 2009-10-01. Москва: Стандартинформ, 2009. 30 с.

36. ГОСТ Р 53115-2008. Национальный стандарт Российской Федерации. Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищённости от несанкционированного доступа. Методы и средства: дата введения 2009-10-01. Москва: Стандартинформ, 2018. 38 с.

37. ГОСТ Р 52633.1-2009. Национальный стандарт Российской Федерации. Защита информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадёжной биометрической аутентификации: 2010-01-01. Москва: Стандартинформ, 2019. 24 с.

38. ГОСТ Р 52633.6-2012. Национальный стандарт Российской Федерации. Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу «Свой»: дата введения 2012-12-01. Москва: Стандартинформ, 2018. 24 с.

39. ГОСТ Р 7.0.8–2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу.

Делопроизводство и архивное дело. Термины и определения: дата введения 2013-10-17. Москва, Стандартинформ, 2014. 32 с.

40. ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения: дата введения 2014-09-01. Москва, Стандартинформ, 2014. 20 с.

41. ГОСТ Р 56546-2015. Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем: дата введения 2015-08-19. Москва: Стандартинформ, 2015. 12 с.

42. ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов: дата введения 2018-07-01. Москва: Стандартинформ, 2016. 37 с.

43. О создании государственного учреждения Тюменской области «Государственный архив Тюменской области: распоряжение Администрации Тюменской области от 28 июня 2002 г., № 509-р // Консультант Плюс: справочно-поисковая система. Режим доступа: локальная сеть ТюмГУ (дата обращения 15.01.2021).

44. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации в Управлении по делам архивов Тюменской области // Текущий архив Управления по делам архивов Тюменской области.

45. Модель нарушителя безопасности информации в ИСПДн «Директум Управления по делам архивов Тюменской области // Текущий архив Управления по делам архивов Тюменской области.

46. Технический паспорт на ИСПДн «Директум» Управления по делам архивов Тюменской области // Текущий архив Управления по делам архивов Тюменской области.

47. О назначении ответственного за обеспечение информационной безопасности: приказ Государственного архива Тюменской области от 15 мая 2015 г., № 11 // Текущий архив ГБУТО «Государственный архив Тюменской области».

48. Об обеспечении безопасности персональных данных: приказ Государственного архива Тюменской области от 07 декабря 2016 г., № 22 // Текущий архив ГБУТО «Государственный архив Тюменской области».

49. Об утверждении перечней должностей, допущенных к обработке персональных данных сотрудников Государственного бюджетного учреждения Тюменской области «Государственный архив Тюменской области»: приказ Государственного архива Тюменской области от 23 декабря 2020 г., № 30 // Текущий архив ГБУТО «Государственный архив Тюменской области».

50. О назначении ответственных за обеспечение информационной безопасности в Государственном бюджетном учреждении Тюменской области «Государственный архив Тюменской области: приказ Государственного архива Тюменской области от 26 июня 2020 г., № 18 // Текущий архив ГБУТО «Государственный архив Тюменской области».

51. Штатное расписание ГБУТО «Государственный архив Тюменской области. Утв. Приказом ГБУТО ГАТО от 29 декабря 2018 г. № 30 // Текущий архив ГБУТО «Государственный архив Тюменской области».

52. Номенклатура дел ГБУТО ГАТО. Утв. приказом ГБУТО ГАТО от 30 ноября 2016 г., № 11 // Текущий архив ГБУТО «Государственный архив Тюменской области».

53. Положение об обработке и защите персональных данных в ГБУТО «Государственный архив Тюменской области». Утв. приказом ГБУТО ГАТО от

27 июля 2014 г., № 26 // Текущий архив ГБУТО «Государственный архив Тюменской области».

54. Положение об отделе информационно-поисковых систем и защиты информации ГБУТО «Государственный архив Тюменской области. Утв. Приказом ГБУТО ГАТО от 29 декабря 2018 г. № 35 // Текущий архив ГБУТО «Государственный архив Тюменской области».

55. Инструкция по делопроизводству ГБУТО «Государственный архив Тюменской области». Утв. Приказом ГБУТО ГАТО от 01 июля 2011 г. № 13 // Текущий архив ГБУТО «Государственный архив Тюменской области».

56. Должностная инструкция администратора информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации Государственного бюджетного учреждения Тюменской области «Государственный архив Тюменской области» Утв. приказом ГБУТО ГАТО от 15 ноября 2019 г., № 30 // Текущий архив ГБУТО «Государственный архив Тюменской области».

57. Инструкция администратору безопасности в информационных системах персональных данных. Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 13 // Текущий архив ГБУТО «Государственный архив Тюменской области».

58. Инструкция ответственному за эксплуатацию информационных систем персональных данных. Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 13 // Текущий архив ГБУТО «Государственный архив Тюменской области».

59. Инструкция работнику, ведущему обработку персональных данных без использования средств автоматизации. Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 13 // Текущий архив ГБУТО «Государственный архив Тюменской области».

60. Инструкция ГБУТО ГАТО по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных.

Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 13 // Текущий архив ГБУТО «Государственный архив Тюменской области».

61. Инструкция ГБУТО ГАТО по организации парольной защиты в информационных системах персональных данных. Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 13 // Текущий архив ГБУТО «Государственный архив Тюменской области».

62. Инструкция ГБУТО ГАТО по организации антивирусной защиты в информационных системах персональных данных. Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 13 // Текущий архив ГБУТО «Государственный архив Тюменской области».

63. Инструкция ГБУТО ГАТО по организации резервирования и восстановления программного обеспечения и баз персональных данных. Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 13 // Текущий архив ГБУТО «Государственный архив Тюменской области».

64. Инструкция ГБУТО ГАТО о порядке работы пользователей информационных систем персональных данных. Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 13 // Текущий архив ГБУТО «Государственный архив Тюменской области».

65. Инструкция ГБУТО ГАТО о порядке проверки электронного журнала обращений к информационным системам персональных данных. Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 13 // Текущий архив ГБУТО «Государственный архив Тюменской области».

66. Инструкция ГБУТО ГАТО по использованию средств защиты информации в информационной системе персональных данных. Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 13 // Текущий архив ГБУТО «Государственный архив Тюменской области».

67. Инструкция о порядке учета, хранения, уничтожения носителей персональных данных ГБУТО «Государственный архив Тюменской области».

Утв. приказом ГБУТО ГАТО от 28 июля 2014 г., № 23 // Текущий архив ГБУТО «Государственный архив Тюменской области».

68. Инструкция ответственного за организацию обработки персональных данных в ГБУТО ГАТО. Утв. приказом ГБУТО ГАТО от 07 декабря 2016 г., № 22 // Текущий архив ГБУТО «Государственный архив Тюменской области».

69. Перечень конфиденциальной информации ГБУТО «Государственный архив Тюменской области». Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 14 // Текущий архив ГБУТО «Государственный архив Тюменской области».

70. Перечень персональных данных, обрабатываемых в информационных системах персональных данных ГБУТО «Государственный архив Тюменской области». Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 15 // Текущий архив ГБУТО «Государственный архив Тюменской области».

71. Схема контролируемой зоны ГБУТО ГАТО. Утв. приказом ГБУТО ГАТО от 27 июля 2014 г., № 17 // Текущий архив ГБУТО «Государственный архив Тюменской области».

72. Аттестат соответствия требованиям безопасности информации при её обработке в информационной системе персональных данных «Директум» ГБУТО ГАТО от 01 ноября 2016 г., № 002/14 // Текущий архив ГБУТО «Государственный архив Тюменской области».

73. Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Директум» ГБУТО ГАТО от 11 июля 2014 г. // Текущий архив ГБУТО «Государственный архив Тюменской области».

74. Нормы времени на работы и услуги, выполняемые ГУТО «Государственный архив Тюменской области». Утв. приказом ГУТО ГАТО № 8 от 02.04.2010 // Текущий архив ГБУТО «Государственный архив Тюменской области».

75. Памятка по подготовке методических пособий сотрудниками ГУТО ГАТО. Тюмень, 2008. Утв. директором 05 июня 2008 г. // Текущий архив ГБУТО «Государственный архив Тюменской области».

76. Документы госархива о состоянии защиты информации в организации (акты, заключения, переписка) // Текущий архив ГБУТО «Государственный архив Тюменской области».

77. Журнал ознакомления с положением об отделе и должностными инструкциями сотрудниками отдела // Текущий архив ГБУТО «Государственный архив Тюменской области».

78. Журнал учета проведенных занятий по повышению квалификации сотрудников отдела // Текущий архив ГБУТО «Государственный архив Тюменской области».

79. Журнал регистрации работ по устранению технических неполадок серверного оборудования (внутренняя локальная сеть) // Текущий архив ГБУТО «Государственный архив Тюменской области».

80. Журнал регистрации работ по устранению технических неполадок серверного оборудования (интернет-портал) // Текущий архив ГБУТО «Государственный архив Тюменской области».

81. Журнал учёта сроков действия сертификатов безопасности// Текущий архив ГБУТО «Государственный архив Тюменской области».

82. Журнал учёта выдачи карт и флеш-накопителей с электронной подписью// Текущий архив ГБУТО «Государственный архив Тюменской области».

83. Журнал учёта проведения антивирусных проверок в госархиве // Текущий архив ГБУТО «Государственный архив Тюменской области».

84. Журнал учёта перемещения оргтехники и компьютерного оборудования госархива // Текущий архив ГБУТО «Государственный архив Тюменской области».

ЛИТЕРАТУРА

85. Абидарова А.А. Физические средства защиты информации / А.В. Абидарова // Наука, образование и культура. 2019. № 2. С. 25-26.

86. Авдеева Н.В., Сусь И.В. Актуальные проблемы оформления справочно-библиографического аппарата в научных документах / Н.В. Авдеева, И.В. Сусь // Открытое образование. 2020. № 5. С. 29-35.

87. Андреева В.И. Делопроизводство. Организация и ведение. Москва: Кнорус, 2020. 294 с.

88. Атаманов Г.А. Технические каналы утечки информации: определение, сущность, классификация / Г.А. Атаманов // Защита информации. 2010. № 1 (31). С. 28-33.

89. Афанасьева Д.В. Абидарова А.А. Средства криптографической защиты информации / Д.В. Афанасьева, А.А. Абидарова // Известия Тульского государственного университета. 2019. № 3. С. 67-71.

90. Афанасьева Д.В. Абидарова А.А., Плахина Е.А. Обеспечение безопасности автоматизированных систем при взаимодействии с сетью Интернет / Д.В. Афанасьева, А.А. Абидарова, Е.А. Плахина // Известия Тульского государственного университета. 2019. № 12. С. 382-385.

91. Ахмедова А.Г. Защита информации от внутренних угроз / А.Г, Ахмедова // European Science. 2018. № 5 (37). С. 28-29.

92. Баранов А.С. Использование средств криптографической защиты информации в организациях / А.С. Баранов // Международный научно-исследовательский журнал. 2020. № 6 (96). С. 131-133.

93. Баринов С.В. О правовом определении понятия «Информационная безопасность личности / С.В. Баринов // Актуальные проблемы российского права. 2016. № 4 (65). С. 97-105.

94. Богданова А.М., Путилов А.О. Защита конфиденциальных данных как способ поддержания информационной безопасности / А.М. Богданова, А.О. Путилов // Скиф. Вопросы студенческой науки. 2020. № 5 (45). С. 102-106.

95. Бондарь И.В. Методика построения модели угроз безопасности информации для автоматизированных систем / И.В. Бондарь // Сибирский журнал науки и технологий. 2012. № 21. С. 7-10.

96. Кобышева М.С., Федотов А.В., Кобышев К.И. Моделирование угроз безопасности предприятия при не сохранении конфиденциальности персональной информации работников / М.С. Кобышева, А.В. Федотов, К.И. Кобышев // Управление экономическими системами. 2017. № 5 (99). С. 74-89.

97. Быкова Т.А. Разработка должностной инструкции на основе профессионального стандарта / Т.А. Быкова // Научный вестник. 2017. № 5 (10). С. 3-8.

98. Воронин В.В., Сухоруков Я.П. Аспекты разработки Частной модели угроз безопасности информации в типовых информационных системах / В.В. Воронин, Я.П. Сухоруков // Вестник Приамурского государственного университета им. Шолом-Алейхема. 2020. № 1 (38). С. 24-33.

99. Галахов В.В., Корнеев И.К., Пшенко А.В. Делопроизводство. Образцы, документы. Организация и технология работы. Москва: РГ-Пресс, 2021. 480 с.

100. Герасимова Е.Б., Герасимов Б.И., Тётушкин В.А. Открытость процедур проектирования документов по стандартизации / Е.Б. Герасимова, Б.И. Герасимов, В.А. Тётушкин // Вестник Тамбовского государственного технического университета. 2017. № 3. С. 402-411.

101. Грошева Е.К., Невмержицкий П.И. Информационная безопасность: современные реалии / Е.К. Грошева, П.И. Невмержицкй // Бизнес-образование в экономике знаний. 2017. № 3. С. 35-38.

102. Гугуева Т.А. Конфиденциальное делопроизводство. Москва. Инфра-М, 2021. 199 с.

103. Домбровская Л.А., Васютина Т.Л. Организационные средства защиты информации как элемент общей системы защиты информации / Л.А. Домбровская, Т.Л. Васютина // European Science. 2016. № 11 (21). С. 38-47.

104. Дроздова Е.Ю. Инструкция по антивирусной защите организации: что нужно знать / Е.Ю. Дроздова // European Scientific Conference. 2020. С. 46-48.

105. Дроздова Е.Ю. Как приказы помогают обеспечить безопасность данных в учреждении / Е.Ю. Дроздова // Научное сообщество XXI века. 2020. С. 83-90.

106. Дуплий Е.В., Овсянникова А. Шаг вперёд или назад? О проекте новой версии государственного стандарта «Требования к оформлению документов» / Е.В. Дуплий, А. Овсянникова // Материалы Афанасьевских чтений. 2016. № 2 (15). С. 138-145.

107. Егоров В.П., Слиньков А.В. Конфиденциальное делопроизводство. Учебное пособие. Москва: Юридический институт МИИта, 2015. 178 с.

108. Завгородний В.И. Комплексная защита информации в компьютерных системах. Москва: Логос, 2001. 264 с.

109. Захаров Д.В. Основные понятия информатики. Аппаратное обеспечение информационных технологий. Волгоград: ВА МВД России, 2009. 31 с.

110. Зиновьева Н.Б. Понятие «документ» и границы дисциплины «Документоведение» / Н.Б. Зиновьева // Культурная жизнь Юга России. 2012. № 4 (47). С. 53-58.

111. Иванова А.П. Утечка персональных данных: большая проблема в цифровую эпоху / А.П. Иванова // Социальные и гуманитарные науки. 2020. № 4. С. 100-108.

112. Иванова Н.Ю., Романова Е.Б. Составление и оформление документов: учебно-методическое пособие. Санкт-Петербург: Университет ИТМО, 2019. 78 с.

113. Каменева Е. Технологии работы с проектами документов / Е. Каменева // Делопроизводство и документооборот на предприятии, 2009, № 1. С. 46-62.

114. Капустин Ф.А. Информационная безопасность и защита информации в современном обществе / Ф.А. Капустин // Актуальные проблемы авиации и космонавтики. 2016. № 12. С. 738-740.

115. Карасёв П.А. Информационная безопасность в корпоративных сетях / П.А. Карасёв // Таврических научный обозреватель. 2017. № 3. С. 9-14.

116. Кизелев П.А. Информационные технологии в обществе / П.А. Кизелев // Эпоха науки. 2017. № 9. С. 151-152.

117. Конопкин Н.И. Системы защиты персональных данных: возможно ли учесть современные реалии, основываясь на традиционные подходы? / Н.И. Конопкин // Защита информации. 2010. № 6. С. 14-17.

118. Кириенко А.Е. Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения /

119. А.Е. Кириенко // Молодой учёный, 2012. № 3 (38). С. 40-46.

120. Ланской Г.Н. О взаимосвязи документоведения и архивоведения в информационном обществе / Г.Н. Ланской // История и архивы. 2017. № 1 (7). С. 9-14.

121. Ленковская Р.Р., Шиловская А.Л. Защита информации в сети Интернет / Р.Р. Ленковская, А.Л. Шиловская // Проблемы экономики и юридической практики. 2017. № 5. С. 89-93.

122. Линь До. Основные тенденции в сфере защиты авторского права и персональных данных в сети интернет / До Линь // NB: Административное право и практика администрирования. 2020. № 1. С. 1-8.

123. Луценко Д.А., Кусмагмбетов С.М. Критерии оценки безопасности информационных систем / Д.А. Луценко, С.М. Кусмагмбетов // Материалы 71-й студенческой научной конференции. 2020. № С. 156-161.

124. Мамаева Л.Н., Кондратьева О.А. Основные направления обеспечения информационной безопасности предприятия / Л.Н. Мамаева, О.А. Кондратьева // Информационная безопасность регионов. 2016. № 4 (25). С. 5-9.

125. Мхитарян А.С. Цифровой мир как четвёртый всадник апокалипсиса: настолько ли опасны современные технологии? / А.С. Мхитарян // Вестник Прикамского социального института. 2020. № 2 (86). С. 30-33.

126. Никитин С. Бумажная защита корпоративной сети / С. Никитин // Защита информации. 2010. № 1. С. 50-53.

127. Пинус А.С., Базарова И.А., Хозяинова Т.В. Информационная система учета уязвимостей оборудования и программного обеспечения

автоматизированных систем управления технологическим процессом / А.С. Пинус, И.А. Базарова, Т.В. Хозяинова // Информационные технологии в управлении и экономике. 2019. № 2 (15). С. 27-37.

128. Рогожин М.Ю. Настольная книга ответственного за делопроизводство. Москва: Проспект, 2020. 128 с.

129. Савченко Л.М., Долгова Т.Г. Защита информации / Л.М. Савченко, Т.Г. Долгова // Актуальные проблемы авиации и космонавтики. 2015. № 11. С. 608-610.

130. Северцев Н.А., Бецков А.В. Информационная безопасность и принципы её обеспечения / Н.А. Северцев, А.В. Бецков // Труды Международного симпозиума «Надёжность и качество. 2018. С. 44-47.

131. Скрипник Д. А. Общие вопросы технической защиты информации. Москва: НОУ «ИНТУИТ», 2016. 425 с.

132. Смаженков Н.С. Нормативно-правовое регулирование защиты персональных данных в условиях использования цифровых технологий / Н.С. Смаженков // Вопросы российской юстиции. 2020. № 7. С. 576-583.

133. Солдатова В.И. Защита персональных данных в условиях применения цифровых технологий / В.И. Солдатова // Lex Russica. 2020. № 2 (159). С. 33-43.

134. Суровцева Н.Г. Электронный документ как объект документоведения: историографический обзор / Н.Г. Суровцева // Самарский научный вестник. 2018. № 4 (25). С. 277-285.

135. Трунова А.В. Обеспечение информационной безопасности предприятия / А.В. Трунова // Современные инновации. 2018. № 4 (26). С. 17-19.

136. Фомина Л.Ю. Международные стандарты защиты персональных данных в условиях информационного общества / Л.Ю. Фомина // Международное право. 2019. № 4. С. 50-59.

