ДЕПАРТАМЕНТ ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ СМОЛЕНСКОЙ ОБЛАСТИ

П Р И К А З

"16" августа 2019 г. № 40/01-01

Об утверждении Политики
информационной безопасности
Департамента промышленности
и торговли Смоленской области

Во исполнение требований ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

п р и к а з ы в а ю:

1. Утвердить Политику информационной безопасности Департамента промышленности и торговли Смоленской области (Приложение 1-11).
2. Опубликовать Политику информационной безопасности Департамента промышленности и торговли Смоленской области (далее – Департамент) на официальном сайте Департамента в информационно-телекоммуникационной сети Интернет.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник Департамента **А.А. Афонычев**

Приложение № 1

Утверждено

приказом начальника
Департамента промышленности и
торговли Смоленской области
от 16.08.2019 № 40/01-01

Политика информационной безопасности Департамента промышленности и торговли Смоленской области

Содержание:

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

АИС	Автоматизированная информационная система
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БД	База данных
ВТСС	Вспомогательные технические средства и системы
ВЧВС	Виртуальная частная вычислительная сеть
ЕСКД	Единая система конструкторской документации
ЕСПД	Единая система программной документации
ЕСТД	Единая система технологической документации
ЗИ	Защита информации
ЗП	Защищаемое помещение
ИБ	Информационная безопасность
ИТКС	Информационно-телекоммуникационная система
КЗ	Контролируемая зона
КСЗИ	Комплексная система защиты информации
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОБИ (ОИБ)	Обеспечение безопасности информации
ОТСС	Основные технические средства и системы
ПО	Программное обеспечение
ПС	Программные средства
РД	Руководящий документ
СЗИ НСД	Система защиты информации от НСД
СКЗИ	Средство криптографической защиты информации
СПД	Система передачи данных
СПО	Специальное программное обеспечение
СТК	Система телекоммуникаций;
СУБД	Система управления базами данных
ТП	Технический проект
ТТ	Технические требования
УЦ	Удостоверяющий центр
ФСБ России	Федеральная служба безопасности России

ФСТЭК России	Федеральная служба по техническому и экспертному контролю России
ЭЦП	Электронная цифровая подпись

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

АУТЕНТИФИКАЦИЯ – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

АДМИНИСТРАТОР ЗАЩИТЫ - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ -состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

ВСПОМОГАТЕЛЬНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА И СИСТЕМЫ - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях

ДОСТУП К ИНФОРМАЦИИ - ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

ЗАЩИТА ИНФОРМАЦИИ (ЗИ) - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию.

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА – деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

ЗАЩИЩАЕМАЯ ИНФОРМАЦИЯ - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

ЗАЩИЩАЕМЫЕ ПОМЕЩЕНИЯ – помещения, специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

ЗАЩИЩЕННОЕ СРЕДСТВО ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ (ЗАЩИЩЕННАЯ АВТОМАТИЗИРОВАННАЯ СИСТЕМА) – средство вычислительной техники (автоматизированная система), в которой реализован комплекс средств защиты.

ИНФОРМАЦИОННЫЕ РЕСУРСЫ – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)

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

ИДЕНТИФИКАТОР ДОСТУПА – уникальный признак субъекта или объекта доступа.

КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ – совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

КОНТРОЛИРУЕМАЯ ЗОНА - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств.

КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

НАРУШИТЕЛЬ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА – субъект доступа, осуществляющий несанкционированный доступ к информации.

ОБЪЕКТ ДОСТУПА – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ – содержание и порядок действий по обеспечению защиты информации

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА И СИСТЕМЫ - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации

ПАРОЛЬ – идентификатор субъекта доступа, который является его (субъекта) секретом.

СИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА – совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах

САНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ – доступ к информации, не нарушающий правила разграничения доступа.

СЕРТИФИКАТ ЗАЩИТЫ – документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА - комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

СРЕДСТВО ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА – программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ – реализующие алгоритмы криптографического преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи.