137. Хижняк М.В. Информационная безопасность в РФ: в поиске новых партнёров / М.В. Хижняк // Управленческое консультирование. 2018. № 2. С. 137-144.

138. Хорохордина О.В. Инструкция как тип текста / О.В. Хорохорина // Мир русского слова. 2013. № 1. С. 7-14.

139. Чернова О.А. Делопроизводство и режим секретности. Учебник. Москва: Кнорус, 2021 г., 242 с.

140. Чернышова Е.В., Тупицина С.С. Совершенствование системы документооборота организации / Е.В. Чернышева, С.С. Тупицина // Международный журнал гуманитарных и естественных наук. 2020. № 8 (47). С. 106-110.

141. Шайдуллина В.К. Большие дданные и защита персональных данных: основные проблемы теории и практики правового регулирования / В.К. Шайдуллина // Общество: политика, экономика, право. 2019. № 1 (66). С. 12-116.

142. Яппаров Р.М. Некоторые проблемы защиты конфиденциальной информации в системах электронного документооборота / Р.М. Яппаров // Вестник Уфимского юридического института МВД России. 2019. № 1 (83). С. 27-34.

ЭЛЕКТРОННЫЕ РЕСУРСЫ

143. Банк данных угроз безопасности информации ФСТЭК России [сайт]. Москва, 2015. URL: https://bdu.fstec.ru (дата обращения: 15.01.2021).

144. Государственное бюджетное учреждение Тюменской области «Государственный архив Тюменской области»: официальная страница на Портале Управления по делам архивов Тюменской области. Тюмень. URL: http://archiv.72to.ru/index.php/gosudarstvennyj-arkhiv-tyumenskoj-oblasti (дата обращения: 17.01.2020).

145. Разработчик средств информационной безопасности «Searchinform»: официальный сайт. URL: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/v-korporativnom-i-chastnom-sektore/v-korporativnom-i-chastnom-sektore/ (дата обращения 15.01.2021).

146. Справочно-правовая система КонсультантПлюс: официальный сайт. URL: http://www.consultant.ru (дата обращения 15.01.2021).

147. Федеральная служба по техническому и экспертному контролю Российской Федерации: официальный сайт. URL: http://fstec.ru (дата обращения 06.01.2021).

Приложение 1

Проект дополнений и изменений
в документ «Политика обработки персональных данных
в ГБУТО «Государственный госархив Тюменской области»»

УТВЕРЖДАЮ
Директор ГБУТО ГАТО
О.П. Тарасова
____ _____ 2021 г.

ПОЛИТИКА
обработки персональных данных
в Государственном бюджетном учреждении Тюменской области
«Государственный архив Тюменской области»

СОГЛАСОВАНО
протоколом заседания комиссии
ГБУТО ГАТО по защите информации
от_____ № ___

Тюмень
2021

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2. Блокирование персональных данных – временное прекращение обработки (за исключением случаев, если обработка необходима для уточнения персональных данных).

3. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

4. Конфиденциальность информации – субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

5. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

7. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими

лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

8. Персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

9. Представитель субъекта персональных данных – законный представитель субъекта:

- лицо, выступающее на основании доверенности, удостоверенной в установленном порядке;
- опекун, попечитель с представлением подтверждающего документа;
- родители несовершеннолетнего до 18 лет.

10. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

11. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

12. Субъект персональных данных (субъект) – резиденты РФ; физические лица (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и др.) (субъекты) состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (оператором).

13. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

14. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика обработки персональных данных (далее – Политика) Государственного бюджетного учреждения Тюменской области «Государственный госархив Тюменской области» (далее – госархив) составлена в соответствии с положениями статьи 18.1 Федерального закона от 27 июля 2007 г. № 152-ФЗ «О персональных данных» *и действует в случае обработки персональных данных субъектов персональных данных в информационных системах персональных данных госархива, размещённых в открытом доступе в сети Интернет.*

1.2. Целью Политики является предоставление субъектам персональных данных, чьи персональные данные обрабатываются в *информационных системах персональных данных госархива, размещённых в открытом доступе в сети Интернет, а также* информации, касающейся принципов и условий обработки персональных данных.

1.3. Госархив является оператором персональных данных. *Субъектами персональных данных являются следующие категории граждан, осуществляющие работу в информационных системах персональных данных госархива, размещённых в открытом доступе в сети Интернет:*

- сотрудники госархива;
- пользователи госархива.

1.4. *Обработка персональных данных осуществляется по адресу*: 625035, г. Тюмень, пр. Геологоразведчиков, д. 21/1.

1.5. Политика подлежит пересмотру в случае *изменения действующих или* появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, *и/или при изменении принципов обработки и защиты персональных данных в информационных системах персональных данных госархива, размещённых в открытом доступе в сети Интернет.*

1.6. *В случае необходимости пересмотра Политики, госархив разрабатывает обновлённую редакцию документа.* Новая редакция Политики вступает в силу с момента её подписания, *если иное не предусмотрено приказом о её утверждении. Старая Политика признаётся утратившей силу.*

1.7. Новая редакция Политики подлежит опубликованию на *официальной странице госархива Портала Управления по делам архивов Тюменской области (http://archiv.72to.ru/)* в течение 10 дней после её утверждения. *Старая редакция Политики с сайта удаляется.*

1.8. Актуальная версия Политики размещена без ограничений в доступе и доступна для ознакомления на *официальной странице госархива Портала Управления по делам архивов Тюменской области в разделе «Нормативные документы.*

1.9. Действующая редакция Политики хранится по адресу: 625035, г. Тюмень, пр. Геологоразведчиков, д. 21/1.

1.10. Заявления от субъектов персональных данных принимаются по адресу: 625035, г. Тюмень, пр. Геологоразведчиков, д. 21/1, а также на официальной электронной почте госархива: tumen_arhiv@mail.ru.

2. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Правовым основанием обработки персональных данных *в информационных системах персональных данных госархива, размещённых в открытом доступе в сети Интернет,* являются положения следующих правовых актов:

- Конституция Российской Федерации;
- Гражданский кодекс Российской Федерации;
- *Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;*
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

- Федеральный закон от 22.10.2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;
- Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ России № 416, ФСТЭК № 489 от 31 августа 2010 г. «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»;
- Устав ГБУТО «Государственный госархив Тюменской области»;
- Локальные акты госархива, регламентирующие отдельные вопросы работы с *информационными системами персональных данных госархива, размещёнными в открытом доступе в сети Интернет;*
- *Согласие на обработку персональных данных, данное при регистрации в информационных системах персональных данных госархива, размещённых в открытом доступе в сети Интернет*.

3. ЦЕЛИ СБОРА И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных производится госархивом в целях исполнения государственных услуг и осуществления государственных функций. Целями сбора и обработки персональных данных в информационных системах персональных данных госархива, размещённых в сети Интернет, для пользователей архивных документов являются – организация работы с документами архивного фонда Российской Федерации, другими архивными документами, не содержащими сведения, составляющие государственную тайну и справочно-поисковыми средствами к ним.

3.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей, *предусмотренных*

конкретной информационной системой персональных данных госархива, размещённой в сети Интернет. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4. ОБЪЁМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Содержание и объём обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.2. К категориям обрабатываемых персональных данных *субъектов*, обрабатываемых в госархиве, относятся:

- Фамилия, имя, отчество;
- Сведения об образовании *(категория образования, учёная степень, учёное звание);*
- *Место работы (учёбы) и должность;*
- Контактные данные *(контактный телефон, адрес электронной почты).*

5. ПОРЯДОК И ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Обработка персональных данных осуществляется госархивом с согласия субъекта персональных данных на обработку его персональных данных. *Полномочия должностных лиц госархива по осуществлению такой обработки определяются должностными инструкциями или самостоятельными приказами о возложении обязанностей.*

5.2. Госархив вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, *если иное не предусмотрено российским законодательством*. Поручение госархивом обработки

персональных данных другому лицу возможно с согласия субъекта персональных данных.

5.3. Обработка персональных данных в госархиве включает в себя выполнение следующих действий:

– сбор;
– запись;
– систематизация;
– накопление;
– хранение;
– уничтожение (обновление, изменение);
– извлечение;
– использование;
– передача (распространение, предоставление, доступ) ;
– обезличивание;
– блокирование;
– удаление;
– уничтожение.

5.4. При обработке персональных данных обеспечиваются точность таких данных, их достаточность, в необходимых случаях актуальность по отношению к целям обработки персональных данных.

5.5. Госархив принимает необходимые меры либо обеспечивает их выполнение в случаях возникновения необходимости удаления или уточнения неполных или неточных данных.

5.6. При сборе персональных данных госархив обеспечивает *обработку* персональных данных субъектов *с использованием информационных ресурсов, находящихся на территории Российской Федерации.* При обработке персональных данных *субъектов* трансграничная передача персональных данных не ведётся.

5.7. Хранение персональных данных осуществляется не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных не установлен федеральным законодательством или определён договором, стороной, выгодоприобретателем или поручителем по которому является субъект персональных данных.

5.8. Хранение персональных данных осуществляется непосредственно в конкретной информационной системе персональных данных госархива, размещённой в сети Интернет. Защита данных, хранящихся в информационной системе, осуществляется в соответствии с законодательством и гарантируется разработчиками такой системы.

5.9. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

- *иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;*
- *оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или иными федеральными законами;*
- *иное не предусмотрено иным соглашением между оператором и субъектом персональных данных.*

6. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Субъект персональных данных имеет право:

- требовать от госархива уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– принимать предусмотренные законом меры по защите своих прав.

6.2. Субъект персональных данных имеет право на получение от оператора, осуществляющего обработку его персональных данных, следующих сведений:

– подтверждение факта обработки персональных данных госархивом;
– правовые основания и цели обработки персональных данных;
– цели и применяемые госархивом способы обработки персональных данных;
– наименование и место нахождения госархива, сведения о лицах (за исключением работников госархива), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с госархивом или на основании федерального закона;
– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;
– сроки обработки персональных данных, в том числе сроки их хранения;
– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27 июля 2007 г. № 152-ФЗ «О персональных данных»;
– информацию об осуществленной или о предполагаемой трансграничной передаче данных;
– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению госархива, если обработка поручена или будет поручена такому лицу;
– иные сведения, предусмотренные Федеральным законом от 27 июля 2007 г. № 152-ФЗ «О персональных данных»» или другими федеральными законами.

6.3. Субъект персональных данных имеет право доступа к своим персональным данным *в следующих случаях*:

– при личном обращении к представителю госархива;
– при направлении письменного запроса, который должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие факт обработки персональных данных госархивом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных госархивом и собственноручную подпись субъекта персональных данных. Запрос может быть направлен в форме электронного документа и подписан электронной подписью;
– в случае если сведения об обработке персональных данных, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в госархив или направить повторный запрос в целях ознакомления со сведениями об обработке персональных данных, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, нормативным правовым актом или договором.

6.4. Если субъект персональных данных считает, что госархив осуществляет обработку его персональных данных с нарушением требований или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие госархива в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

6.5. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

7. ОБЯЗАННОСТИ ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе следующую информацию:

- *подтверждение факта обработки персональных данных госархивом;*
- *правовые основания и цели обработки персональных данных;*
- *цели и применяемые госархивом способы обработки персональных данных;*
- *наименование и место нахождения госархива, сведения о лицах (за исключением работников госархива), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с госархивом или на основании федерального закона;*
- *обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;*
- *сроки обработки персональных данных, в том числе сроки их хранения;*
- *порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27 июля 2007 г. № 152-ФЗ «О персональных данных»;*
- *информацию об осуществленной или о предполагаемой трансграничной передаче данных;*
- *наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению госархива, если обработка поручена или будет поручена такому лицу;*

- *иные сведения, предусмотренные Федеральным законом от 27 июля 2007 г. № 152-ФЗ «О персональных данных»» или другими федеральными законами.*

7.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законодательством либо с требованиями информационной системы персональных данных госархива, размещённой в открытом доступе в сети Интернет, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

7.3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных пунктом 7.4 настоящей Политики, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

- *наименование либо фамилия, имя, отчество и адрес оператора или его представителя;*
- *цель обработки персональных данных и ее правовое основание;*
- *предполагаемые пользователи персональных данных;*
- *установленные настоящим Федеральным законом права субъекта персональных данных;*
- *источник получения персональных данных.*

7.4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные пунктов 7.3 настоящей Политики, в случаях, если:

- *субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;*
- *персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;*

- *обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 «Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения» Федерального закона «О персональных данных»;*
- *оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;*
- *предоставление субъекту персональных данных сведений, предусмотренных пунктом 7.3 настоящей Политики, нарушает права и законные интересы третьих лиц.*

7.5. При сборе персональных данных оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона «О персональных данных».

Администратор информационной безопасности вычислительной сети ОИПСиЗИ Е.Ю. Дроздова

__ _____ 2021 г.

Приложение 2

Проект документа «Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» в ГБУТО «Государственный архив Тюменской области»»

УТВЕРЖДАЮ
Директор ГБУТО ГАТО
О.П. Тарасова
____ _____ 2021 г.

ЧАСТНАЯ МОДЕЛЬ УГРОЗ
безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» в ГБУТО «Государственный архив Тюменской области»

СОГЛАСОВАНО
протоколом заседания комиссии
ГБУТО ГАТО по защите информации
от_____ № ___

Тюмень
2021

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вероятность (частота) реализации угрозы – определяемый экспертным путём показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности персональных данных для данной информационной системы персональных данных в складывающихся условиях обстановки.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных – 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.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и(или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие

описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное,

имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее – модель угроз) содержит систематизированный перечень угроз безопасности персональных данных при осуществлении их обработки в ГБУТО «Государственный архив Тюменской области» (далее – архив) в корпоративной информационной системе «Бухгалтерия».

Угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных, которое ведёт к ущербу жизненно важных интересов личности, общества и государства.

Модель угроз безопасности персональных данных при их обработке в информационной системе «Бухгалтерия» разработана с учётом требований следующих нормативных документов:

- Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ - Глава 14 «Защита персональных данных работника»;
- Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;
- Указ Президента Российской Федерации от 06 марта 1997 № 188 «Об утверждении перечня сведений конфиденциального характера;
- Постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

- Постановление Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.

Модель угроз содержит единые исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационных системах персональных данных, связанным:

- с перехватом (съёмом) персональных данных по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в информационные системы персональных данных с целью изменения, копирования, неправомерного распространения персональных данных или деструктивных воздействий на элементы информационных систем персональных данных и обрабатываемых в них персональных данных с использованием программных и программно-аппаратных средств, с целью уничтожения или блокирования персональных данных.

С применением модели угроз решаются следующие задачи:

- анализ защищенности информационных систем персональных данных от угроз безопасности персональных данных в ходе организации и выполнения работ по обеспечению безопасности персональных данных в архиве;

- разработка системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем персональных данных;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства информационных систем персональных данных архива, в результате которого может быть нарушено их функционирование;
- контроль обеспечения уровня защищенности персональных данных в архиве.

Информационная система персональных данных представляет собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке персональных данных.

Основными элементами информационной системы персональных данных являются:

- персональные данные, содержащиеся в базах данных, как совокупность информации и её носителей, используемых в информационных системах персональных данных;
- информационные технологии, применяемые при обработке персональных данных;
- технические средства, осуществляющие обработку персональных данных (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки персональных данных, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования

документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации) (далее – технические средства информационных систем персональных данных);

- программные средства (операционные системы, системы управления базами данных и т.п.);
- средства защиты информации;
- вспомогательные технические средства и системы – технические средства и системы, их коммуникации, не предназначенные для обработки персональных данных, но размещенные в помещениях (далее – служебные помещения), в которых расположены Информационных систем персональных данных, их технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электрочасофикации).

Угрозы безопасности персональных данных, обрабатываемых в информационных системах персональных данных архива, содержащиеся в настоящей модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угрозы безопасности персональных данных в информационных системах персональных данных.

Модель угроз подлежит пересмотру по решению оператора на основе проведённых анализа и оценки угроз безопасности персональных данных с учётом особенностей и изменений конкретной информационной системы, а также по результатам мероприятий по контролю за выполнением требований к

обеспечению безопасности персональных данных при их обработке в информационной системе.

1. КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Состав и содержание угроз безопасности персональных данных определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, обрабатываемым в архиве. Совокупность таких условий и факторов формируется с учётом характеристик информационных систем персональных данных, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

К характеристикам информационных систем персональных данных, обусловливающим возникновение угроз безопасности персональных данных, можно отнести категорию и объём персональных данных обрабатываемых в информационных системах, структуру таких систем, наличие подключений информационных систем персональных данных к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности персональных данных, обрабатываемых в информационных системах персональных данных, режимы обработки персональных данных, режимы разграничения прав доступа пользователей информационных систем, местонахождение и условия размещения технических средств информационных систем персональных данных.

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются персональные данные, и определяются при оценке возможности реализации угроз безопасности персональных данных.

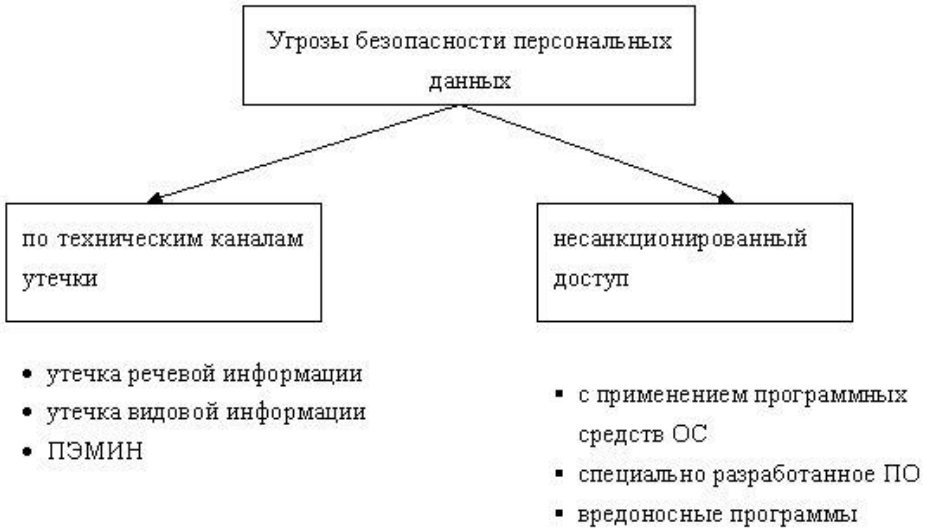
Возможности источников угроз безопасности персональных данных обусловлены совокупностью способов несанкционированного и (или) случайного доступа к персональным данным, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) персональных данных.

Угроза безопасности персональных данных реализуется в результате образования канала реализации угроз безопасности персональных данных между источником угрозы и носителем (источником) персональных данных, что создает условия для нарушения безопасности персональных данных (несанкционированный или случайный доступ).