СУБЪЕКТ ДОСТУПА – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ – устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

3.ОБЩИЕ ПОЛОЖЕНИЯ

3.1.Назначение Политики

Настоящая Политика определяет систему взглядов на проблему обеспечения комплексной безопасности информации и устанавливает порядок организации и правила обеспечения информационной безопасности в Департаменте, распределение функций и ответственности за обеспечение информационной безопасности между подразделениями и сотрудниками Департамента, требования по информационной безопасности к информационным средствам, применяемым в Департаменте. Документ представляет собой методологическую основу для разработки и реализации комплексных целевых программ обеспечения защиты информации на объектах информатизации Департамента.

3.2. Сфера применения Департамента

Требования настоящей Политики обязательны для всех структурных подразделений Департамента и распространяются на:

- автоматизированные системы Департамента;
- средства телекоммуникаций;
- помещения;
- сотрудников Департамента.

Внутренние документы Департамента, затрагивающие вопросы, рассматриваемые в данном документе, должны разрабатываться с учетом положений Политики и не противоречить им.

3.3.Правовая основа Политики

Правовую основу Концепции составляют:

- Конституция Российской Федерации;
- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 26.07.2006 № 149-ФЗ;
- Федеральный закон «О персональных данных» от 27.07.06 № 152-ФЗ;

– другие законодательные акты, руководящие и нормативно-методические документы Российской Федерации в области обеспечения информационной безопасности.

3.4.Цели и задачи обеспечения безопасности информации

Главная цель обеспечения безопасности информации, циркулирующей в Департаменте - реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационно-телекоммуникационной системы Департамента.

Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в Департаменте;
- предотвращение нарушений прав личности клиентов на сохранение конфиденциальности информации, циркулирующей в Департаменте
- предотвращение несанкционированных действий по блокированию информации;

Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;
- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам Департамента, нарушению нормального функционирования и развития Департамента;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;
- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

- создание условий для максимально возможного возмещения и локализации наносимого интересам Департамента ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности;
- разработка нормативно-правовой базы обеспечения информационной безопасности, координация деятельности подразделений Департамента по обеспечению защиты информации;
- развитие системы защиты, совершенствование ее организации, форм, методов и средств, предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;
- создание и применение защищенных информационных объектов и АИС, центров обработки защищаемой информации;
- развитие и совершенствование защищенного юридически значимого электронного документооборота.
- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности
- создание механизмов управления системой информационной безопасности;

4. ОБЪЕКТЫ ЗАЩИТЫ

4.1. Объектами защиты Департамента являются:

- информационные ресурсы;
- средства и системы обработки информации;
- средства и системы защиты информации, в т.ч. криптографической защиты информации;
- помещения или объекты, предназначенные для ведения закрытых переговоров.

4.2. Информационные ресурсы Департамента

Под информационными ресурсами в Департаменте понимаются совокупности сведений в электронном и бумажном виде (база данных и другие виды информационных массивов), поддерживаемые программно-техническими средствами автоматизированной информационной системы. Информационные ресурсы представляют собой хранилища данных, из которого путем специализированной обработки пользователю предоставляется информация на электронных или бумажных носителях, в том числе в виде отдельных фрагментов баз данных, отчетов и справок.

Технологической основой формирования информационных ресурсов является программно-техническая среда автоматизированных информационных систем, используемых в Департаменте.

Используемые в информационных системах Департамента технологии взаимодействия при обработке информационных ресурсов включают:

- электронную почту (протоколы SMTP и IMAP);
- электронный обмен файлами (протокол FTP);
- обмен файлами на магнитных носителях в формате XML;
- Web - доступ к ресурсам сети (протоколы HTTP/HTTPS/HTML);
- технологию терминального доступа для взаимодействия с удаленными пользователя (протокол RDP);

Основным источником информации для наполнения первичных баз данных ИТКС являются документы и сообщения, поступающие от структурных подразделений Департамента и внешних организаций.

Вся информация, хранимая, обрабатываемая или передаваемая в рамках подразделений Департамента с использованием информационной системы, классифицирована по степени важности и критичности.

Конфиденциальная информация

К конфиденциальной относится информация, составляющая коммерческую тайну, информация о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющая идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях, а также любая другая закрытая информация, являющаяся собственностью Департамента. При обработке этой информации необходимо соблюдать требования "Специальных требований и рекомендаций по защите информации с ограниченным доступом, обрабатываемой техническими средствами (СТР-К)" Государственной технической комиссии при Президенте РФ, положения Федерального закона «О персональных данных», а также прочих нормативных правовых актов, регламентирующих работу с конфиденциальной информацией.

При хранении, передаче и обработке данной информации необходимо обеспечить максимальный уровень её защиты.

Служебная информация

К служебной информации могут быть отнесены любые сведения, относящиеся к деятельности подразделений Департамента, несанкционированное распространение которых может привести к отрицательным экономическим, этическим или иным последствиям для Департамента. Хранение, обработка и передача такой информации должна осуществляться в соответствии с требованиями настоящего документа.

Рабочая информация

Рабочая информация включает в себя сведения, имеющие отношение к внутренней деятельности подразделений Департамента и не относящиеся к конфиденциальной или служебной информации. При хранении, передаче и

обработке такой информации необходимо обеспечить максимальный уровень её целостности и аутентичности в соответствии с положениями настоящего документа.

Прочие виды информации

Для прочих видов информации порядок хранения, передачи и обработки с использованием автоматизированных систем не регламентируется.

4.3. Средства и системы обработки информации

Средства и системы обработки информации Департамента представляют собой совокупность программного обеспечения и технических средств обработки и передачи информации, а также систему телекоммуникаций (СТК).

Техническое обеспечение (ТО) включает следующие компоненты:

- серверные комплексы (платформы);
- рабочие станции пользователей;
- технические средства ввода/вывода информации:
- сканеры;
- принтеры.
- средства хранения и архивирования данных;
- активное и пассивное оборудование локальной вычислительной сети (ЛВС);
- средства бесперебойного питания.

Система телекоммуникаций (СТК), поддерживает информационный обмен между внутренними абонентами и информационными системами Департамента, а также информационную связь с внешними абонентами. В системной архитектуре СТК выделены следующие функциональные подсистемы:

- Транспортная подсистема;
- Ведомственная телефонная сеть;
- Подсистема удаленного доступа к информационным ресурсам;
- Подсистема электронной почты;
- Подсистема сервисов глобальной сети Интернет;
- Подсистема управления, мониторинга и обслуживания СТК.

В состав **программного обеспечения** информационных систем входят:

- общесистемное программное обеспечение;
- специальное (прикладное) программное обеспечение.

Общесистемное программное обеспечение включает в себя:

- серверные и клиентские операционные системы;
- СУБД;
- пакеты офисных программ;
- антивирусные программы;
- пакеты программ для групповой работы
- терминальные серверные и клиентские программы
- средства электронной почты;
- средства управления информационной безопасностью;
- средства управления и администрирования системой;

Специальное программное обеспечение (СПО) является совокупностью аналитических и логических методов и алгоритмов, программ их реализации, отражающих специфику автоматизируемых процессов и предназначенных для обеспечения деятельности должностных лиц Департамента.

4.4. Средства обеспечения

Под средствами обеспечения Департамента понимаются вспомогательные инженерно-технические системы, не участвующие в обработке информации, содержащей конфиденциальные сведения. В общем виде к этим системам относятся:

- системы электропитания и заземления объектов;
- системы связи (ведомственной, междугородней, городской, внутренней), не предназначенной для закрытых переговоров;
- системы пожарной и охранной сигнализации;
- электронные системы контроля и управления доступом на территорию и в помещения;
- системы громкоговорящей связи и оповещения;
- системы кондиционирования, отопления и воздухоснабжения.