Основными элементами канала реализации угроз безопасности персональных данных (рисунок 1) являются:

- источник угроз безопасности персональных данных – субъект, материальный объект или физическое явление, создающие угроз безопасности персональных данных;
- среда (путь) распространения персональных данных или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) персональных данных;
- носитель персональных данных – физическое лицо или материальный объект, в том числе физическое поле, в котором персональных данных находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Рисунок 1



Обобщенная схема канала реализации угроз безопасности персональных данных

В целях формирования систематизированного перечня угроз безопасности персональных данных при их обработке в информационных системах персональных данных и разработке на их основе частных моделей применительно к конкретному виду информационных систем угрозы классифицируются в соответствии со следующими признаками:

- по виду защищаемой от угроз безопасности персональных данных информации, содержащей персональные данные;
- по видам возможных источников угроз безопасности персональных данных;
- по типу информационных систем персональных данных, на которые направлена реализация угроз безопасности персональных данных;
- по способу реализации угроз безопасности персональных данных;
- по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с персональными данными);
- по используемой уязвимости;
- по объекту воздействия.

По видам возможных источников угроз безопасности персональных данных выделяются следующие классы угроз:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к информационным системам персональных данных, включая пользователей информационных систем персональных данных, реализующих угрозы непосредственно в таких системах (внутренний нарушитель);
- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к информационным системам персональных данных, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

По типу информационных систем персональных данных, на которые направлена реализация угроз безопасности персональных данных, выделяются следующие классы угроз:

- угрозы безопасности персональных данных, обрабатываемых в информационных системах персональных данных на базе автономного автоматизированного рабочего места;
- угрозы безопасности персональных данных, обрабатываемых в информационных системах на базе автоматизированного рабочего места, подключенного к сети общего пользования (к сети международного информационного обмена);
- угрозы безопасности персональных данных, обрабатываемых в информационных системах на базе локальных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);
- угрозы безопасности персональных данных, обрабатываемых в информационных системах на базе локальных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена);

- угрозы безопасности персональных данных, обрабатываемых в информационных системах на базе распределенных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);
- угрозы безопасности персональных данных, обрабатываемых в информационных системах на базе распределённых информационных систем с подключением к сети общего пользования (к сети международного информационного обмена).

По способам реализации угроз безопасности персональных данных выделяются следующие классы угроз:

- угрозы, связанные с несанкционированным доступом к персональным данным (в том числе угрозы внедрения вредоносных программ);
- угрозы утечки персональных данных по техническим каналам утечки информации;
- угрозы специальных воздействий на информационные системы персональных данных.

По виду несанкционированных действий, осуществляемых с персональными данными, выделяются следующие классы угроз:

- угрозы, приводящие к нарушению конфиденциальности персональных данных (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;
- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение персональных данных или их уничтожение;
- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы информационной системы персональных данных «Бухгалтерия», в результате которого осуществляется блокирование персональных данных.

По используемой уязвимости выделяются следующие классы угроз:

- угрозы, реализуемые с использованием уязвимости системного программного обеспечения;
- угрозы, реализуемые с использованием уязвимости прикладного программного обеспечения;
- угрозы, возникающие в результате использования уязвимости, вызванной наличием в автоматизированной системе аппаратной закладки;
- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации средств защиты информации от несанкционированного доступа;
- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;
- угрозы, реализуемые с использованием уязвимостей средств защиты информации.

По объекту воздействия выделяются следующие классы угроз:

- угрозы безопасности персональных данных, обрабатываемых на автоматизированном рабочем месте;
- угрозы безопасности персональных данных, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);
- угрозы безопасности персональных данных, передаваемых по сетям связи;
- угрозы прикладным программам, с помощью которых обрабатываются персональные данные;
- угрозы системному программному обеспечению, обеспечивающему функционирование информационных систем персональных данных.

Реализация одной из угроз безопасности персональных данных перечисленных классов или их совокупности может привести к следующим типам последствий для субъектов персональных данных:

- значительным негативным последствиям для субъектов персональных данных;
- негативным последствиям для субъектов персональных данных;
- незначительным негативным последствиям для субъектов персональных данных.

2. ХАРАКТЕРИСТИКА УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Угрозы утечки персональных данных по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки персональных данных.

Основными элементами описания угроз утечки информации по техническим каналам являются: источник угрозы, среда (путь) распространения информативного сигнала и носитель защищаемой информации.

Источниками угроз утечки информации по техническим каналам являются физические лица, не имеющие доступа к информационным системам персональных данных, а также зарубежные спецслужбы или организации (в том числе конкурирующие или террористические), криминальные группировки, осуществляющие перехват (съем) информации с использованием технических средств её регистрации, приёма или фотографирования.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником. Среда распространения может быть как

однородной (например, только воздушной), так и неоднородной за счет перехода сигнала из одной среды в другую (например, в результате акустоэлектрических или виброакустических преобразований).

Носителем персональных данных является пользователь информационных систем персональных данных, осуществляющий голосовой ввод персональных данных в информационные системы, акустическая система информационных систем персональных данных, воспроизводящая персональные данные, а также технические средства информационных систем и вспомогательные технические средства и системы, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

При обработке персональных данных в информационных системах персональных данных за счет реализации технических каналов утечки информации возможно возникновение следующих угроз безопасности персональных данных:

- угроза утечки акустической (речевой) информации;
- угроза утечки видовой информации;
- угроза утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Носители персональных данных могут содержать информацию, представленную в следующих видах:

- акустическая (речевая) информация, содержащаяся непосредственно в произносимой речи пользователя информационных систем персональных данных при осуществлении им функции голосового ввода персональных данных в информационных системах персональных данных, либо воспроизводимая акустическими средствами этих систем (если такие функции предусмотрены технологией обработки персональных данных), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

- видовая информация, представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационных систем персональных данных;
- информация, обрабатываемая (циркулирующая) в информационных системах персональных данных, в виде электрических, электромагнитных, оптических сигналов;
- информация, обрабатываемая в информационных системах персональных данных, представленная в виде бит, байт, файлов и других логических структур.

2.2. УГРОЗЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Угрозы, связанные с несанкционированным доступом, представляются в виде совокупности обобщенных классов возможных источников угроз, уязвимостей программного и аппаратного обеспечения информационных систем персональных данных, способов реализации угроз, объектов воздействия (носителей защищаемой информации, директориев, каталогов, файлов с персональных данных или самих персональных данных) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью:

угроза несанкционированного доступа: = <источник угрозы>, <уязвимость программного или аппаратного обеспечения>, <способ реализации угрозы>, <объект воздействия>, <несанкционированный доступ>.

Угрозы несанкционированного доступа в информационные системы персональных данных архива с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного, доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное

распространение), целостности (уничтожение, изменение) и доступности (блокирование) персональных данных, и включают в себя:

- угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программно-математического воздействия).

Возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для несанкционированного доступа в операционную среду компьютера, в том числе путём формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду информационных систем персональных данных с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Эти угрозы реализуются относительно информационных систем персональных данных как на базе автоматизированного рабочего места, не включенного в сети связи общего пользования, так и применительно ко всем Информационных систем персональных данных, имеющим подключение

к сетям связи общего пользования и сетям международного информационного обмена.

Описание угроз доступа (проникновения) в операционную среду компьютера формально может быть представлено следующим образом:

угроза несанкционированного доступа в информационные системы персональных данных: = <источник угрозы>, <уязвимость информационных систем персональных данных>, <способ реализации угрозы>, <объект воздействия (программа, протокол, данные и др.)>, <деструктивное действие>.

Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств – это угрозы «Отказа в обслуживании». Как правило, данные угрозы рассматриваются применительно к информационным системам персональных данных на базе локальных и распределённых информационных систем вне зависимости от подключения информационного обмена. Их реализация обусловлена тем, что при разработке системного или прикладного программного обеспечения не учитывается возможность преднамеренных действий по целенаправленному изменению:

- содержания служебной информации в пакетах сообщений, передаваемых по сети;
- условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);
- форматов представления данных (с несоответствием измененных форматов, установленных для обработки по протоколам сетевого взаимодействия);
- программного обеспечения обработки данных.

В результате реализации угрозы «Отказ в обслуживании» происходит переполнение буферов и блокирование процедур обработки, «зацикливание» процедур обработки и «зависание» компьютера, отбрасывание пакетов сообщений и др. Описание таких угроз формально может быть представлено следующим образом:

угроза «Отказа в обслуживании» = <источник угрозы>, <уязвимость информационных систем персональных данных>, <способ реализации угрозы>, <объект воздействия (носитель персональных данных)>, <непосредственный результат реализации угрозы (переполнение буфера, блокирование процедуры обработки, «зацикливание» обработки и т.п.)>.

угроза программно-математического воздействия в информационных системах персональных данных: = <класс вредоносной программы (с указанием среды обитания)>, <источник угрозы (носитель вредоносной программы)>, <способ инфицирования>, <объект воздействия (загрузочный сектор, файл и т.п.)>, <описание возможных деструктивных действий>,<дополнительная информация об угрозе (резидентность, скорость распространения, полиморфичность и др.)>.

Ниже дается общая характеристика источников угроз безопасности информации, уязвимостей, которые могут быть использованы при реализации угроз НСД, и характеристика результатов несанкционированного или случайного доступа. Характеристика способов реализации угроз дается при описании угроз доступа (проникновения) в операционную среду компьютера, угроз отказа в обслуживании и угроз программно-математического воздействия.

Источниками угроз несанкционированного доступа в информационных системах персональных данных архива могут быть:

- нарушитель;
- носитель вредоносной программы;
- аппаратная закладка.

По наличию права постоянного или разового доступа в контролируемую зону и к информационным системам персональных данных нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к информационных системам персональных данных, реализующие угрозы из внешних сетей связи

общего пользования и (или) сетей международного информационного обмена, – внешние нарушители;

– нарушители, имеющие доступ к информационных системам персональных данных, включая пользователей таких систем, реализующие угрозы непосредственно в информационных системах персональных данных, – внутренние нарушители.

Внешними нарушителями могут быть:

– разведывательные службы государств;
– криминальные структуры;
– конкуренты (конкурирующие организации);
– недобросовестные партнеры;
– внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

– осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
– осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
– осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
– осуществлять несанкционированный доступ через элементы информационной инфраструктуры информационных систем персональных данных, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;

– осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к Информационных систем персональных данных.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к персональным данным и контролю за порядком проведения работ.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к персональным данным.

Реализация угроз несанкционированного доступа к информации может приводить к следующим видам нарушения её безопасности:

1. Нарушение конфиденциальности (копирование, неправомерное распространение);
2. Нарушение целостности (уничтожение, изменение) информации в информационной системе персональных данных может также быть вызвано внедрением в неё вредоносной программы программно-аппаратной закладки или воздействием на систему защиты информации или её элементы.

В информационной системе персональных данных возможно воздействие на технологическую сетевую информацию, которая может обеспечивать функционирование различных средств управления вычислительной сетью:

– конфигурацией сети;
– адресами и маршрутизацией передачи данных в сети;
– функциональным контролем сети;
– безопасностью информации в сети.

Нарушение доступности (блокирование) информации обеспечивается путём формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват

(загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры.

Указанные действия могут привести к нарушению или отказу функционирования технических средств информационной системы персональных данных:

- средств обработки информации;
- средств ввода/вывода информации;
- средств хранения информации;
- аппаратуры и каналов передачи;
- средств защиты информации.

Под уровнем технической подготовленности понимается степень технических навыков и знаний, а также технические ресурсы и средства, которые нарушитель может задействовать для достижения поставленной цели.

Нарушителями безопасности персональных данных при их обработке в информационной системе персональных данных могут быть следующие категории лиц, представленные в таблице 1.

Таблица 1

Обобщённая характеристика нарушителей

Шифр	**Описание**	**Возможности**	**Уровень знаний об объектах атак**	**Уровень техни-ческой подго-товлен-ности**
Внутренние нарушители				
К1	Лица, имеющие санкционированный доступ к информационной системе персональных данных, но не имеющие доступа к персональным данным (должностные лица, обеспечивающие нормальное функционирование информационной системы персональных данных).	– наличие доступа к фрагментам информации, содержащей персональные данные и распространяющейся по внутренним каналам связи информационной системе персональных данных; – может располагать фрагментами информации о топологии информационной системе персональных данных (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; – может располагать именами и вести выявление паролей зарегистрированных пользователей; – может изменять конфигурацию технических средств информационной системе персональных данных, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам информационной системе персональных данных.	Низкий	Низкий
К2	Зарегистрированные пользователи информационной системы персональных данных, осуществляющие ограниченный доступ к ресурсам информационной системы персональных данных с рабочего места.	– обладает всеми возможностями лиц предыдущей категории; – знает, по меньшей мере, одно легальное имя доступа; – обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству персональных данных; – располагает конфиденциальными данными, к которым имеет доступ.	Высокий	Низкий

К3	Зарегистрированные пользователи информационной системы персональных данных, осуществляющие удаленный доступ к ресурсам информационной системы персональных данных по локальным и (или) распределенным информационным системам.	– обладает всеми возможностями лиц предыдущей категории; – располагает информацией о топологии информационной системы персональных данных на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств информационной системы персональных данных; – имеет возможность прямого (физического) доступа к фрагментам технических средств информационной системы персональных данных.	Не актуальна, т.к. возможность удаленного доступа отсутствует	Не актуальна, т.к. возможность удаленного доступа отсутствует
К4	Зарегистрированные пользователи с полномочиями системного администратора информационной системы персональных данных	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении информационной системы персональных данных; – обладает полной информацией о технических средствах и конфигурации информационной системы персональных данных; – имеет доступ ко всем техническим средствам обработки информации и данным информационной системы персональных данных; – обладает правами конфигурирования и административной настройки технических средств информационной системы персональных данных	Высокий	Средний

К5	Зарегистрированные пользователи информационной системы персональных данных с полномочиями администратора безопасности сегмента (фрагмента) информационной системы персональных данных	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) информационной системы персональных данных; – обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) информационной системы персональных данных; – имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) информационной системы персональных данных; – имеет доступ ко всем техническим средствам сегмента (фрагмента) информационной системы персональных данных; – обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) информационной системы персональных данных.	Средний	Высокий
К6	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	– обладает информацией об алгоритмах и программах обработки информации на информационной системе персональных данных; – обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение информационной системы персональных данных на стадии ее разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии информационной системы персональных данных и технических средствах обработки и защиты персональных данных, обрабатываемых в информационной системе персональных данных.	Низкий	Высокий

К7	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств информационной системы персональных данных	– обладает возможностями внесения закладок в технические средства информационной системы персональных данных на стадии их разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии информационной системы персональных данных и технических средствах обработки и защиты информации в информационной системы персональных данных.		
Внешние нарушители				
К8	Физические и юридические лица, желающие заполучить доступ к конфиденциальной информации с целью извлечения выгоды - лица, не имеющие доступа к информационной системе персональных данных, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (конкуренты, недобросовестные партнеры, внешние субъекты (физические лица) и др.).	– может осуществлять несанкционированный доступ к каналам связи, выходящим за пределы контролируемой зоны; – может осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена; – может осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок; – может осуществлять несанкционированный доступ через элементы информационной инфраструктуры информационной системе персональных данных, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны; – может осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к информационной системе персональных данных. – может осуществлять перехват информации по техническим каналам утечки информации; – может осуществлять несанкционированный доступ с помощью методов социальной инженерии; – может осуществлять совместные действия с лицами, имеющими доступ к информационной системе персональных данных.	Низкий	Низкий

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве её носителя рассматриваются:

- отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый винчестер и т.п.;
- встроенные носители информации (винчестеры, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок, – видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);
- микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то её носителями являются:

- пакеты передаваемых по компьютерной сети сообщений;
- файлы (текстовые, графические, исполняемые и т.д.).

3. ОБЩАЯ ХАРАКТЕРИСТИКА УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ «БУХГАЛТЕРИЯ»

Уязвимость информационной системы персональных данных – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным.

Причинами возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;
- неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
- несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Основные группы уязвимостей информационных систем персональных данных включают:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

3.1. ОБЩАЯ ХАРАКТЕРИСТИКА УЯЗВИМОСТЕЙ СИСТЕМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем. При этом возможны уязвимости:

- в микропрограммах, в прошивках запоминающих устройств;
- в средствах операционной системы, предназначенных для управления локальными ресурсами информационных систем персональных данных (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;
- в средствах операционной системы, предназначенных для выполнения вспомогательных функций, – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиках и т.п.), программах предоставления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.д.);
- в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах операционной системы, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ («дыры», «люки»), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;

- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др. Краткая характеристика этих уязвимостей применительно к протоколам приведена в таблице 2.

Таблица 2

Уязвимости отдельных протоколов TCP/IP

Наименование протокола	Уровень стека протоколов	Наименование(характеристика) уязвимости	Содержание нарушения безопасности информации
FTP (File Transfer Protocol) – протокол передачи файлов по сети	Прикладной, представительный, сеансовый	1. Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) 2. Доступ по умолчанию 3. Наличие двух открытых портов	Возможность перехвата данных учетной записи (имен зарегистрированных пользователей, паролей). Получение удаленного доступа к хостам
telnet – протокол управления удаленным терминалом	Прикладной, представительный, сеансовый	Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде)	Возможность перехвата данных учетной записи пользователя. Получение удаленного доступа к хостам
UDP – протокол передачи данных без установления соединения	Транспортный	Отсутствие механизма предотвращения перегрузок буфера	Возможность реализации UDP-шторма. В результате обмена пакетами происходит существенное снижение производительности сервера
ARP – протокол преобразования IP-адреса в физический адрес	Сетевой	Аутентификация на базе открытого текста (информация пересылается в незашифрованном виде)	Возможность перехвата трафика пользователя злоумышленником
RIP – протокол маршрутной информации	Транспортный	Отсутствие аутентификации управляющих сообщений об изменении маршрута	Возможность перенаправления трафика через хост злоумышленника
TCP – протокол управления передачей	Транспортный	Отсутствие механизма проверки корректности заполнения служебных заголовков пакета	Существенное снижение скорости обмена и даже полный разрыв произвольных соединений по протоколу TCP

DNS – протокол установления соответствия мнемонических имен и сетевых адресов	Прикладной, представительный, сеансовый	Отсутствие средств проверки аутентификации полученных данных от источника	Фальсификация ответа DNS-сервера
IGMP – протокол передачи сообщений о маршрутизации	Сетевой	Отсутствие аутентификации сообщений об изменении параметров маршрута	Зависание систем Win 9x/NT/200
SMTP – протокол обеспечения сервиса доставки сообщений по электронной почте	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность подделывания сообщений электронной почты, а также адреса отправителя сообщения
SNMP – протокол управления маршрутизаторами в сетях	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность переполнения пропускной способности сети

К прикладному программному обеспечению относятся прикладные программы общего пользования и специальные прикладные программы. Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т.п.), системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т.п.

Специальные прикладные программы – это программы, которые разрабатываются в интересах решения конкретных прикладных задач в информационной системе персональных данных (в том числе программные средства защиты информации, разработанные для конкретной системы).