4.5. Объекты, предназначенные для ведения закрытых переговоров

В качестве объектов, предназначенных для ведения закрытых переговоров, необходимо рассматривать следующие помещения центрального аппарата и территориальных органов Департамента:

- кабинеты руководящего состава, используемые для обсуждения конфиденциальной информации;
- помещения для проведения совещаний и переговоров по конфиденциальным вопросам (комнаты переговоров, конференц - залы);
- другие помещения, в том числе и технические, в которых может обсуждаться конфиденциальная информация.

5. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ДЕПАРТАМЕНТЕ

5.1. Основные факторы, воздействующие на информационную безопасность Департамента»

Основными факторами, воздействующими на информационную безопасность Департамента, являются:

- Природный фактор. Совокупность угроз природного характера, являющихся следствием воздействия естественной непреодолимой силы (стихии) – землетрясения, наводнения, метеорологические катаклизмы и т.п., приводящие к устойчивому нарушению функционирования информационных и телекоммуникационных ресурсов, вплоть до их утраты или физического уничтожения. Вероятность определяется спецификой территории, на которой дислоцируется защищаемый объект – многолетними метеорологическими наблюдениями, геотектоническими данными и др.
- Техногенный фактор. Совокупность угроз искусственного характера, вызванных результатами человеческой деятельности (цивилизации) – пожары, взрывы, затопления, радиационные и химические заражения, энергетические аварии, разрешение коммуникаций, в том числе – в результате террористических актов, диверсий, массовый беспорядков и ведения боевых действий.
- Системный фактор. Возникновение угрозы целостности информации и (или) функционированию информационно-телекоммуникационных средств, систем и сетей в результате ошибок в их проектировании и разработке или возникновения внутрисистемных сбоев (фатальных ошибок) при их эксплуатации, в том числе – из-за несовершенства или конфликтов программного обеспечения или неисправности оборудования.
- Человеческий фактор. Возникновение угрозы безопасности информации в результате отсутствия профессиональных навыков, недостаточной подготовки, халатности, ненадлежащего исполнения обязанностей или злого умысла персонала, эксплуатирующего

информационно-телекоммуникационные средства, системы и сети, разработчиков программного обеспечения и пользователей, имеющих допуск к информации на законном основании. Нарушение правил эксплуатации ЭВМ, их систем и сетей лицами, ответственными за эту работу.

- Криминальный фактор. Целенаправленное внешнее воздействие на информационные ресурсы и информационно-телекоммуникационные средства, системы и сети («атаки», вторжения) с целью уничтожения, блокирования или копирования информации, разработка и внедрение вредоносных программ (вирусов, симуляторов, «троянских» программ, клавиатурных перехватчиков и др.) внедрение специальных технических средств для негласного получения информации.

5.2. Угрозы безопасности информации и их источники

Информация, обрабатываемая в ИТКС Департамента, дает потенциальную возможность для проявления угроз безопасности, вызванных действиями, процессами или явлениями, приводящими к нанесению ущерба Департамента. Предусматривается два типа угроз безопасности:

- связанные с утечкой информации (разглашение, утечка, несанкционированный доступ);
- связанные с несанкционированным воздействием на информацию и ее носители (искажение, уничтожение, копирование, блокирование, утрата, сбой функционирования носителя информации, сбои и ошибки техники, ошибки пользователей, природные явления, другие случайные воздействия).

Основными источниками угроз безопасности информации являются:

- Стихийные: Стихийные бедствия, катаклизмы;
- Техногенные: аварии, сбои и отказы оборудования (технических средств);
- Ошибки проектирования и разработки компонентов АС (аппаратных средств, технологии обработки информации, программного обеспечения и т. п.);
- Антропогенные: Ошибки эксплуатации;

– Антропогенные: Преднамеренные действия нарушителей и злоумышленников.

5.3. Классификация способов реализации угроз информационной безопасности

Угрозы информационной безопасности по отношению к защищаемым объектам могут быть разделены на:

– угрозы, связанные с применением технических средств;

– угрозы, связанные с использованием программного обеспечения;

– угрозы, связанные с нарушением технологического процесса обмена данными;

– угрозы, связанные с использованием сетей передачи данных.

5.4. Пути реализации непреднамеренных субъективных угроз безопасности информации

Пользователи, операторы, системные администраторы и сотрудники, обслуживающие информационные системы Департамента, являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций и процедур.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз информационной безопасности (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла) следующие:

– Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств: отключению оборудования или изменению режимов работы устройств и программ; разрушению информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение программ или файлов с важной информацией, в том числе системных, повреждение каналов связи, неумышленная порча носителей информации и т.п.)

- Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.)
- Несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т.п.)
- Непреднамеренное заражение компьютера вирусами
- Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования или ЭЦП, идентификационных карточек, пропусков и т.п.)
- Игнорирование организационных ограничений (установленных правил) при работе в системе
- Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом подразделения безопасности
- Ввод ошибочных данных

5.5. Пути реализации преднамеренных субъективных угроз безопасности информации

Основные возможные пути умышленной дезорганизации работы, вывода информационных систем Департамента из строя, проникновения в систему и несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.) могут быть следующими:

- Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов автоматизированной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.), отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, линий связи и т.п.)

- Хищение носителей информации (распечаток, магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ), хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.)
- Несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств.
- Использование чужих прав по доступу к ресурсам АС путем незаконного получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы программными закладками и т.д.).
- Несанкционированное использование АРМ пользователей, имеющих уникальные физические характеристики, такие как имя рабочей станции в сети, физический адрес, адрес в системе связи и другие.
- Несанкционированная модификация программного обеспечения – внедрение программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи защищаемой информации или дезорганизации функционирования АС
- Перехват данных, передаваемых по каналам связи, и их анализ с целью получения сведений, в том числе ограниченного распространения и выяснения протоколов обмена, правил вхождения в связь и авторизации пользователей и последующих попыток их имитации для проникновения в систему
- Вмешательство в процесс функционирования АС сетей общего пользования с целью несанкционированной модификации данных, доступа к сведениям ограниченного распространения, дезорганизации работы подсистем АС и т.п.

5.6. Пути реализации непреднамеренных техногенных угроз безопасности информации

- закупки несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;
- аварии в системах электропитания;
- аварии в системах отопления и водоснабжения в непосредственной близости к техническим средствам обработки информации;
- нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи);
- неумышленное повреждение внешних кабельных систем связи строительными организациями, физическими лицами и т.п. в результате проведения несогласованных работ в местах прокладки кабелей связи;
- возникновение пожаров в непосредственной близости к техническим средствам обработки информации в результате неисправной электропроводки, неисправных технических средств, нарушения сотрудниками правил противопожарной безопасности.

5.7. Пути реализации непреднамеренных стихийных угроз безопасности информации

- Разрушение зданий, отдельных помещений, в которых установлены технические средства обработки информации, хранилища данных в результате стихийных бедствий (наводнений, землетрясений, ураганов) в районе размещения объекта информатизации Департамента
- воздействие атмосферного электричества на технические средства обработки информации и системы обеспечения (электропитание, охранная, пожарная сигнализация и т.п.)
- возникновение стихийных очагов пожаров (лесные пожары) в непосредственной близости от объекта информатизации Департамента

5.8. Классификация нарушителей информационной безопасности Департамента

При анализе угроз информационной безопасности используется модель нарушителя по признаку принадлежности к Департаменту. В соответствии с этой моделью все нарушители делятся на две основные группы: внутренние и внешние.

Под внутренними нарушителями подразумеваются все сотрудники Департамента, имеющие санкционированный доступ на территорию Департамента или к ресурсам АС. Под внешними нарушителями подразумеваются все остальные лица.

Внутренним нарушителем может быть лицо из следующих категорий сотрудников:

- пользователи информационных ресурсов;
- обслуживающий персонал (системные администраторы, администраторы АС, администраторы баз данных, инженеры);
- сотрудники-программисты, сопровождающие системное, общее и прикладное программное обеспечение;
- другие сотрудники подразделений Департамента, имеющие санкционированный доступ в здания, где расположено оборудование передачи и обработки информации Департамента.

Предполагается, что несанкционированный доступ на объекты Департамента посторонних лиц исключается организационными мерами (охрана территории, организация пропускного режима).