Уязвимости прикладного программного обеспечения могут представлять собой:

- функции и процедуры, относящиеся к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду информационных систем персональных данных и вызова штатных функций операционной системы, выполнения несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ («дыры», «люки»), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в операционной системе;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений,

блокирования несанкционированно модифицированных функций и т.п.);

- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

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

- к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) информационных систем персональных данных, с возможностью перехвата управления загрузкой операционной системы и получением прав доверенного пользователя;
- в операционную среду, то есть в среду функционирования локальной операционной системы отдельного технического средства информационной системы персональных данных с возможностью выполнения несанкционированного доступа путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;
- в среду функционирования прикладных программ (например, к локальной системе управления базами данных);
- непосредственно к информации пользователя (к файлам, текстовой, аудио- и графической информации, полям и записям в электронных базах данных) с возможностью нарушения её конфиденциальности, целостности и доступности.

Угрозы могут быть реализованы в случае получения физического доступа к информационным системам персональных данных или к средствам

ввода информации в такие системы. По условиям реализации угрозы доступа (проникновения) в операционную среду подразделяются на три группы.

Первая группа включает в себя угрозы безопасности информации, реализуемые в ходе загрузки операционной системы. Такие угрозы направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации для получения несанкционированного доступа в операционную среду информационных систем персональных данных. Такие угрозы реализуются с использованием отчуждаемых носителей информации.

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

- программами просмотра и модификации реестра;
- программами поиска текстов в текстовых файлах по ключевым ловам и копирования;
- специальными программами просмотра и копирования записей в базах данных;
- программами быстрого просмотра графических файлов, их редактирования или копирования;
- программами поддержки возможностей реконфигурации программной среды (настройки информационных систем персональных данных в интересах нарушителя) и др.

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

Если информационная система персональных данных реализована на базе локальной или распределенной информационной системы, то в ней могут быть реализованы угрозы безопасности информации путём использования протоколов межсетевого взаимодействия. При этом может обеспечиваться несанкционированный доступ к персональным данным или реализовываться угроза отказа в обслуживания. Особенно опасны угрозы, когда информационные системы персональных данных представляет собой распределённую информационную систему, подключенную к сетям общего пользования и (или) сетям международного информационного обмена. В её основу положено семь первичных признаков классификации, указанных в таблице 3.

Таблица 3

Первичные признаки классификации угроз информационной системы персональных данных

Характер угрозы	Пассивная угроза	угроза, при реализации которой не оказывается непосредственное влияние на работу информационных систем персональных данных, но могут быть нарушены установленные правила разграничения доступа к персональным данным или сетевым ресурсам. Примером таких угроз является угроза «Анализ сетевого трафика», направленная на прослушивание каналов связи и перехват передаваемой информации
	Активная угроза	угроза, связанная с воздействием на ресурсы Информационных систем персональных данных, при реализации которой оказывается непосредственное влияние на работу системы (изменение конфигурации, нарушение работоспособности и т.д.), и с нарушением установленных правил разграничения доступа к персональных данных или сетевым ресурсам. Примером таких угроз является угроза «Отказ в обслуживании», реализуемая как «шторм TCP-запросов
Цель реализации угрозы	Такие угрозы могут быть направлены на нарушение конфиденциальности, целостности и доступности информации (в том числе на нарушение работоспособности информационной системы персональных данных или её элементов)	
Условие начала осуществления процесса реализации угрозы	По этому признаку может реализовываться угроза: – по запросу от объекта, относительно которого реализуется угроза. В этом случае нарушитель ожидает передачи запроса определенного типа, который и будет условием начала осуществления несанкционированного доступа; – по наступлению ожидаемого события на объекте, относительно которого реализуется угроза. В этом случае нарушитель осуществляет постоянное наблюдение за состоянием операционной системы информационной системы персональных данных и при возникновении определенного события в этой системе начинает несанкционированный доступ; – безусловное воздействие. В этом случае начало осуществления несанкционированного доступа безусловно по отношению к цели доступа, то есть угроза реализуется немедленно и безотносительно к состоянию системы	

Наличие обратной связи с информационной системой персональных данных	По этому признаку процесс реализации угрозы может быть с обратной связью и без обратной связи. Угроза, осуществляемая при наличии обратной связи с информационной системой персональных данных, характеризуется тем, что на некоторые запросы, переданные в систему, нарушителю требуется получить ответ. Следовательно, между нарушителем и информационной системой персональных данных существует обратная связь, которая позволяет нарушителю адекватно реагировать на все изменения, происходящие в информационной системе. В отличие от угроз, реализуемых при наличии обратной связи с информационной системой персональных данных, при реализации угроз без обратной связи не требуется реагировать на какие-либо изменения, происходящие в информационной системе
Расположение нарушителя относительно информационной системы персональных данных	В соответствии с этим признаком угроза реализуется как внутрисегментно, так и межсегментно. Сегмент сети – физическое объединение хостов (технических средств информационной системы персональных данных или коммуникационных элементов, имеющих сетевой адрес). Например, сегмент информационной системы образует совокупность хостов, подключенных к серверу по схеме «общая шина». В случае, когда имеет место внутрисегментная угроза, нарушитель имеет физический доступ к аппаратным элементам информационной системы персональных данных. Если имеет место межсегментная угроза, то нарушитель располагается вне информационной системы персональных данных, реализуя угрозу из другой сети или из другого сегмента информационной системы
Уровень эталонной модели взаимодействия открытых систем (ISO/OSI), на котором реализуется угроза	По этому признаку угроза может реализовываться на физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном уровне модели ISO/OSI
Соотношение количества нарушителей и элементов информационной системы персональных данных, относительно которых реализуется угроза	По этому признаку угроза может быть отнесена к классу угроз, реализуемых одним нарушителем относительно одного технического средства Информационных систем персональных данных (угроза «один к одному»), сразу относительно нескольких технических средств информационной системы персональных данных (угроза «один ко многим») или несколькими нарушителями с разных компьютеров относительно одного или нескольких технических средств информационной системы персональных данных (распределенные или комбинированные угрозы).

С учётом проведенной классификации выделяются восемь наиболее часто реализуемых угроз, перечисленных в таблице 4.

Таблица 4

Угрозы несанкционированного доступа к информационной системе персональных данных

Анализ сетевого трафика	Реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель изучает логику работы сети, в целях получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. Это позволяет злоумышленнику на основе применения соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней, перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающим шифрование), её подмены, модификации и т.п.
Сканирование сети	Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов информационной системы персональных данных и анализе ответов от них. Целью является выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей
Угроза выявления пароля	Цель реализации угрозы состоит в получении несанкционированного доступа путём преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа

Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа	Угроза эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу. Существуют две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.	Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений
		Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных
Навязывание ложного маршрута сети	Реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности, из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе информационной системы персональных данных. Реализация угрозы основывается на несанкционированном использовании протоколов маршрутизации и управления сетью для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение	
Внедрение ложного объекта сети	Основан на использовании недостатков алгоритмов удаленного поиска. В случае, если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска, заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети	

Отказ в обслуживании	Основан на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты. Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к персональным данным в информационной системе персональных данных, передача с одного адреса такого количества запросов на подключение к техническому средству в составе Информационных систем персональных данных, какое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полную остановку компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов	К разновидностям таких угроз относятся: – скрытый отказ в обслуживании, вызванный привлечением части ресурсов информационной системы персональных данных на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований ко времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу; – явный отказ в обслуживании, вызванный исчерпанием ресурсов информационной системы персональных данных при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam); – явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами информационной системы персональных данных при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих

		к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации; – явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Удаленный запуск приложений	Угроза заключается в стремлении запустить на хосте информационной системы персональных данных различные предварительно внедрённые вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых – нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др. Выделяют три подкласса данных угроз: – распространение файлов, содержащих несанкционированный исполняемый код; – удаленный запуск приложения путем переполнения буфера приложений-серверов; – удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами.	Типовые угрозы первого подкласса основываются на активизации распространяемых файлов при случайном обращении к+ ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в виде макрокоманд (документы Microsoft Word, Excel и т.п.); html-документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы
		При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля переполнения буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение вируса-червя Морриса
		При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими») либо штатными средствами управления и администрирования компьютерных сетей. В результате их использования удается добиться удаленного контроля над станцией в сети.

Возможные последствия реализации угроз различных классов представлены в Таблице 5.

Таблица 5

Последствия реализации угроз несанкционированного доступа к информационной системе персональных данных

№ п/п	Тип атаки	Возможные последствия	
1	Анализ сетевого трафика	Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей	
2	Сканирование сети	Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей	
3	«Парольная» атака	Выполнение любого деструктивного действия, связанного с получением несанкционированного доступа	
4	Подмена доверенного объекта сети	Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации	
5	Навязывание ложного маршрута	Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений	
6	Внедрение ложного объекта сети	Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации	
7	Отказ в обслуживании	Частичное исчерпание ресурсов	Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений
		Полное исчерпание ресурсов	Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения. Отказ в предоставлении сервиса (электронной почты, файлового и т.д.)
		Нарушение логической связности между атрибутами, данными, объектами	Невозможность передачи, сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т.п.
		Использование ошибок в программах	Нарушение работоспособности сетевых устройств

8	Удаленный запуск приложений	Путем рассылки файлов, содержащих деструктивный исполняемый код, вирусное заражение	Нарушение конфиденциальности, целостности, доступности информации
		Путем переполнения буфера серверного приложения	
		Путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами	Скрытое управление системой

Процесс реализации угрозы в общем случае состоит из четырех этапов:

– сбора информации;
– вторжения (проникновения в операционную среду);
– осуществления несанкционированного доступа;
– ликвидации следов несанкционированного доступа.

На этапе сбора информации нарушителя могут интересовать различные сведения об информационной системе персональных данных, в том числе:

а) о топологии сети, в которой функционирует система. При этом может исследоваться область вокруг сети (например, нарушителя могут интересовать адреса доверенных, но менее защищенных хостов). Если информационная система персональных данных находится за межсетевым экраном, возможен сбор информации о конфигурации такого экрана и о топологии информационной системы персональных данных за межсетевым экраном, в том числе путем посылки пакетов на все порты всех предполагаемых хостов внутренней (защищаемой) сети;

б) о типе операционной системы в информационной системе персональных данных;

в) о функционирующих сервисах.

На этапе вторжения исследуется наличие типовых уязвимостей в системных сервисах или ошибок в администрировании системы. Успешным результатом использования уязвимостей является получение процессом нарушителя привилегированного режима выполнения (доступа к привилегированному режиму выполнения командного процессора), внесение в систему учетной записи незаконного пользователя, получение файла паролей или нарушение работоспособности атакуемого хоста.

Угрозы, реализуемые на этапе вторжения, формируются на сетевом, транспортном или прикладном уровне в зависимости от используемого механизма вторжения.

К типовым угрозам, реализуемым на сетевом и транспортном уровнях, относятся:

- угроза, направленная на подмену доверенного объекта;
- угроза, направленная на создание в сети ложного маршрута;
- угрозы, направленные на создание ложного объекта с использованием недостатков алгоритмов удаленного поиска;
- угрозы типа «отказ в обслуживании», основанные на IP-дефрагментации, на формировании некорректных ICMP-запросов (например, атака «Ping of Death» и «Smurf»), на формировании некорректных TCP-запросов (атака «Land»), на создании «шторма» пакетов с запросами на соединение (атаки «SYN Flood») и др.

К типовым угрозам, реализуемым на прикладном уровне, относятся угрозы, направленные на несанкционированный запуск приложений, угрозы, реализация которых связана с внедрением программных закладок (типа «троянский конь»), с выявлением паролей доступа в сеть или к определенному хосту и т.д.

Если реализация угрозы не принесла нарушителю наивысших прав доступа в системе, возможны попытки расширения этих прав до максимально возможного уровня. Для этого могут использоваться уязвимости не только сетевых сервисов, но и уязвимости системного программного обеспечения хостов Информационных систем персональных данных.

На этапе реализации несанкционированного доступа осуществляется достижение цели реализации угрозы:

- нарушение конфиденциальности (копирование, неправомерное распространение);
- нарушение целостности (уничтожение, изменение);
- нарушение доступности (блокирование).

На этом же этапе, после указанных действий, формируется «черный вход» в виде одного из сервисов (демонов), обслуживающих некоторый порт и выполняющих команды нарушителя. «Чёрный вход» оставляется в системе в интересах обеспечения:

- возможности получить доступ к хосту, даже если администратор устранит использованную для успешной реализации угрозы уязвимость;
- возможности получить доступ к хосту как можно наиболее скрытно;
- возможности получить доступ к хосту быстро (не повторяя заново процесс реализации угрозы).

На этапе ликвидации следов реализации угрозы осуществляется попытка уничтожения следов действий нарушителя. При этом удаляются соответствующие записи из всех возможных журналов аудита, в том числе записи о факте сбора информации.

3.2. ОБЩАЯ ХАРАКТЕРИСТИКА УГРОЗ ПРОГРАММНО-МАТЕМАТИЧЕСКИХ ВОЗДЕЙСТВИЙ

Программно-математическое воздействие – это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирование, уничтожение, блокирование и т.п.);

- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в информационной системе персональных данных, в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации информационных систем персональных данных с внешних носителей информации или посредством сетевого взаимодействия как в результате несанкционированного доступа, так и случайно пользователями информационных систем.

Современные вредоносные программы основаны на использовании уязвимостей различного рода программного обеспечения (системного, общего, прикладного) и разнообразных сетевых технологий, обладают широким спектром деструктивных возможностей (от несанкционированного исследования параметров информационных систем персональных данных без вмешательства в функционирование информационных систем, до уничтожения персональных данных и программного обеспечения таких систем) и могут действовать во всех видах программного обеспечения (системного, прикладного, в драйверах аппаратного обеспечения и т.д.).

Наличие в информационных системах персональных данных вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную и криптографическую защиту.

Основными видами вредоносных программ являются:

- программные закладки;
- классические программные (компьютерные) вирусы;
- вредоносные программы, распространяющиеся по сети (сетевые черви);
- другие вредоносные программы, предназначенные для осуществления несанкционированного доступа.

К программным закладкам относятся программы, фрагменты кода, инструкции, формирующие недекларированные возможности программного обеспечения. Вредоносные программы могут переходить из одного вида в другой, например, программная закладка может сгенерировать программный вирус, который, в свою очередь, попав в условия сети, может сформировать сетевого червя или другую вредоносную программу, предназначенную для осуществления несанкционированного доступа.

Рисунок 2

Классификация программных вирусов и сетевых червей

Основными деструктивными действиями, выполняемыми этими вирусами, являются:

- уничтожение информации в секторах дисков;
- исключение возможности загрузки операционной системы;
- искажение кода загрузчика;
- форматирование дискет или логических дисков винчестера;
- закрытие доступа к COM- и LPT-портам;
- замена символов при печати текстов;
- подергивания экрана;
- изменение метки диска или дискеты;
- создание псевдосбойных кластеров;
- создание звуковых и (или) визуальных эффектов (например, падение букв на экране);
- порча файлов данных;
- перезагрузка компьютера;
- вывод на экран разнообразных сообщений;
- отключение периферийных устройств (например, клавиатуры);
- изменение палитры экрана;
- заполнение экрана посторонними символами или изображениями;
- погашение экрана и перевод в режим ожидания ввода с клавиатуры;
- шифрование секторов винчестера;
- выборочное уничтожение символов, выводимых на экран при наборе с клавиатуры;
- уменьшение объема оперативной памяти;
- вызов печати содержимого экрана;
- блокирование записи на диск;
- уничтожение таблицы разбиения (Disk Partition Table), после этого компьютер можно загрузить только с флоппи-диска;
- блокирование запуска исполняемых файлов;

– блокирование доступа к винчестеру.

Файловые вирусы при своем размножении используют файловую систему операционной системы. По способу заражения файлов вирусы делятся на семь типов, которые перечислены в таблице 6.

Таблица 6

Типы файловых вирусов

Файловый вирус	Характеристика
Метод заражения «overwriting»	является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. При этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать
Паразитические файловые вирусы	которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными. Основными типами таких вирусов являются вирусы, записывающиеся в начало, середину или конец файлов. Такие вирусы записывают команду перехода на свой код в какую-либо часть файла и получают управление не непосредственно при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса. Причем выполняться эта процедура может крайне редко (например, при выводе сообщения о какой-либо специфической ошибке). В результате вирус может долгие годы «спать» внутри файла и проявить себя только при некоторых ограниченных условиях
«*Компаньон*»	вирусы, не изменяющие заражаемые файлы. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно он, то есть вирус. Вторую группу составляют вирусы, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на под именем заражаемого файла.
Файловые черви (worms)	являются разновидностью компаньон-вирусов, но при этом никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на запуск своей копии – например, INSTALL.EXE или WINSTART.BAT. Существуют вирусы-черви, использующие довольно необычные приемы, например, записывающие свои копии в архивы (ARJ, ZIP и прочие)

Link-вирусы	не изменяют физического содержимого файлов, но при запуске зараженного файла помощью модификацией необходимых полей файловой системы «заставляют» операционную систему выполнить свой код. Получив управление, файловый вирус совершает следующие общие действия: – проверяет оперативную память на наличие своей копии и инфицирует память компьютера, если копия вируса не найдена (в случае, если вирус является резидентным), ищет незараженные файлы в текущем и (или) корневом каталоге путем сканирования дерева каталогов логических дисков, а затем заражает обнаруженные файлы; – выполняет дополнительные (если они есть) функции: деструктивные действия, графические или звуковые эффекты и т.д. (дополнительные функции резидентного вируса могут вызываться спустя некоторое время после активизации в зависимости от текущего времени, конфигурации системы, внутренних счетчиков вируса или других условий, в этом случае вирус при активизации обрабатывает состояние системных часов, устанавливает свои счётчики и т.д.); – возвращает управление основной программе (если она есть). Паразитические вирусы при этом либо лечат файл, выполняют его, а затем снова заражают, либо восстанавливают программу (но не файл) в исходном виде.
Макровирусы (macro viruses)	являются программами на языках (макроязыках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. 12.9.6.1. Для существования вирусов в конкретной системе (редакторе) необходимо наличие встроенного в систему макроязыка с возможностями: – привязки программы на макроязыке к конкретному файлу; – копирования макропрограмм из одного файла в другой; – получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы). 12.9.6.2. К особенностям макровирусов относятся следующие свойства: 1) макропрограммы привязаны к конкретному файлу или находятся внутри файла; 2) макроязык позволяет копировать файлы или перемещать макропрограммы в служебные файлы системы и редактируемые файлы; 3) при работе с файлом при определенных условиях (открытие, закрытие и т.д.) вызываются макропрограммы (если таковые есть), которые определены специальным образом или имеют стандартные имена. 12.9.6.2. Большинство макровирусов активны не только в момент открытия (закрытия) файла, но до тех пор, пока активен сам редактор. Они содержат все свои функции в виде стандартных макросов Word/Excel/Office

Сетевые вирусы	вирусы, которые для своего распространения используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают ещё и возможностью запустить на выполнение свой код на удаленном компьютере или «подтолкнуть» пользователя к запуску зараженного файла

Вредоносными программами, обеспечивающими осуществление несанкционированного доступа, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;
- программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения информационных систем персональных данных;
- программы-генераторы компьютерных вирусов;
- программы, демонстрирующие уязвимости средств защиты информации и др.

4. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ «БУХГАЛТЕРИЯ» ГБУТО ГАТО

4.1. ОБЩАЯ ХАРАКТЕРИСТИКА ИНФОРМАЦИОНОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ «БУХГАЛТЕРИЯ» ГБУТО ГАТО

Информационная система персональных данных «Бухгалтерия» Государственного бюджетного учреждения Тюменской области «Государственный архив Тюменской области» используется для оптимизации процессов подбора, приёма, перевода и увольнения сотрудников, а также для ведения бухгалтерского учёта – начисления заработной платы, учёта материальной ответственности, подотчётных лиц, ведения оперативного учета, расчётов с контрагентами, расчётом налогов.

Работа в информационной системе персональных данных «Бухгалтерия» осуществляется с использованием следующих программных продуктов:

- ПАРУС Бюджет;
- Контур Экстерн;
- СУФД;
- Континент АП;
- Такском-Сертификаты;
- для обеспечения безопасности данных при их обработке в информационной системе персональных данных «Бухгалтерия» применяется такое специализированное программное обеспечение, как Secret Net Stodio, Dr.Web, КриптоПро CSP;
- работа на онлайн-платформах осуществляется с использованием браузеров IE e и Opera;
- обработка текстовых документов осуществляется с помощью офисного пакета MS Office.

Обслуживанием программных продуктов информационной системы персональных данных «Бухгалтерия» занимается системный администратор отдела информационно-поисковых систем и защиты информации архива.

Информационная система персональных данных «Бухгалтерия» состоит из двух автоматизированных рабочих мест, расположенных обособлено от других рабочих мест архива в пределах отдельного рабочего помещения внутри контролируемой зоны.

Перечень должностей сотрудников архива, имеющих доступ к информационной системе персональных данных «Бухгалтерия», закрепляется приказом архива от 23.12.2020 № 30 «Об утверждении перечней должностей, допущенных к обработке персональных данных сотрудников Государственного бюджетного учреждения Тюменской области «Государственный архив Тюменской области». Так ответственность за работу в системе несут главный бухгалтер и главный архивист, доступ к информационной системе персональных данных в соответствии с должностными обязанностями имеют директор,

заместитель директора, администрирование системы осуществляют системный администратор и администратор информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации архива.

При настройке доступа сотрудника в программных продуктах, входящих в состав информационной системы персональных данных «Бухгалтерия» системный администратор назначает сотруднику индивидуальные права доступа к различным категориям персональных данных в зависимости от обязанностей, возлагаемых
в соответствии с должностной инструкцией.

В информационной системе персональных данных «Бухгалтерия» осуществляется обработка следующих персональных данных сотрудников архива:

- Фамилия;
- Имя;
- Отчество;
- Адрес регистрации;
- ИНН;
- СНИЛС;
- Паспортные данные;
- Сведения из трудовой книжки;
- Сведения об образовании;
- Сведения о судимости;
- Сведения о заработной плате.

Хранение документов, содержащих персональные данные, в электронном виде производится непосредственно в информационной системе персональных данных «Бухгалтерия» на автоматизированных рабочих местах. Право самостоятельного доступа в помещения и архивы имеют директор архива, заместитель директора, главный бухгалтер, главный архивист.

Сотрудники архива при обработке персональных данных в информационной системе персональных данных «Бухгалтерия» работают непосредственно в программах путём внесения, изменения или удаления записей либо осуществляется работа с уже готовыми документами, выгруженными из программ, входящим в информационную систему.

Выгружаемые персональные данные из информационной системы персональных данных «Бухгалтерия» в соответствии с Налоговым кодексом РФ, с Федеральным законом от 24.07.2009 № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования», Трудовым кодексом РФ (глава 14, ст. 136), Федеральным Законом от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе», Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации» передаются в следующие организации: Федеральная налоговая служба, Пенсионный фонд, Фонд социального страхования, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования, банки (для начисления заработной платы), военный комиссариат, центр занятости, поликлиники. Персональные данные передаются в указанные органы в электронном виде по каналам связи с использованием электронной подписи.

4.2. ОПРЕДЕЛЕНИЕ УРОВНЯ ИСХОДНОЙ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ «БУХГАЛТЕРИЯ» ГБУТО ГАТО

Актуальной считается угроза, которая может быть реализована в информационной системе персональных данных и представляет опасность для персональных данных. Для оценки возможности реализации угрозы применяются два показателя - уровень исходной защищенности информационной системы персональных данных и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик информационной системы персональных данных «Бухгалтерия» (Y_1).

Исходная степень защищенности определяется следующим образом:

- информационная система персональных данных имеет высокий уровень исходной защищенности, если не менее 70% характеристик информационной системы персональных данных соответствуют уровню «высокий»;
- информационная система персональных данных имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1, и не менее 70% характеристик информационной системы персональных данных соответствуют уровню не ниже "средний";
- информационная система персональных данных имеет низкую степень исходной защищенности, если не выполняется условия по пунктам 1 и 2.

В соответствии с показателями Таблицы 7, в информационной системе персональных данных «Бухгалтерия» 71,4% характеристик соответствуют уровню не ниже «средний», следовательно $Y_1 = 5$.

Таблица 7

Показатели исходной защищенности информационной системы персональных данных «Бухгалтерия»

Технические и эксплуатационные характеристики информационной системы персональных данных	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
локальная информационная система персональных данных, развернутая в пределах одного здания	+		
2. По наличию соединения с сетями общего пользования:			
информационная система персональных данных, имеющая одноточечный выход в сеть общего пользования		+	
3. По встроенным (легальным) операциям с записями баз персональных данных:			
запись, удаление, сортировка		+	
4. По разграничению доступа к персональным данным:			
информационная система персональных данных, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем информационной системы персональных данных, либо субъект персональных данных		+	
5. По наличию соединений с другими базами персональных данных иных информационных систем персональных данных:			
интегрированная информационная система персональных данных (организация использует несколько баз персональных данных информационной системы персональных данных, при этом организация не является владельцем всех используемых баз персональных данных);			+
6. По уровню (обезличивания) персональных данных:			
информационная система персональных данных, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта персональных данных)			+
7. По объему персональных данных, которые предоставляются сторонним пользователям информационной системы персональных данных без предварительной обработки:			
информационная система персональных данных, предоставляющая часть персональных данных		+	

Таким образом, информационная система персональных данных «Бухгалтерия» имеет среднюю степень исходной защищенности.

4.3. ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГРОЗ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ «БУХГАЛТЕРИЯ» ГБУТО ГАТО

В информационной системе персональных данных «Бухгалтерия» и осуществляется обработка персональных данных, позволяющих идентифицировать субъекта персональных данных.

Информационные системы в зависимости от категорий обрабатываемых в них персональных данных подразделяются на 4 группы. Они перечислены в таблице 8.

Таблица 8

Характеристика категорий
информационных систем персональных данных

Категория систем	Характеристика
ИСПДн-С	это специальные категории персональных данных, к которым относятся информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информацию о здоровье и интимной жизни субъекта
ИСПДн-Б	это биометрические персональные данные, то есть данные, характеризующие биологические или физиологические особенности субъекта, например фотография или отпечатки пальцев
ИСПДн-О	это общедоступные персональные данные, то есть сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом
ИСПДн-И	это иные категории персональных данных, не представленные в трех предыдущих группах

Используемая в архиве информационная система персональных данных «Бухгалтерия» относится к первой категории – специальные. То есть это информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных.

В соответствии с объёмом персональных данных, обрабатываемых в информационной системе персональных данных, системы бывают трёх видов. Они перечислены в таблице 9.

Таблица 9

Категории объёмов данных в информационных системах

Категория объёма	Характеристика
3	одновременно обрабатываются данные менее чем 1 000 субъектов персональных данных в пределах конкретной организации
2	одновременно обрабатываются персональные данные от 1 000 до 100 000 субъектов персональных данных, работающих в отрасли экономики РФ, в органе государственной власти, проживающих в пределах муниципального образования
1	одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных в пределах РФ или субъекта РФ

Штатная численность сотрудников архива составляет менее одной тысячи человек, то есть число субъектов, чьи персональные данные обрабатываются в архиве, составляет менее 100 000 человек, и относится к 3 категории.

Согласно Постановлению Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для информационных систем персональных данных различают угрозы трёх типов:

- Угрозы 1 типа - связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.
- Угрозы 2 типа - связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.
- Угрозы 3 типа - не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Для информационной системы персональных данных архива «Бухгалтерия» характерны угрозы 2 типа, то есть угрозы наличия недокументированных возможностей в прикладном программном обеспечении.

По результатам анализа исходных данных информационной системе персональных данных присваивается один из следующих классов защищенности.

Рисунок 3

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
ИСПДн-С	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Любое	УЗ 1	УЗ 2	УЗ 3
ИСПДн-Б	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Любое	УЗ 1	УЗ 2	УЗ 3
ИСПДн-И	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 1	УЗ 3	УЗ 4
ИСПДн-О	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 2	УЗ 3	УЗ 4

Классы защищённости информационной системы персональных данных

Информационной системе персональных данных «Бухгалтерия» присваивается 2 класс защищённости: она относится к специальным информационным системам персональных данных, то есть обрабатываемые в системе персональные данные являются персональными данными сотрудников архива, системам архива присвоен 2 тип актуальных угроз.

В соответствии с Постановлением Правительства №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для обеспечения 2 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным,

обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
- назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе;
- доступ к содержанию электронного журнала сообщений должен быть возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

При составлении перечня актуальных угроз безопасности персональных данных каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент (Y_2). Характеристика вероятностей возникновения угроз представлена в таблице 10.

Таблица 10

Характеристика вероятностей возникновения угроз несанкционированного доступа к информационной системе персональных данных

Градация	Описание	Вероятность (Y_2)
маловероятно	отсутствуют объективные предпосылки для осуществления угрозы	0
низкая вероятность	объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию	2
средняя вероятность	объектные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности персональных данных недостаточны	5

высокая вероятность	объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности персональных данных не приняты	10

Для расчёта общей вероятности реализации каждой из возможных угроз проводится оценка вероятности реализации каждой угрозы нарушителем определенной категории. Общая вероятность угрозы (Y_2) определяется пропорционально наибольшей из приведённых для различных категорий нарушителей возможной вероятности. Оценка вероятности реализации угрозы рассмотрена в таблице 11.

Таблица 11

Оценка вероятности реализации угрозы безопасности информационной системы персональных данных «Бухгалтерия» архива различными категориями нарушителей

Угроза безопасности персональных данных	Вероятность реализации угрозы нарушителем категории Кn								
	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$	$К_6$	$К_7$	$К_8$	Итог Y_2
Угрозы утечки акустической информации	0	2	0	0	0	0	0	2	2
Угрозы утечки видовой информации	2	2	0	0	0	0	0	2	2
Угрозы утечки информации по каналам ПЭМИН	0	0	0	0	0	0	0	2	2
Угроза доступа к данным, её модификации, уничтожения данных, в том числе непреднамеренно	0	0	0	2	0	0	0	2	2
Угроза модификации BIOS	0	0	0	0	0	0	0	0	0
Угроза перехвата управления загрузкой	0	0	0	0	0	0	0	2	2
Угроза несанкционированного доступа к данным, содержащимся в информационной системе персональных данных, путём физического доступа к его элементам	0	0	0	0	0	2	0	2	2
Угроза несанкционированного доступа с использованием не декларированных возможностей системного программного обеспечения и программного обеспечения, предназначенного для обработки персональных данных	0	0	0	0	0	0	0	2	2

Угроза несанкционированного доступа с применением стандартных функций операционной системы	0	0	0	0	0	0	0	0	0
Угроза несанкционированного доступа с помощью прикладной программы	0	0	0	0	0	0	0	2	2
Угроза несанкционированного доступа с применением специально созданных для этого программ	0	0	0	0	0	0	0	2	2
Угроза несанкционированного доступа при передаче информации по внешним каналам	0	0	0	0	0	0	0	0	0
Угроза утечки информации с использованием копирования её на съемные носители	2	0	0	2	0	0	0	2	2
Угроза утечки информации посредством её печати на множительной технике	2	2	0	0	0	0	2	2	2
Угроза утечки информации за счет её несанкционированной передачи по каналам связи	2	0	0	0	0	0	2	2	2
Угроза внедрения вредоносных программ с использованием съемных носителей	2	2	0	0	0	0	2	2	2
Угроза «Анализ сетевого трафика»	0	0	0	0	0	0	0	2	2
Угроза сканирования открытых портов, служб и соединений	0	0	0	0	0	0	0	2	2
Угроза внедрения ложного объекта сети	0	0	0	0	0	0	0	2	2
Угроза навязывания ложного маршрута	0	0	0	0	0	0	0	2	2
Угроза перехвата и взлома паролей	0	0	0	0	0	0	0	2	2
Угроза подбора паролей доступа	0	0	0	0	0	0	0	2	2
Угроза типа «Отказ в обслуживании»	0	0	0	0	0	0	0	2	2
Угроза атаки типа «Переполнение буфера»	0	0	0	0	0	0	0	2	2
Угроза удаленного запуска приложений с использованием средств удаленного администрирования	0	0	0	0	0	0	0	0	0
Угроза внедрения аппаратных закладок	0	0	0	0	0	2	2	2	2
Угроза внедрения вредоносных программ	0	2	0	0	0	0	2	2	2
Несанкционированное отключение средств защиты	2	2	0	0	0	2	2	2	2

По итогам оценки уровня исходной защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y)

и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы рассчитывается по формуле: $Y=(Y_1+Y_2)/20$.

По значению коэффициента реализуемости угрозы Y формируется вербальная (словесная) интерпретация реализуемости угрозы:

- $0 < Y < 0,3$ - возможность реализации угрозы низкая;
- $0,3 < Y < 0,6$ - возможность реализации угрозы средняя;
- $0,6 < Y < 0,8$ - возможность реализации угрозы высокая;
- $Y > 0,8$ - возможность реализации угрозы очень высокая.

Расчёт вероятности реализации угроз приведён в таблице 12,

Таблица 12

Расчёт вероятности реализации угроз безопасности персональных данных при их обработке в информационной системы персональных данных «Бухгалтерия»

Угроза безопасности персональных данных	Y_1	Y_2	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы
Угрозы утечки акустической информации	5	2	0,35	средняя
Угрозы утечки видовой информации	5	2	0,35	средняя
Угрозы утечки информации по каналам ПЭМИН	5	2	0,35	средняя
Угроза доступа к данным, её модификации, уничтожения данных, в том числе непреднамеренно	5	2	0,35	средняя
Угроза модификации BIOS	5	0	0,25	низкая
Угроза перехвата управления загрузкой	5	2	0,35	средняя
Угроза несанкционированного доступа к данным, содержащимся в информационной системе персональных данных, путём физического доступа к его элементам	5	2	0,35	средняя
Угроза несанкционированного доступа с использованием не декларированных возможностей системного программного обеспечения и программного обеспечения, предназначенного для обработки персональных данных	5	2	0,35	средняя
Угроза несанкционированного доступа с применением стандартных функций операционной системы	5	0	0,25	низкая

Угроза несанкционированного доступа с помощью прикладной программы	5	2	0,35	средняя
Угроза несанкционированного доступа с применением специально созданных для этого программ	5	2	0,35	средняя
Угроза несанкционированного доступа при передаче информации по внешним каналам	5	0	0,25	низкая
Угроза утечки информации с использованием копирования её на съемные носители	5	2	0,35	средняя
Угроза утечки информации посредством её печати на множительной технике	5	2	0,35	средняя
Угроза утечки информации за счет её несанкционированной передачи по каналам связи	5	2	0,35	средняя
Угроза внедрения вредоносных программ с использованием съемных носителей	5	2	0,35	средняя
Угроза «Анализ сетевого трафика»	5	2	0,35	средняя
Угроза сканирования открытых портов, служб и соединений	5	2	0,35	средняя
Угроза внедрения ложного объекта сети	5	2	0,35	средняя
Угроза навязывания ложного маршрута	5	2	0,35	средняя
Угроза перехвата и взлома паролей	5	2	0,35	средняя
Угроза подбора паролей доступа	5	2	0,35	средняя
Угроза типа «Отказ в обслуживании»	5	2	0,35	средняя
Угроза атаки типа «Переполнение буфера»	5	2	0,35	средняя
Угроза удаленного запуска приложений с использованием средств удаленного администрирования	5	0	0,25	низкая
Угроза внедрения аппаратных закладок	5	2	0,35	средняя
Угроза внедрения вредоносных программ	5	2	0,35	средняя
Несанкционированное отключение средств защиты	5	2	0,35	средняя

4.4. ОЦЕНКА ОПАСНОСТИ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ «БУХГАЛТЕРИЯ» ГБУТО ГАТО

Оценка опасности реализации угроз информационным системам персональных данных архива производится на основе общей оценки специалистов по защите информации в архиве и определяется вербальным показателем опасности, который имеет 3 значения:

- низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

- средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Правила отнесения угрозы безопасности персональных данных к актуальной указаны в таблице 13.

Таблица 13

Правила отнесения угрозы безопасности персональных данных к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Для оценки степени возможного ущерба от реализации угрозы безопасности информации определяются:

- возможный результат реализации угрозы безопасности информации в информационной системе,
- вид ущерба, к которому может привести реализация угрозы безопасности информации,
- степень последствий от реализации угрозы безопасности информации для каждого вида ущерба.

В качестве результата реализации угрозы безопасности информации рассматриваются непосредственное или опосредованное воздействие на конфиденциальность, целостность, доступность информации, содержащейся в информационной системе.

Объектами воздействия угрозы являются непосредственно информация и (или) иные объекты защиты информационной системы или обеспечивающей инфраструктуры, которые обеспечивают получение, обработку, хранение,

передачу, уничтожение информации в информационной системе, в результате доступа к которым или воздействия на которые возможно воздействие на конфиденциальность, целостность или доступность информации.

Результат реализации угрозы безопасности информации определяется воздействием угрозы на каждое свойство безопасности информации (конфиденциальность, целостность, доступность) в отдельности. В таблице 14 рассмотрены виды ущерба от реализации угроз, в таблице 15 перечислены основные виды такого ущерба.

Таблица 14

Возможный ущерб от реализации угроз безопасности информации

Свойство безопасности информации	Результат реализации угрозы безопасности информации	
	Не оказывает воздействия	Оказывает воздействие
Конфиденциальность	В результате реализации угрозы безопасности информации отсутствует возможность неправомерного доступа, копирования, предоставления или распространения информации	В результате реализации угрозы безопасности информации возможны неправомерный доступ, копирование, предоставление или распространение информации
Целостность	В результате реализации угрозы безопасности информации отсутствует возможность уничтожения или модифицирования информации	В результате реализации угрозы безопасности информации возможно уничтожение или модифицирование информации
Доступность	В результате реализации угрозы безопасности информации отсутствует возможность блокирования информации	В результате реализации угрозы безопасности информации возможно блокирование информации

Таблица 15

Основные виды ущерба и возможные негативные последствия, к которым может привести нарушение безопасности информации

Вид ущерба	Возможные негативнее последствия от нарушения конфиденциальности, целостности, доступности информации
Экономический (финансовый)	Снижение, как минимум, одного экономического показателя. Потеря (кража) финансовых средств. Недополучение ожидаемой (прогнозируемой) прибыли. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Потеря клиентов, поставщиков. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений. Другие прямые или косвенные финансовые потери
Социальный	Создание предпосылок для нанесения вреда здоровью граждан. Возможность нарушения функционирования объектов обеспечения жизнедеятельности граждан. Организация пикетов, забастовок, митингов и других акций. Увольнения. Увеличение количества жалоб в органы государственной власти или органы местного самоуправления. Появление негативных публикаций в общедоступных источниках. Невозможность (прерывание) предоставления социальных услуг (сервисов). Другие последствия, приводящие к нарастанию социальной напряженности в обществе
Политический	Создание предпосылок к обострению отношений в международных отношениях. Срыв двусторонних (многосторонних) контактов с зарубежными партнерами. Неспособность выполнения международных (двусторонних) договорных обязательств. 29 Невозможность заключения международных (двусторонних) договоров, соглашений. Создание предпосылок к внутриполитическому кризису. Нарушение выборного процесса. Другие последствия во внутриполитической и внешнеполитической областях деятельности
Репутационный	Нарушение законодательных и подзаконных актов. Нарушение деловой репутации. Снижение престижа. Дискредитация работников. Утрата доверия. Неспособность выполнения договорных обязательств. Другие последствия, приводящие к нарушению репутации
Ущерб в области обороны, безопасности и правопорядка	Создание предпосылок к наступлению негативных последствий для обороны, безопасности и правопорядка. Нарушение общественного правопорядка. Неблагоприятное влияние на обеспечение общественного правопорядка. Возможность потери или снижения уровня контроля за общественным правопорядком. Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации. Другие последствия, приводящие к ущербу в области обороны, безопасности и правопорядка

Ущерб субъекту персональных данных	Создание угрозы личной безопасности. Финансовые или иные материальные потери физического лица. Вторжение в частную жизнь. Создание угрозы здоровью. Моральный вред. Утрата репутации. Другие последствия, приводящие к нарушению прав субъекта персональных данных
Технологический	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). Принятие неправильных решений. Простой информационной системы или сегмента информационной системы. Другие последствия, приводящие к нарушению технологии обработки информации

Степень возможного ущерба от реализации угрозы безопасности информации определяется степенью негативных последствий от нарушения конфиденциальности, целостности или доступности каждого вида информации, содержащейся в информационной системе, с учётом специфики конкретного случая.

В качестве единой шкалы измерения степени негативных последствий принимаются значения «незначительные», «умеренные» и «существенные» негативные последствия, то есть последствиям реализации угроз присваиваются низкая, средняя и высокая степени ущерба соответственно. Характеристика степеней ущерба приведена в таблице 16.

Таблица 16

Степень возможного ущерба

Степень ущерба	Характеристика степени ущерба
Высокая	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
Средняя	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
Низкая	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств

5. ПЕРЕЧЕНЬ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ «БУХГАЛТЕРИЯ» ГБУТО ГАТО

В соответствии с правилами отнесения угроз безопасности к актуальным, для информационной системы персональных данных «Бухгалтерия» существуют следующие актуальные угрозы, представленные в таблице 17..

Таблица 17

Расчёт актуальности реализации угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия»

Угроза безопасности персональных данных	Возможность реализации угрозы	Показатель опасности	Показатель актуальности
Угрозы утечки акустической информации	средняя	низкая	неактуальная
Угрозы утечки видовой информации	средняя	средняя	актуальная
Угрозы утечки информации по каналам ПЭМИН	средняя	высокая	актуальная
Угроза доступа к данным, её модификации, уничтожения данных, в том числе непреднамеренно	средняя	средняя	актуальная
Угроза модификации BIOS	низкая	средняя	неактуальная
Угроза перехвата управления загрузкой	средняя	средняя	актуальная
Угроза несанкционированного доступа к данным, содержащимся в информационной системе персональных данных, путём физического доступа к его элементам	средняя	средняя	актуальная
Угроза несанкционированного доступа с использованием не декларированных возможностей системного программного обеспечения и программного обеспечения, предназначенного для обработки персональных данных	средняя	средняя	актуальная
Угроза несанкционированного доступа с применением стандартных функций операционной системы	низкая	средняя	неактуальная
Угроза несанкционированного доступа с помощью прикладной программы	средняя	средняя	актуальная
Угроза несанкционированного доступа с применением специально созданных для этого программ	средняя	средняя	актуальная

Угроза несанкционированного доступа при передаче информации по внешним каналам	низкая	высокая	актуальная
Угроза утечки информации с использованием копирования её на съемные носители	средняя	высокая	актуальная
Угроза утечки информации посредством её печати на множительной технике	средняя	высокая	актуальная
Угроза утечки информации за счет её несанкционированной передачи по каналам связи	средняя	высокая	актуальная
Угроза внедрения вредоносных программ с использованием съемных носителей	средняя	средняя	актуальная
Угроза «Анализ сетевого трафика»	средняя	средняя	актуальная
Угроза сканирования открытых портов, служб и соединений	средняя	средняя	актуальная
Угроза внедрения ложного объекта сети	средняя	высокая	актуальная
Угроза навязывания ложного маршрута	средняя	высокая	актуальная
Угроза перехвата и взлома паролей	средняя	высокая	актуальная
Угроза подбора паролей доступа	средняя	высокая	актуальная
Угроза типа «Отказ в обслуживании»	средняя	низкая	неактуальная
Угроза атаки типа «Переполнение буфера»	средняя	низкая	неактуальная
Угроза удаленного запуска приложений с использованием средств удаленного администрирования	низкая	низкая	неактуальная
Угроза внедрения аппаратных закладок	средняя	средняя	актуальная
Угроза внедрения вредоносных программ	средняя	высокая	актуальная
Несанкционированное отключение средств защиты	средняя	средняя	актуальная

Таким образом, актуальными угрозами безопасности персональных данных при их обработке в архиве в информационной системе персональных данных «Бухгалтерия» являются:

- Угрозы утечки видовой информации;
- Угрозы утечки информации по каналам ПЭМИН;
- Угроза доступа к данным, её модификации, уничтожения данных, в том числе непреднамеренно;
- Угроза перехвата управления загрузкой;

- Угроза несанкционированного доступа к данным, содержащимся в информационной системе персональных данных, путём физического доступа к его элементам;
- Угроза несанкционированного доступа с использованием недекларированных возможностей системного программного обеспечения и программного обеспечения, предназначенного для обработки персональных данных;
- Угроза несанкционированного доступа с помощью прикладной программы;
- Угроза несанкционированного доступа с применением специально созданных для этого программ;
- Угроза несанкционированного доступа при передаче информации по внешним каналам;
- Угроза утечки информации с использованием копирования её на съемные носители;
- Угроза утечки информации посредством её печати на множительной технике;
- Угроза утечки информации за счет её несанкционированной передачи по каналам связи;
- Угроза внедрения вредоносных программ с использованием съемных носителей;
- Угроза «Анализ сетевого трафика»;
- Угроза сканирования открытых портов, служб и соединений;
- Угроза внедрения ложного объекта сети;
- Угроза навязывания ложного маршрута;
- Угроза перехвата и взлома паролей;
- Угроза подбора паролей доступа;
- Угроза внедрения аппаратных закладок;
- Угроза внедрения вредоносных программ;
- Несанкционированное отключение средств защиты.

6. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМЫЕ ВИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ «БУХГАЛТЕРИЯ» ГБУТО ГАТО

Для обеспечения защиты информации от актуальных угроз безопасности, в том числе персональных данных, обрабатываемых в информационной системе персональных данных «Бухгалтерия» в архиве применяются следующие меры, отражённые в таблице 18.

Таблица 18

Меры противодействия реализации угроз безопасности персональных данных при их обработке в архиве

Угроза безопасности персональных данных	Меры по противодействию угрозе	
	Технические	Организационные
Угрозы утечки видовой информации	Блокировка персонального компьютера, на котором осуществляется обработка персональных данных, в случае бездействия на протяжении 3 минут.	Расположение мониторов автоматизированных рабочих мест, на которых осуществляется обработка персональных данных, в обратную от входной двери сторону. Жалюзи на окнах. Постоянное присутствие ответственного сотрудника архива в случае посещения кабинете, в котором осуществляется обработка персональных данных, посторонними лицами.
Угроза доступа к данным, её модификации, уничтожения данных, в том числе непреднамеренно	Шифрование данных при помощи встроенных в используемое программное обеспечение модулей. Функционирование системы защиты от несанкционированного доступа (Secret Net, Dr.Web). Использование механизмов архивации и восстановления Windows.	Пропускной режим в здание. Разграничение прав доступа к информационной системе, в защищаемое помещение. Назначение ответственного за обработку персональных данных из числа сотрудников архива.
Угроза перехвата управления загрузкой	Применение антивирусного программного обеспечения. Установка соответствующих параметров безопасности механизмов идентификации и аутентификации при настройке операционной системы на сертифицированную конфигурацию для пользователей домена и локальных пользователей. В случае использования других элементов общего программного обеспечения (SQL Server, ExchangeServer и др.) дополнительно используются их встроенные механизмы «Идентификация и аутентификация» и «Защита данных пользователя». Использование протокола защищенного соединения (HTTPS).	Регулярные проверки работоспособности информационной системы персональных данных «Бухгалтерия», состояния функционирования её модулей. Контроль обновления лицензий программного обеспечения.

Угроза несанкционированного доступа к данным, содержащимся в информационной системе персональных данных, путём физического доступа к его элементам	Блокировка персонального компьютера, на котором осуществляется обработка персональных данных, в случае бездействия на протяжении 3 минут.	Пропускной режим в здание. Разграничение прав доступа к информационной системе, в защищаемое помещение.
Угроза несанкционированного доступа с использованием недекларированных возможностей системного программного обеспечения и программного обеспечения, предназначенного для обработки персональных данных	Настройка системы регистрации и разграничения прав Windows (функция AppLocker Windows). Сбор, запись, хранение и защита информации о событиях, происходящих в системе с использованием Журнала событий в операционной системе. Использование механизмов «Аудит безопасности» и «Защита данных пользователя» Windows. Контроль журнала событий операционной системы и другого программного обеспечения.	В случае повышенного риска наличия чужих закладок осуществление внеплановой проверки наличия посторонних кодов и недокументированных функций в системе.
Угроза несанкционированного доступа с помощью прикладной программы	Сбор, запись, хранение и защита информации о событиях, происходящих в системе с использованием Журнала событий в операционной системе. Использование средств защиты информации от несанкционированного доступа механизмов защиты на прикладном уровне. Настройка аутентификации при доступе к компонентам информационной системы и разграничения доступа к ним.	Регулярные проверки работоспособности информационной системы персональных данных «Бухгалтерия», состояния функционирования её модулей.
Угроза несанкционированного доступа с применением специально созданных для этого программ	Использование антивирусного программного обеспечения, дополнительных модулей используемых в работе программных средств, систем обнаружения вторжений. Настройка аутентификации пользователей при запуске программ в информационной системе.	Регулярные проверки работоспособности информационной системы персональных данных «Бухгалтерия», состояния функционирования её модулей.

Угроза несанкционированного доступа при передаче информации по внешним каналам	Использование антивирусного программного обеспечения, дополнительных модулей используемых в работе программных средств, систем обнаружения вторжений, межсетевого экрана. Использование протокола защищенного соединения (HTTPS).	Контроль почтовых сервисов и иных программ, осуществляющих передачу данных без встроенных специализированных систем защиты. Использование лицензионных программ, применяемых для обработки персональных данных. Разграничение доступа к переносным устройствам (съёмным носителям информации).
Угроза утечки информации с использованием копирования её на съемные носители	Блокировка персонального компьютера, на котором осуществляется обработка персональных данных, в случае бездействия на протяжении 3 минут.	Пропускной режим в здание. Разграничение прав доступа к информационной системе, в защищаемое помещение.
Угроза утечки информации посредством её печати на множительной технике	Блокировка персонального компьютера, на котором осуществляется обработка персональных данных, в случае бездействия на протяжении 3 минут.	Пропускной режим в здание. Разграничение прав доступа к информационной системе, в защищаемое помещение.
Угроза утечки информации за счет её несанкционированной передачи по каналам связи	Блокировка персонального компьютера, на котором осуществляется обработка персональных данных, в случае бездействия на протяжении 3 минут. Использование антивирусного программного обеспечения, дополнительных модулей используемых в работе программных средств, систем обнаружения вторжений, межсетевого экрана. Использование протокола защищенного соединения (HTTPS).	Пропускной режим в здание. Разграничение прав доступа к информационной системе, в защищаемое помещение.
Угроза внедрения вредоносных программ с использованием съемных носителей	Блокировка персонального компьютера, на котором осуществляется обработка персональных данных, в случае бездействия на протяжении 3 минут. Автоматическая проверка съёмных носителей антивирусным программным обеспечением	Пропускной режим в здание. Разграничение прав доступа к информационной системе, в защищаемое помещение. Регламентация правил работы со съёмными носителями информации в локальных актах архива. Назначение ответственного за обработку персональных данных из числа сотрудников архива.

Угроза «Анализ сетевого трафика»	Использование антивирусного программного обеспечения, дополнительных модулей используемых в работе программных средств, систем обнаружения вторжений, межсетевого экрана. Использование протокола защищенного соединения (HTTPS).	Пропускной режим в здание. Разграничение прав доступа к информационной системе, в защищаемое помещение. Периодические проверки исходящего и входящего трафика.
Угроза сканирования открытых портов, служб и соединений	Использование антивирусного программного обеспечения, дополнительных модулей используемых в работе программных средств, систем обнаружения вторжений, межсетевого экрана.	Пропускной режим в здание. Разграничение прав доступа к информационной системе, в защищаемое помещение.
Угроза внедрения ложного объекта сети	Настройка параметров идентификация и аутентификация (определение подлинности). Использование антивирусного программного обеспечения, дополнительных модулей используемых в работе программных средств, систем обнаружения вторжений, межсетевого экрана.	Периодическая контроль работоспособности установленного аппаратного и программного обеспечения.
Угроза навязывания ложного маршрута	Использование протокола TCP. Использование антивирусного программного обеспечения, дополнительных модулей используемых в работе программных средств, систем обнаружения вторжений, межсетевого экрана. Использование протокола защищенного соединения (HTTPS).	Периодическая контроль работоспособности установленного аппаратного и программного обеспечения.
Угроза перехвата и взлома паролей	Использование персональных различных электронных подписей при работе с программами, в которых осуществляется обработка персональных данных. Запрет автосохранения паролей при работе на интернет-платформах и в программных средствах. Деактивация хеша пароля LM в Windows.	Регламентация правил работы с парольной информацией к различным системам в локальных актах архива. Соблюдение правил составления паролей к системам. Проверка действующего пароля на надёжность.

Угроза подбора паролей доступа	Установка паролей для программного обеспечения на учётные записи сотрудника, осуществляющего обработку персональных данных, непосредственно на персональном компьютере, на котором осуществляется эта обработка. Защита процесса загрузки – установка пароля при загрузке BIOS. Настройка блокировки возможности входа в учётную запись и конкретное программное обеспечение после введения определённого числа неудачных попыток ввода пароля.	Регламентация правил работы с парольной информацией к различным системам в локальных актах архива. Соблюдение правил составления паролей к системам. Проверка действующего пароля на надёжность.
Угроза внедрения аппаратных закладок	-	Ежедневный визуальный осмотр автоматизированных рабочих мест, аппаратного и программного обеспечения, входящих в состав информационной системы персональных данных «Бухгалтерия». Организация разграничения прав сотрудников на установку стороннего программного обеспечения, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов информационной системы персональных данных «Бухгалтерия» и средств защиты.
Угроза внедрения вредоносных программ	Блокировка персонального компьютера, на котором осуществляется обработка персональных данных, в случае бездействия на протяжении 3 минут. Использование антивирусного программного обеспечения, дополнительных модулей используемых в работе программных средств, систем обнаружения вторжений, межсетевого экрана.	Пропускной режим в здание. Разграничение прав доступа к информационной системе, в защищаемое помещение. Регламентация правил работы со съёмными носителями информации в локальных актах архива. Контроль почтовых сервисов и иных программ, осуществляющих передачу данных без встроенных специализированных систем защиты. Организация разграничения прав сотрудников на установку стороннего программного обеспечения, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов информационной системы персональных данных «Бухгалтерия» и средств защиты.

Несанкционированное отключение средств защиты	Доступ к установке и настройке аппаратного и программного обеспечения, входящего в состав информационной системы персональных данных «Бухгалтерия» предоставляется только уполномоченным сотрудникам архива.	Периодический контроль работоспособности установленного аппаратного и программного обеспечения. Организация разграничения прав сотрудников на установку стороннего программного обеспечения, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов информационной системы персональных данных «Бухгалтерия» и средств защиты.

ЗАКЛЮЧЕНИЕ

В настоящем документе проведена классификация угроз безопасности персональных данных при их автоматизированной обработке, дано общее описание угроз безопасности персональных данных и построена Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия». В соответствии с требованиями методических документов ФСТЭК России, выявлены актуальные угрозы безопасности персональных данных для информационной системы персональных данных «Бухгалтерия» Государственного бюджетного учреждения Тюменской области «Государственный архив Тюменской области».

Построенная Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» применима к существующему состоянию рассмотренной информационной системы при условии соблюдения основных (базовых) исходных данных:

- технические средства информационной системы персональных данных «Бухгалтерия» находятся в пределах контролируемой зоны и не перемещаются на какой-либо промежуток времени в иные помещения архива;
- информационная система персональных данных «Бухгалтерия» физически отделена от сетей общего пользования;
- отсутствует возможность неконтролируемого пребывания посторонних лиц в служебных помещениях архива, где осуществляется работа в информационной системе персональных данных «Бухгалтерия».

В случае несоблюдения и/или изменения вышеуказанных условий Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» должна быть пересмотрена.

Администратор информационной безопасности вычислительной сети ОИПСиЗИ Е.Ю. Дроздова

__ _____ 2021 г.

Приложение 3

Проект Инструкции по организации антивирусной защиты
в ГБУТО «Государственный архив Тюменской области»

УТВЕРЖДАЮ
Директор ГБУТО ГАТО
О.П. Тарасова
____ _____ 2021 г.

ИНСТРУКЦИЯ

по организации антивирусной защиты
в Государственном бюджетном учреждении Тюменской области
«Государственный архив Тюменской области»

СОГЛАСОВАНО
протоколом заседания комиссии
ГБУТО ГАТО по защите информации
от_____ № ___

Тюмень
2021

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция разработана в соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Регулярный периодический антивирусный контроль производится в целях обеспечения защиты от деструктивных воздействий компьютерных вредоносных программ и утраты служебной информации и иных категорий информации ограниченного доступа, работа с которыми осуществляется в Государственном бюджетном учреждении Тюменской области «Государственный архив Тюменской области» (далее – архив).