Внешние нарушители информационной безопасности:

- лица, самостоятельно осуществляющие создание методов и средств реализации атак, а также самостоятельно реализующие атаки, совершающие свои действия с целью нанесения ущерба Департамента (съем информации, искажение информации, разрушение системного или прикладного ПО);

Потенциальные нарушители делятся на три группы:

1 группа - субъекты, не имеющие доступ в пределы контролируемой зоны Департамента.

2 группа - субъекты, не имеющие доступ к работе со штатными средствами АС Департамента, но имеющие доступ в помещения, где они размещаются.

3 группа – субъекты, имеющие доступ к работе со штатными средствами АС Департамента.

Квалификация потенциального нарушителя.

А – не является специалистом в области вычислительной техники.

В – самый низкий уровень возможностей – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции при обработке информации.

С – возможности создания и запуска собственных программ с новыми функциями по обработке информации.

Д – возможность управления функционированием автоматизированной системы, т.е. воздействием на базовое программное обеспечение системы, на конфигурацию ее оборудования.

Е – включает весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств автоматизированной системы, вплоть до включения в состав АС собственных технических средств с новыми функциями по обработке информации.

Наряду с классификацией, приведенной выше, нарушителей информационной безопасности можно разделить на следующие виды - неосторожные (халатные), манипулируемые, саботажники, нелояльные и мотивируемые извне.

5.9. Обобщенная модель угроз безопасности информации Департамента

Угроза информационной безопасности	Источник угроз	Способы реализации угроз
I. Получение информации	1. Антропогенный	а) Разглашение, передача или утрата атрибутов разграничения доступа
		б) Внедрение агентов в число персонала системы
		в) Хищение носителей информации
		г) Незаконное получение паролей и других реквизитов разграничения доступа
		д) Несанкционированная модификация программного обеспечения
		е) Перехват данных, передаваемых по каналам связи

Угроза информационной безопасности	Источник угроз	Способы реализации угроз
		ж) Несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств
II. Анализ характеристик информации	1. Антропогенный	а) Хищение носителей информации хищение производственных отходов
		б) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств
		в) Несанкционированная модификация программного обеспечения
		г) Перехват данных, передаваемых по каналам связи, и их анализ
III. Изменение (искажение, подмена) информации	1. Антропогенный	а) Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.)
		б) Непреднамеренное заражение компьютера вирусами
		в) Ввод ошибочных данных
		г) Вмешательство в процесс функционирования АС сетей общего пользования с целью несанкционированной модификации данных
	2. Техногенный	а) аварии в системах электропитания
		б) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате неисправности систем кондиционирования
IV. Нарушение информации	1. Антропогенный	а) Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств
		б) Несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т.п.)
		в) Непреднамеренное заражение компьютера вирусами
		г) Игнорирование организационных ограничений (установленных правил) при работе в системе

Угроза информационной безопасности	Источник угроз	Способы реализации угроз
		д) Ввод ошибочных данных
	2. Техногенный	а) аварии в системах электропитания
		б) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате неисправности систем кондиционирования
V. Нарушение работоспособности систем	1. Антропогенный	а) Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств
		б) Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов автоматизированной системы
	2. Техногенный	а) закупки несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;
		б) аварии в системах электропитания;
		в) аварии в системах отопления и водоснабжения в непосредственной близости к техническим средствам обработки информации;
		г) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате неисправности систем кондиционирования;
		д) неумышленное повреждения внешних кабельных систем связи строительными организациями, физическими лицами и т.п. в результате проведения несогласованных работ в местах прокладки кабелей связи;
		е) возникновение пожаров в непосредственной близости к техническим средствам обработки информации в результате неисправной электропроводки, неисправных технических средств, нарушения сотрудниками правил противопожарной безопасности.
	3. Стихийный	а) Разрушение зданий, отдельных помещений
		б) воздействие атмосферного электричества
		в) возникновение стихийных очагов пожаров

6. ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕПАРТАМЕНТА

6.1. Организационно-штатная структура подразделений отвечающих за обеспечение информационной безопасности Департамента

Общее руководство системой информационной безопасности и принятие всех решений по вопросам ее функционирования осуществляют ответственные за защиту информации в Департаменте.

Руководство и контроль, за выполнением мероприятий по защите информации в Департаменте осуществляют руководители.

Жизненный цикл системы обеспечения информационной безопасности Департамента включает этапы постоянного функционирования и совершенствования.

7. Мероприятия для организации системы комплексного мониторинга и контроля состояния информационной безопасности

Должна быть организована система непрерывного контроля за состояние системы информационной безопасности следующим образом:

- определение перечня подразделений, рабочих мест, систем, процессов, по которым должен проводиться контроль выполнения требований.
- определение списка требований, для каждой структурной единицы.
- организация сбора отчетности о выполнении требований по ИБ.
- обработка и анализ собранных форм отчетности выводами о выполнении требований;
- периодический пересмотр системы требований
- контроль полноты и непротиворечивости системы требований.

8. Мероприятия по решению задач защиты информации от несанкционированного доступа в информационно-телекоммуникационных системах Департамента

Основные мероприятия по защите информации от несанкционированного доступа в ИТКС должны предусматривать следующее:

- Применение сертифицированных аппаратно-программных средств защиты информации от НСД.
- Механизмы защиты от НСД должны осуществлять защиту системы от возможности посторонних лиц осуществлять работу в системе (механизмы идентификации и аутентификации), а также получать НСД к информационным ресурсам системы (механизмы разграничения доступа в соответствии с полномочиями субъекта). При реализации этих механизмов защиты должна использоваться совокупность организационных, программных (пароли, матрицы доступа и др.), аппаратно-программных и технических методов защиты.
- Защита системы от НСД должна обеспечиваться на всех технологических этапах передачи, обработки и хранения информации и при всех режимах работы системы, в том числе при проведении ремонтных и регламентных работ. При этом реализованные в системе средства защиты от НСД не должны ухудшать основные функциональные характеристики системы.
- Защита системы от НСД с помощью программных, программно-аппаратных и технических методов должна обеспечивать:
    - защиту технических средств обработки информации;
    - защиту баз данных;
    - защиту системы управления.
- Защита от НСД должна строиться на основе системы разграничения доступа (СРД) пользователей к системе и ее информационным ресурсам. Основными функциями СРД должны являться:
    - реализация правил разграничения доступа (ПРД) пользователей и их процессов к информационным ресурсам;
    - реализация ПРД пользователей к устройствам создания твердых копий;
    - изоляция программ процесса, выполняемого в интересах пользователя, от других пользователей системы;

- реализация правил обмена данных между пользователями системы, построенных по сетевым принципам.

- Обеспечивающие средства СРД должны выполнять следующие основные функции:
  - идентификацию и аутентификацию пользователей системы и поддержание привязки к их процессам, выполняемым в их интересах;
  - регистрацию действий пользователей и выполняемых в их интересах процессов, предоставление возможности исключения и включения новых пользователей и объектов доступа, а также изменение полномочий пользователей;
  - реакцию на попытки несанкционированного доступа (сигнализацию, блокировку и т.д.), восстановление механизмов защиты после НСД;
  - тестирование;
  - очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищенными данными;
  - учет выходных печатных и графических форм, а также твердых копий в системе;
  - контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.
- Практическая реализация СРД должна определяться с учетом конкретных особенностей системы и может включать в себя следующие способы и их сочетания:
  - распределенная система разграничения доступа и СРД, локализованная в аппаратно-программном комплексе системы;
  - СРД в рамках операционной системы, системы управления базами данных или прикладных программ;
  - СРД в средствах реализации сетевых протоколов взаимодействия или на уровне приложений;
  - Программная и (или) техническая реализация СРД;
  - Программная и (или) аппаратная реализация криптографических функций.

В рамках системы защиты от НСД необходимо внедрить комплексную систему защиты баз данных, содержащих критичную к нарушению

безопасности информацию.