1.3. Настоящая Инструкция определяет требования к порядку организации антивирусной защиты и проведения антивирусных проверок в архиве.

1.4. Действие настоящей Инструкции распространяется на всех сотрудников архива.

1.5. Непосредственную ответственность за соблюдение в повседневной рабочей деятельности установленных норм обеспечения антивирусной защиты информации и требований настоящей Инструкции несут сотрудники архива, за которыми закреплены соответствующие автоматизированные рабочие места (персональные компьютеры и периферийная техника).

1.6. Контроль за периодичностью проведения в архиве антивирусных проверок, соблюдение в повседневной рабочей деятельности установленных норм обеспечения антивирусной защиты информации и требований настоящей Инструкции осуществляет начальник отдела информационно-поисковых систем и защиты информации.

1.7. Ответственными за организацию антивирусной защиты в архиве являются системный администратор и администратор информационной

безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации.

1.8. Доведение положений Инструкции до сотрудников архива под подпись в Листе ознакомления с локальными актами госархива, входящими в состав личных дел сотрудников, осуществляется ответственными за организацию антивирусной защиты в архиве при приёме нового сотрудника на работу.

1.9. В целях закрепления знаний по вопросам практического выполнения требований настоящей Инструкции, разъяснения возникающих вопросов, ответственными организацию антивирусной защиты в архиве могут проводиться групповые и индивидуальные инструктажи для сотрудников архива.

1.10. Настоящая Инструкция подлежит пересмотру в случае существенного изменения условий (изменение требований к антивирусному программному обеспечению, корректировка процесса проведения антивирусного контроля и др.).

2. ЗАДАЧИ И НАПРАВЛЕНИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

2.1. Основными задачами обеспечения антивирусной защиты в архиве являются:

- исключение или существенное затруднение осуществления противоправных действий в отношении информации, содержащейся на персональных компьютерах сотрудников архива, серверах и съёмных носителях информации, выданных в служебное пользование как носителей защищаемой информации;
- обеспечение условий для устойчивой бесперебойной работы.

2.2. Обеспечение антивирусной защиты включает выполнение следующих процедур:

- регулярные профилактические работы, в т.ч. периодичные антивирусные проверки;

- анализ ситуации проявления вредоносных программ и причины их появления;
- уничтожение вредоносных программ на персональных компьютерах сотрудников, серверах архива и съёмных носителях информации, выданных
  в служебное пользование сотрудникам архива;
- принятие мер по предотвращению причин появления вредоносных программ с учётом текущей практики работы.

2.3. Для выполнения требований по антивирусной защите архива используется специализированное программное обеспечение, обеспечивающее надежную автоматическую антивирусную защиту и контроль уровня защищённости информационных массивов данных от вредоносных программ.

2.4. Настройка специализированного антивирусного программного обеспечения осуществляется системным администратором отдела информационно-поисковых систем и защиты информации.

2.5. Ответственные сотрудники, на которых возлагаются обязанности по обеспечению антивирусной защиты в госархиве, имеют полноправный доступ ко всем автоматизированным рабочим местам, серверам и другому оборудованию архива.

2.6. Для сотрудников архива, в чьи должностные обязанности не входит обеспечение защиты информации в архиве, изменение настроек и параметров защиты антивирусных средств не допускается.

3. ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К АНТИВИРУСНОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ АРХИВА

3.1. В архиве допускается применение как лицензионного, так и нелицензионного антивирусного программного обеспечения.

3.2. Для наиболее защищаемых точек (автоматизированные рабочие места сотрудников, осуществляющих обработку персональных данных

с использованием средств автоматизации) применяется лицензионное антивирусное программное обеспечение, закупленное у разработчиков или официальных поставщиков.

3.3. Обеспечение обновлений, консультаций и других форм сопровождения эксплуатации антивирусного программного обеспечения должно гарантироваться поставщиком.

3.4. Надежность и работоспособность антивирусного программного обеспечения должны быть гарантированы в любом из предусмотренных режимов работы в рускоязычной среде.

3.5. Установленное в архиве антивирусное программное обеспечение должно соответствовать системным требованиям, характеристикам и комплектации персональных компьютеров архива.

3.6. Установленное в архиве антивирусное программное обеспечение должно иметь возможность регулярного обновления антивирусных баз на персональных компьютерах архива без участия пользователя.

4. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ АНТИВИРУСНОГО КОНТРОЛЯ

4.1. Даты антивирусных проверок определяются заранее и обозначаются в тексте плана работы архива на год.

4.2. Все процессы по организации и проведению мероприятий по обеспечению антивирусной защиты архива производятся ответственными за организацию антивирусной защиты в архиве без помех для работы основного и специального программного обеспечения.

4.3. Процесс плановой полной проверки персональных компьютеров архива проводится во время наименьшей нагрузки оборудования пользовательскими задачами в заранее назначенный рабочий день.

4.4. В случае изменения даты проведения антивирусной проверке при возникновении служебной необходимости такого переноса новая дата определяется по согласованию с сотрудником архива, для автоматизированного рабочего места которого необходим перенос даты антивирусного контроля.

При этом временной разрыв между проверкой отдельных автоматизированных рабочих мест сотрудников архива не должен превышать трёх недель в целях обеспечения комплексного подхода к проведению цикличной антивирусной проверки.

4.5. Обязательному антивирусному контролю подлежит любая информация, содержащаяся на автоматизированных рабочих местах сотрудников архива, серверах, расположенных по адресам: г. Тюмень, пр. Геологоразведчиков, д. 21 и г. Тюмень, ул. Воровского, д. 35, а также съёмных носителях информации, выданных сотрудникам архива в служебное пользование, в том числе получаемая по электронной почте и на внешних носителях из сторонних организаций и частных лиц.

4.6. Полный антивирусный контроль всех автоматизированных рабочих местах, серверах архива проводится не реже одного раза в квартал ответственными за организацию антивирусной защиты.

4.7. Антивирусный контроль исходящей документации необходимо проводить только в необходимых случаях непосредственно перед отправкой или записью на съёмный носитель.

4.8. Антивирусный контроль входящей документации в электронном виде (посредством систем электронного документооборота, систем межведомственного электронного взаимодействия и др.) проводится сразу после её приёма.

5. ПРИЗНАКИ ЗАРАЖЕНИЯ ВРЕДОНОСНЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

5.1. Вредоносная программа – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам компьютеров и серверов учреждения или к информации, хранимой на них, с целью несанкционированного использования ресурсов или причинения вреда (нанесения ущерба) владельцу информации,

и/или учреждению, путём копирования, искажения, удаления или подмены информации.

5.2. К признакам заражения вредоносными программами относятся:

- автоматическое открытие окон с незнакомым содержимым при запуске компьютера;
- блокировка доступа к официальным сайтам антивирусных компаний;
- появление новых неизвестных процессов, которые можно отследить в диспетчере задач Windows;
- появление в разделах реестра, отвечающего за автозапуск, новых записей;
- запрет на изменение настроек компьютера в учётной записи администратора;
- невозможность запустить исполняемый файл (выдаётся сообщение об ошибке);
- появление всплывающих окон или системных сообщений с непривычным текстом, в том числе содержащих неизвестные веб-адреса и названия;
- перезапуск компьютера во время старта какой-либо программы;
- случайное и/или беспорядочное отключение компьютера или сервера;
- нетипичная работа программ;
- случайное аварийное завершение программ;
- снижение производительности при достаточном объёме памяти, вплоть до полной остановки работоспособности н кратковременные или долговременные промежутки времени;
- появление неизвестных файлов и каталогов в файловой системе операционной системы, при попытке удаления которых обычно возникает сообщение об ошибке удаления;
- шифрование или повреждение пользовательских файлов;
- неизвестные изменения в содержимом системных файлов при открытии их в текстовом редакторе;

- появление нетипичных графических и звуковых эффектов;
- быстрая утечка памяти и/или пространства на жёстком диске (использование большего объёма памяти, чем необходимо для нормальной работы запущенных программ) и др.

6. МЕРОПРИЯТИЯ ПО УНИЧТОЖЕНИЮ ВРЕДОНОСНЫХ ПРОГРАММ

6.1. При возникновении подозрения на наличие компьютерного вируса на автоматизированном рабочем месте сотрудник архива обязан сообщить об этом любому из ответственных за организацию антивирусной защиты в архиве.

6.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудник архива обязан:

- приостановить выполнение любой работы на компьютере, в том числе сохранить все открытые документы и закрыть все папки;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов любого из ответственных за организацию антивирусной защиты в архиве;
- по завершении лечения или уничтожения зараженных файлов поставить в известность о факте обнаружения зараженных вирусом файлов владельца зараженных файлов (если они были переданы сотрудниками иных организаций), а также другие отделы архива, использующие эти файлы в работе.

6.3. В случае заражения автоматизированного рабочего места сотрудника архива вредоносными программами ответственный за организацию антивирусной защиты в архиве выполняет следующие действия:

- осуществляет обновление антивирусных баз всех объектов антивирусной защиты архива;

- проверяет состояние всех объектов антивирусной защиты архива, выявляет наличие других зараженных рабочих станций;
- в случае заражения нескольких автоматизированных рабочих мест проводит внеочередной антивирусный контроль всех автоматизированных рабочих мест архива;
- оперативно принимает меры по предотвращению распространения заражения вредоносными программами и при необходимости отключает от сети зараженные автоматизированные рабочие места;
- осуществляет действия, направленные на устранение вредоносной программы на всех пораженных участках локальной сети архива;
- по завершении мероприятий по устранению последствий заражения восстанавливает работоспособность автоматизированного рабочего места

  и передает его ответственному пользователю;
- подготавливает отчёт заместителю директора, ответственному за контроль за обеспечением информационной безопасности в архиве, о факте заражения автоматизированного рабочего места архива с подробным описанием всех осуществлённых действий, указанием причин заражения, последствий и внесением предложений по предотвращению аналогичных случаев.

6.4. Если вредоносная программа поразила какие-либо программы, то уничтожение вредоносной программы выполняется путём уничтожения такой программы в случае, когда такое удаление не принесёт ущерб рабочей деятельности. После уничтожения зараженной программы она подлежит восстановлению с использованием её резервной копии либо переустанавливается заново.

6.5. Если вредоносная программа поразила рабочие файлы, то вредоносная программа уничтожается либо путём стирания этих файлов, либо путём использования специального «лечащего» режима антивирусного программного обеспечения. Использование «лечащего» режима не даёт полной гарантии

восстановления файла, поэтому после «лечения» необходима повторная антивирусная проверка восстановленного файла. «Лечение» используются в тех случаях, когда отсутствует резервная копия зараженной программы или файла.

6.6. По факту появления и проникновения вредоносных программ, повлекших неустойчивую работу и (или) вывод из строя оборудования, локально-вычислительной сети и информационных массивов архива, ответственными организацию антивирусной защиты в архиве проводится служебное расследование.

6.7. Результаты расследования причин появления и последствий от воздействия вредоносных программ на персональные компьютеры, серверы, локальную вычислительную сеть, съёмные носители информации архива докладываются комиссии архива по защите информации с предложениями по принятию мер, предотвращающих в будущем повторение подобных фактов.

7. ОТВЕТСТВЕННОСТЬ

7.1. Организация работ по антивирусной защите и ответственность за выполнение требований настоящей Инструкции сотрудниками архива возлагается на администратора информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации.

7.2. Сопровождение антивирусного программного обеспечения, выполнение технических мероприятий по антивирусной защите в архиве возлагается на системного администратора отдела информационно-поисковых систем и защиты информации.

7.3. В обязанности администратора информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации в рамках организации работ по антивирусной защите в архиве входит:

- контроль своевременного приобретения, инсталляции средств антивирусной защиты информации и регулярного обновление баз данных антивирусного программного обеспечения;
- осуществление контроля за соблюдением сотрудниками архива требований антивирусной защиты;
- обеспечение контроля за соблюдением требований при работе с сетью Интернет, а также, в случае необходимости, за характером и объемом трафика, получаемого из сети Интернет, и его соответствия служебной необходимости;
- контроль за проведением всех необходимых мероприятий по обеспечению антивирусной защиты в архиве;
- проведение работ по обнаружению и обеззараживанию угроз на серверах, автоматизированных рабочих местах сотрудников архива и съёмных носителях информации, выданных в служебное пользование;
- фиксация результатов проведения антивирусных проверок осуществляется незамедлительно после проведения такой проверки в Журнале учёта проведения антивирусных проверок (форма документа приведена в приложении 1);
- анализ результатов работы средств антивирусной защиты архива;
- организация и проведение мероприятий (технических учёб, обсуждений и др.)по улучшению антивирусной защиты архива, в т.ч. проведение инструктажей для сотрудников архива о работе антивирусного программного обеспечения и возможности заражения автоматизированных рабочих мест, вынесение вопросов и предложений на рассмотрение комиссии архива по защите информации;
- участие в проведении служебных расследований по фактам обнаружения вредоносных программ, повлекших неустойчивую работу и (или) ущерб;
- подготовка ежегодных отчётов о состоянии антивирусной защиты в архиве.

7.4. В основные обязанности системного администратора в рамках организации работ по антивирусной защите в архиве входит:

- установка средств антивирусной защиты на все объекты антивирусной защиты в порядке, описанном в эксплуатационной документации;
- контроль актуальности версий антивирусных баз и модулей сканирования программного обеспечения;
- настройку ежедневных автоматических обновлений и иных параметров средств антивирусной защиты;
- проверка соблюдения порядка и периодичности обновления баз данных средств антивирусной защиты;
- осуществление контроля за состоянием средств антивирусной защиты на серверах архива;
- настройка параметров антивирусного программного обеспечения в архиве в соответствии с официальными руководствами по применению используемых в архиве антивирусных средств;
- проведение работ по обнаружению и обеззараживанию угроз на серверах, ПК сотрудников архива и съёмных носителях информации, выданных в служебное пользование;
- фиксация результатов проведения антивирусных проверок в Журнале учёта проведения антивирусных проверок;
- участие в проведении служебных расследований по фактам обнаружения вредоносных программ, повлекших неустойчивую работу и (или) ущерб;
- проведение периодического анализа и оценки результатов проведения работ по обеспечению антивирусной безопасности, контроль степени защищённости серверов, локальной сети и автоматизированных рабочих мест сотрудников архива, съёмных носителей информации, выданных в служебное пользование, выработка предложений по изменению и улучшению порядка проведения работ;

- хранение физических носителей программного обеспечения архива (установочных дисков, флеш-накопителей и др.);
- формирование отчетов о работе средств антивирусной защиты в случаях возникновения инцидентов, сбоев в работе систем;
- проведение инструктажей для сотрудников архива о работе антивирусного ПО и возможности заражения ПК;
- участие в разработке локальных нормативных актов в сфере обеспечения антивирусной безопасности в архиве.

7.5. В ежегодный отчёт администратора информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации о состоянии антивирусной защиты в архиве для рассмотрения на заседании комиссии архива по защите информации включается следующая информация:

- сведения об установленном программном обеспечении, его производителе и количестве установленных лицензий антивирусных программ на серверы и автоматизированные рабочие места архива;
- количество обнаруженных угроз за данный период, характеристика выявленных уязвимостей и перечень проведённых мероприятий, направленных на их устранение;
- перечень серверов, автоматизированных рабочих мест и съёмных носителей информации, выданных в служебное пользование, на которых обнаружено действие вредоносных программ за рассматриваемый период с указанием имён и должностей сотрудников, ответственных за их эксплуатацию.

7.6. В случае, если инцидентов в работе средств антивирусной защиты за годовой период не наблюдалось, ежегодный отчёт не составляется.

Администратор информационной безопасности вычислительной сети ОИПСиЗИ Е.Ю. Дроздова

__ _____ 2021 г.

Приложение 1

к Инструкции по организации антивирусной защиты

в ГБУТО «Государственный архив Тюменской области»

Форма Журнала учёта проведения в ГБУТО ГАТО Тюменской области» антивирусных проверок

№ п/п	Дата проведения проверки	Отдел	Имя компьютера	Наименование антивирусной программы	Результаты проверки		Примечания (принятые меры)	Фамилия, имя, отчество исполнителя
					Кол-во проверенных файлов	Кол-во и наименования инфицированных файлов, источник поступления (при наличии)		
1	2	3	4	5	6	7	8	9

Приложение 4

Проект Инструкции по работе со съёмными носителями информации
в ГБУТО «Государственный архив Тюменской области»

УТВЕРЖДАЮ
Директор ГБУТО ГАТО
О.П. Тарасова
___ _____ 2021 г.

ИНСТРУКЦИЯ

по работе со съёмными носителями информации
в Государственном бюджетном учреждении Тюменской области
«Государственный архив Тюменской области»

СОГЛАСОВАНО
протоколом заседания комиссии
ГБУТО ГАТО по защите информации
от_____ № ___

Тюмень
2021

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция по работе со съёмными носителями информации в Государственном бюджетном учреждении Тюменской области «Государственный архив Тюменской области» (далее – инструкция) разработана в соответствии с требованиями № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 27002-2012 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» (утв. и введен в действие Приказом Росстандарта от 24.09.2012 N 423-ст).

1.2. Настоящая инструкция регламентирует проведение организационно-технических мер при работе со съёмными носителями информации, в том числе содержащих персональные данные, ГБУТО «Государственный архив Тюменской области» (далее – архив).

1.3. Съёмными носителями информации являются:

– USB-накопители (флеш-диски);

– съёмные накопители на жестких магнитных дисках;

– диски;

– внешние жёсткие диски и др.

1.4. Съёмные накопители применяются для хранения служебной документации, электронных баз данных, персональных данных, передачи сведений во второе здание архива или в сторонние организации, а также в иных целях, обусловленных рабочей необходимостью.

1.5. Ответственность за доведение положений настоящей Инструкции до сотрудников архива, осуществляющих использование съёмных носителей информации возлагается на администратора информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации архива и начальника хозяйственного отдела архива.

1.6. Общий контроль за соблюдением положений настоящей Инструкции в архиве осуществляет заместитель директора, ответственный за контроль за обеспечением информационной безопасности в архиве.

1.7. Действие настоящей Инструкции распространяется на всех сотрудников архива, в ходе осуществления рабочей деятельности которых осуществляется использование съёмных носителей информации.

1.8. Инструкция подлежит пересмотру в случае возникновения необходимости при изменении целей, задач, требований к порядку работы со съёмными носителями.

2. ЦЕЛИ И УСЛОВИЯ ИСПОЛЬЗОВАНИЯ СЪЁМНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

2.1. Под использованием съёмных носителей информации понимается их подключение к информационной системе (серверу или компьютеру госархива) с целью обработки, приёма, передачи данных между такой системой и носителями информации.

2.2. Перед использованием съёмный носитель информации должен быть проверен средствами антивирусной защиты на наличие вредоносных программ, в случае необходимости осуществлено «лечение» заражённых объектов и удаление угроз.

2.3. В архиве допускается использование учтённых съёмных носителей информации, которые являются собственностью архива и подвергаются регулярной ревизии и периодическому антивирусному контролю, а также прошедшим антивирусный контроль носителями информации иных организаций и физических лиц, чьё применение необходимо для реализации функций архива.

3. ПОРЯДОК УЧЁТА И ВЫДАЧИ СЪЁМНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ В ГОСАРХИВЕ

3.1. Учёт и выдача съёмных носителей информации осуществляются начальником хозяйственного отдела архива.

3.2. Носители конфиденциальной информации предоставляются сотрудникам архива по запросу руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника организации производственной необходимости.

3.3. Все находящиеся на хранении и в обращении съёмные носители информации архива, в том числе содержащие персональные данные, подлежат учёту.

3.4. Учёт съёмных накопителей ведётся начальником хозяйственного отдела госархива в Журнале учёта съёмных носителей информации ГБУТО ГАТО (форма документа представлена в Приложении 1).

3.5. Соответствующие записи в Журнале учёта съёмных носителей информации делаются при выдаче съёмного носителя информации в служебное пользование и возвращении его по результатам проведения работ либо в случае утраты.

3.6. Каждый съёмный носитель с записанными на нём персональными данными должен иметь уникальный учётный номер. Допускается проставление учётного номера на самом носителе информации несмываемыми средствами записи.

3.7. Допускается не наносить учётный номер на съёмный носитель информации, хранение персональных данных на котором не предполагается.

3.8. Сотрудниками архива, в ходе осуществления рабочей деятельности которых применяются съёмные носители информации, должно гарантироваться текущее хранение таких носителей в местах не доступных для доступа

посторонних лиц. В случае хранения на носителе сведений ограниченного доступа хранение осуществляется в местах не доступных также для других сотрудников архива – в запирающихся шкафах или сейфах.

3.9. Сотрудники архива получают учтённый съёмный носитель информации на конкретный срок – для выполнения определённых работ. Возможна выдача съёмного носителя информации сотруднику архива на весь период осуществления им рабочей деятельности.

3.10. По окончании работ сотрудник архива сдает съёмный носитель информации начальнику хозяйственного отдела, о чём делается соответствующая запись в Журнале учёта съёмных носителей информации.

3.11. В случае выдачи съёмного носителя информации сотруднику архива на длительный срок, наличие и состояние такого носителя подлежит проверке, которую один раз в год осуществляет начальник хозяйственного отдела.

4. ПОРЯДОК ИСПОЛЬЗОВАНИЯ СЪЁМНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

4.1. Применение съёмных носителей информации сотрудникам архива, в ходе осуществления рабочей деятельности которых необходимо использование таких носителей, допускается исключительно для выполнения служебных обязанностей.

4.2. При использовании съёмных носителей информации сотрудникам запрещается:

- использовать съёмные носители информации в личных целях;
- передавать съёмные носители информации другим лицам;
- хранить съёмные носители, использующиеся для хранения конфиденциальной информации (персональные данные), вместе с носителями открытой информации;
- оставлять съёмные носители информации на рабочих столах, оставлять их без присмотра в случае нахождения в рабочем помещении посторонних лиц, передавать съёмные носители информации на хранение другим лицам.

4.3. Любое взаимодействие (обработка, приём, передача информации) инициированное сотрудником организации между серверами, автоматизированными рабочими местами архива и неучтёнными (личными) носителями информации рассматривается как несанкционированное (за исключением случаев, отдельно оговорённых с администратором информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации архива).

4.4. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициируется служебная проверка, проводимая комиссией госархива по защите информации на основании служебной записки сотрудника, установившего факт фактов несанкционированного и/или нецелевого использовании носителей информации.

4.5. В случае необходимости по факту выясненных обстоятельств составляется докладная записка или акт расследования инцидента, который (-ая) передаётся заместителю директора, ответственному за контроль за обеспечением информационной безопасности в архиве.

4.6. Съёмные носители информации при каждом их использовании подлежат обязательной антивирусной проверке.

4.7. При передаче информации адресатам с использованием съёмных носителях информации на них записываются только предназначенные адресатам данные.

4.8. Перед передачей съёмного носителя информации архива для записи данных сторонней организацией, съёмный носитель информации подлежит форматированию.

4.9. Вынос съёмных носителей информации архива для непосредственной передачи адресату осуществляется только после уведомления администратора информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации архива и регистрации факта такого перемещения в Журнале учёта вноса/выноса съёмных носителей информации ГБУТО ГАТО (форма документа представлена в Приложении 2).

4.10. В случае утраты или непреднамеренного уничтожения съёмных носителей информации либо разглашения содержащихся в них конфиденциальных сведений немедленно ставится в известность администратор информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации. Сотрудником, допустившим утрату или непреднамеренное уничтожение съёмных носителей информации составляется объяснительная записка, которая передаётся администратору информационной безопасности вычислительной сети. На её основании администратором информационной безопасности вычислительной сети составляется докладная записка с объяснением всех установленных фактов происшествия, которая предоставляется комиссии госархива по защите информации для вынесения решения. Соответствующие отметки об утрате или непреднамеренном уничтожении съёмных носителей информации вносятся в Журнал учёта съёмных носителей информации архива в графу «Примечания».

4.11. Съёмные носители информации, пришедшие в негодность по каким-либо причинам (техническая поломка, невозможность использования в аппаратных технических средствах и др.), подлежат уничтожению. Уничтожение съёмных носителей с конфиденциальной информацией осуществляется начальником хозяйственного отдела архива. По результатам уничтожения носителей составляется акт (форма документа представлена в Приложении 3). Соответствующие отметки вносятся в Журнал учёта съёмных носителей информации архива.

4.12. В случае увольнения или перевода работника в другое структурное подразделение на должность, которой для исполнения служебных обязанностей съёмный носитель информации не требуется, предоставленные ранее носители сдаются начальнику хозяйственного отдела архива. Соответствующие отметки вносятся в Журнал учёта съёмных носителей информации архива.

5. ОТВЕТСТВЕННОСТЬ

5.1. Сотрудники архива, в ходе осуществления рабочей деятельности которых необходимо использование съёмных носителей информации, несут ответственность за обеспечение сохранности и соблюдение правил эксплуатации съёмных носителей информации.

5.2. Сотрудники архива, в ходе осуществления рабочей деятельности использующие съёмные носители, обязаны ставить в известность о возникновении любых фактов нарушения требований эксплуатации и хранения съёмных носителей информации архива начальника подразделения, в котором работают, начальника отдела информационно-поисковых систем и защиты информации и администратора информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации архива.

Администратор информационной безопасности вычислительной сети ОИПСиЗИ Е.Ю. Дроздова

__ _____ 2021 г.

Приложение 1

к Инструкции по работе со съёмными носителями информации

в ГБУТО «Государственный архив Тюменской области»

Форма Журнала учёта съёмных носителей информации ГБУТО ГАТО

№ п/п	Учётный номер носителя	Вид и описание носителя	ФИО сотрудника, которому произведена выдача	Дата выдачи	Подпись получателя	Дата возврата носителя	Подпись сдатчика	Подпись получателя	№ и дата уничтожения информации, содержащейся на носителе (полное форматирование)	Примечания
1	2	3	4	5	6	7	8	9	10	11

Приложение 2

к Инструкции по работе со съёмными носителями информации

в ГБУТО «Государственный архив Тюменской области»

Форма Журнала учёта вноса/выноса съёмных носителей информации ГБУТО ГАТО

№ п/п	Дата выноса съёмного носителя информации из рабочего помещения госархива	Цель выноса съёмного носителя информации	Наименование и адрес учреждения, в которое осуществляется вынос	Наименование структурного подразделения и ФИО должностного лица, которому передаётся съёмный носитель информации	ФИО сотрудника, ответственного за использование съёмного носителя информации, осуществляющего его вынос	Подпись сотрудника, осуществляющего вынос съёмного носителя информации	Дата возврата съёмного носителя информации в рабочее помещение госархива	Подпись сотрудника, ответственного за использование съёмного носителя информации, в его возврате	Примечания
1	2	3	4	5	6	7	8	9	10

Приложение 3
к Инструкции по работе со съёмными носителями информации
в ГБУТО «Государственный архив Тюменской области»

Форма Акта об уничтожении съёмных носителей информации

**ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ТЮМЕНСКОЙ ОБЛАСТИ
«ГОСУДАРСТВЕННЫЙ АРХИВ
ТЮМЕНСКОЙ ОБЛАСТИ»
(ГБУТО ГАТО)**

АКТ
№
об уничтожении
съёмных носителей информации

Комиссия по защите информации в составе председателя _____

членов комиссии – _____

_____

_____

провела отбор _____ носителей информации

(бумажных, электронных, магнитных, оптических)

в количестве _____

и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит гарантированному уничтожению.

Комиссия составила настоящий акт о том, что произведено уничтожение съёмных носителей информации в следующем составе:

№ п/п	Дата уничтожения	Тип носителя	Учетный номер носителя	Примечание
1	2	3	4	5

Всего уничтожено _____ носителей.
(цифрами и прописью количество)

На указанных съёмных носителях информации данные уничтожены путём _____
(форматирования, повреждение материального носителя)

Перечисленные съёмные носители информации уничтожены путём

_____
(разрезания / сжигания / размагничивания / физического или механического уничтожения / иного способа)

Председатель комиссии: _____ Фамилия И.О.

Члены комиссии: _____ Фамилия И.О.

_____ Фамилия И.О.

_____ Фамилия И.О.

Приложение 5

Проект Инструкции по организации парольной защиты
в ГБУТО «Государственный архив Тюменской области»

УТВЕРЖДАЮ
Директор ГБУТО ГАТО
О.П. Тарасова
____ _____ 2021 г.

ИНСТРУКЦИЯ
по организации парольной защиты
в Государственном бюджетном учреждении Тюменской области
«Государственный архив Тюменской области»

СОГЛАСОВАНО
протокол заседания комиссии ГБУТО
ГАТО по защите информации
от_____ № ___

Тюмень
2021

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1. Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

2. Информационная система персональных данных – 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.

3. Компрометация – факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

4. Объект доступа - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

5. Пароль - уникальный признак субъекта

6. Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

7. Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

8. Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция разработана в соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Инструкция по организации парольной защиты ГБУТО «Государственный архив Тюменской области» (далее – архив) определяет требования к организации парольной защиты в архиве при осуществлении сотрудниками должностных обязанностей с использованием средств автоматизации, в том числе определяет порядок генерации, использования, смены и прекращения действия паролей сотрудников, а также контроль действий пользователей при работе с паролями.

1.3. Действие настоящей Инструкции распространяется на всех сотрудников архива.

1.4. Доведение положений Инструкции до сотрудников архива осуществляется администратором информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации архива под подпись в Журнале ознакомления сотрудников ГБУТО ГАТО с локальными нормативными актами по защите информации (форма документа представлена в Приложении 1).

1.5. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль за реализацией требований по обеспечению безопасности при использовании паролей возлагается на системного администратора отдела информационно-поисковых систем и защиты информации архива.

1.6. Ответственность за неразглашение паролей лежит на системном администраторе отдела информационно-поисковых систем и защиты

информации архива и сотруднике, которому был выдан пароль, а также на иных должностных лицах, которым в ходе выполнения служебных обязанностей стали доступны данные сведения.

1.7. Общий контроль за соблюдением требований парольной защиты в архиве осуществляет администратор информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации архива.

1.8. В целях закрепления знаний по вопросам практического выполнения требований настоящей Инструкции, разъяснения возникающих вопросов, системным администратором и администратором информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации архива могут проводятся групповые и индивидуальные инструктажи.

1.10. Ответственные сотрудники, на которых возлагаются обязанности по обеспечению парольной защиты в госархиве, имеют полноправный доступ ко всем автоматизированным рабочим местам, установленному программному обеспечению архива.

1.12. Настоящая Инструкция подлежит пересмотру в случае существенного изменения условий или порядка работы с парольной информацией в архиве.

2. ТРЕБОВАНИЯ К ГЕНЕРАЦИИ ПАРОЛЕЙ

2.1. Пароли сотрудников архива к различным системам должны отвечать следующим требованиям:

- Длина пароля для учётных записей сотрудников, осуществляющих автоматизированную обработку информации, составляющей персональные данные, должна составлять не менее 8 символов. Для учётных записей, используемых при авторизации в иных программных комплексах количество парольных символов ограничений не имеет.

– В числе символов пароля для учётных записей сотрудников обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

2.2. Пароль не должен включать в себя:

- легко вычисляемые сочетания символов;
- клавиатурные последовательности символов и знаков;
- общепринятые сокращения;
- аббревиатуры;
- номера телефонов, автомобилей;
- прочие сочетания букв и знаков, ассоциируемые с пользователем.

2.3. Для сотрудников архива, не имеющих доступ к обработке персональных данных в автоматизированном виде или полномочий администратора системы, допускается использование единого пароля для доступа к различным информационным ресурсам. Для сотрудников, осуществляющих автоматизированную обработку информации, составляющей персональные данные, для каждой системы должен быть присвоен уникальный пароль.

3. МЕРОПРИЯТИЯ ПРИ СМЕНЕ ПАРОЛЯ

3.1. Плановое удаление или блокировка учётной записи сотрудника архива производится в следующих случаях:

– по окончании срока действия пароля;

– в случае прекращения полномочий пользователя.

3.2. Внеплановая замена паролей сотрудников архива проводится в следующих случаях:

– при смене сотрудника, имеющего доступ к логину и паролю общего профиля архива (например, официальной электронной почте);

– в случае компрометации паролей нескольких сотрудников;

- в случае прекращения полномочий системного администратора, администратора информационной безопасности вычислительной сети отдела информационно-поисковых систем и защиты информации архива или других сотрудников, которым в связи с выполнением должностных обязанностей были предоставлены полномочия по управлению парольной защитой;
- при обнаружении факта успешной попытки несанкционированного доступа;

при обнаружении факта компрометации пароля.

3.3. Порядок внеплановой смены пароля аналогичен порядку плановой смены пароля.

3.4. В случае компрометации личного пароля пользователя сотрудник архива обязан незамедлительно уведомить о таком факте системного администратора. Системный администратор незамедлительно ограничивает доступ к учётной записи сотрудника. Для сотрудника создаётся новая учётная запись пользователя или производится изменения пароля путём восстановления доступа к системе с учётом технических возможностей информационной системы, пароль к которой был скомпрометирован.

3.5. Восстановление утраченного по каким-либо причина пароля пользователя осуществляется системным администратором путём изменения (сброса) основного пароля пользователя на первичный пароль с учётом технических возможностей информационной системы на основании заявки пользователя, направленной в любом виде. Для пользователей, осуществляющих автоматизированную обработку персональных данных, такая заявка составляется в бумажной форме.

4. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ПРИ РАБОТЕ С СИСТЕМАМИ, ПРЕДУСМАТРИВАЮЩИМИ ПАРОЛЬНУЮ ЗАЩИТУ

4.1. При работе с парольной защитой пользователям запрещается:

- разглашать кому-либо персональный пароль и прочие идентифицирующие сведения, позволяющие получить доступ к используемым в работе информационным системам;
- предоставлять доступ от своей учётной записи посторонним лицам;
- записывать пароли на бумаге, в электронной форме, размещать их на съёмных носителях информации.

4.2. Сотрудники архива обязаны своевременно сообщать лицам, ответственным за обеспечение безопасности информации в архиве, обо всех нештатных ситуациях, нарушениях работы используемого в целях защиты от несанкционированного доступа программного обеспечения, возникающих при работе с паролями.

4.3. При вводе пароля сотрудник обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

4.4. При наличии в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и иных ситуациях необходимости использования идентификаторов и паролей сотрудников архива в их отсутствие другими должностными лицами, такие сотрудники обязаны сразу же после выхода произвести смену своих паролей совместно с системным администратором отдела информационно-поисковых систем и защиты информации архива.

5. МЕРОПРИЯТИЯ, ПРОВОДИМЫЕ В СЛУЧАЯХ КОМПРОМЕТАЦИИ ПАРОЛЕЙ

5.1. Под компрометацией следует понимать:

- утеря физического носителя с парольной информацией;
- передача идентификационной информации по открытым каналам связи;

- проникновение постороннего лица в помещение физического хранения носителя парольной информации или подозрение факта такого проникновения (срабатывание сигнализации, повреждение слепков печатей, повреждение замков и т. п.);
- визуальный осмотр носителя идентификационной информации посторонним лицом;
- перехват пароля при распределении идентификаторов;
- сознательная передача парольной информации сотрудником архива постороннему лицу.

5.2. Действия при компрометации пароля:

- для системного администратора отдела информационно-поисковых систем и защиты информации – с учётом технических возможностей информационной системы скомпрометированный подлежит сбросу, взамен его вводится запасной или новый пароль;
- для сотрудников – о компрометации пароля к информационной системе немедленно оповещаются все участники, участвующие в процедуре обмена информацией в этой системе.

5.3. По каждому случаю, связанному с компрометацией действующих паролей, администратором информационной безопасности вычислительной сети принимается решение об организации служебного расследования комиссией госархива по защите информации.

5.4. О фактах проведения служебного расследования уведомляются в виде служебной записки директор и заместитель директора, ответственный за контроль за обеспечением информационной безопасности в архиве.

6. ОТВЕТСТВЕННОСТЬ

6.1. Сотрудники архива, которым в целях выполнения служебных обязанностей выдаётся пароль к информационным системам, должны быть ознакомлены под подпись с требованиями настоящей Инструкции, а также предупреждены об ответственности за разглашение парольной информации.

6.2. Ответственность за техническую часть организации парольной защиты (генерация, смена, восстановление и др.) возлагается на системного администратора отдела информационно-поисковых систем и защиты информации архива.

6.3. Все создаваемые пароли заносятся системным администратором отдела информационно-поисковых систем и защиты информации архива в электронный Журнал учёта логинов и паролей сотрудников ГБУТО ГАТО в электронном виде в защищённом паролем файле (форма документа представлена в Приложении 2). В журнале на каждого сотрудника в табличной форме вносится следующая информация:

- фамилия и инициалы сотрудника архива;
- должность с указанием отдела;
- сведения о программном комплексе или базе данных, к которому создаётся учётная запись;
- логин и пароль к системе;
- дата присвоения идентификатора и пароля.

6.4. При изменении пароля уже существующей учётной записи в новую запись в Журнале вносятся сведения об изменённом пароле, дате и причинах осуществления изменений. Старая запись зачёркивается, удалению не подлежит.

Администратор информационной безопасности вычислительной сети ОИПСиЗИ Е.Ю. Дроздова

__ _____ 2021 г.

Приложение 1

к Инструкции по организации парольной защиты

в ГБУТО «Государственный архив Тюменской области»

Форма Журнала ознакомления сотрудников ГБУТО ГАТО с локальными нормативными актами по защите информации

№ п/п	ФИО сотрудника	Название документа	Дата ознакомления	Подпись сотрудника в ознакомлении	Примечания
1	2	3	4	5	6

Приложение 2

к Инструкции по организации парольной защиты

в ГБУТО «Государственный архив Тюменской области»

Форма Журнала учёта логинов и паролей сотрудников ГБУТО ГАТО

Ф.И.О. сотрудника	Отдел, занимаемая должность	Наименование программного комплекса или базы данных, в котором создаётся учётная запись	Логин	Пароль	Дата присвоения идентификаторов	Примечания
1	2	3	4	5	6	7