Для создания системы защиты информации от несанкционированного доступа в информационно-телекоммуникационных системах Департамента необходимо разработать следующие организационно-распорядительные и нормативно-технические документы:

- Положение о разграничении прав доступа к информационным ресурсам
- Должностные инструкции администраторов и сотрудников безопасности.

9. Мероприятия по организации криптографической защиты информации

В целях защиты конфиденциальной информации в Департаменте должны применяться средства криптографической защиты информации (СКЗИ).

К СКЗИ предъявляются следующие требования:

– СКЗИ должны допускать их встраивание в технологическую схему обработки электронных сообщений, обеспечивать взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;

– СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;

– СКЗИ должны быть реализованы на основе алгоритмов, соответствующих национальным стандартам Российской Федерации и (или) условиям договоров с контрагентами;

– СКЗИ должны иметь строгий регламент использования ключей, предполагающий контроль со стороны администратора безопасности за действиями пользователя на всех этапах работы с ключевой информацией (получение ключевого носителя, ввод ключей, использование ключей и сдача ключевого носителя);

– СКЗИ должны обеспечивать реализацию процедур сброса ключей в случаях отсутствия штатной активности пользователей в соответствии с регламентом использования ключей;

– СКЗИ не должны предъявлять требований к ЭВМ по специальной проверке на отсутствие закладных устройств, если иное не оговорено в

технической документации на конкретное средство защиты;

– СКЗИ не должны требовать дополнительной защиты от утечки по побочным каналам электромагнитного излучения.

При применении СКЗИ в АИС должны поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для всех элементов АИС.

Информационная безопасность процессов изготовления ключевой информации документов СКЗИ должна обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты.

Использование СКЗИ должно осуществляться в полном соответствии с конструкторской и эксплуатационной документацией, представляемой производителем СКЗИ. Внутренний порядок применения СКЗИ в Департаменте должен включать:

– порядок ввода в действие;

– порядок эксплуатации;

– порядок восстановления работоспособности в аварийных случаях;

– порядок внесения изменений;

– порядок снятия с эксплуатации;

– порядок управления ключевой системой;

– порядок обращения с носителями ключевой информации.

10. Положение об обработке персональных данных

1.1. Настоящее Положение об обработке персональных данных Департамента разработано в соответствии с Конституцией Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных»

1.2. Цель разработки Положения — определение порядка обработки персональных данных сотрудников Департамента; обеспечение защиты прав и свобод сотрудников Департамента при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным сотрудников Департамента, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения заместителем Губернатора Смоленской области – начальником Департамента и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом.

1.4. Все сотрудники Департамента должны быть ознакомлены с настоящим Положением под роспись.

1.5. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии Департамента, если иное не определено законом.

II. Основные понятия и состав персональных данных сотрудников

2.1. Для целей настоящего Положения используются следующие основные понятия:

– персональные данные сотрудника — любая информация, относящаяся к определенному или определяемому на основании такой информации сотруднику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая представителю нанимателя, в связи с трудовыми отношениями;

– обработка персональных данных — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных сотрудников Департамента;

– конфиденциальность персональных данных — обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным сотрудников, требование не допускать их распространения без согласия сотрудника или иного законного основания;

– распространение персональных данных — действия, направленные на передачу персональных данных сотрудников определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных сотрудников в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным сотрудников каким-либо иным способом;

– использование персональных данных — действия (операции) с персональными данными, совершаемые должностным лицом Департамента в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении сотрудников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

– блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных сотрудников, в том числе их передачи;

– уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных сотрудников или в результате которых уничтожаются материальные носители персональных данных работников;

– обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному сотруднику;

– общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия сотрудника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

– информация — сведения (сообщения, данные) независимо от формы их представления.

– документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. В состав персональных данных сотрудников Департамента входят документы, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, состоянии здоровья, а также о предыдущих местах их работы.

2.3. Комплекс документов, сопровождающий процесс оформления трудовых отношений сотрудника в Департаменте при его приеме, переводе и увольнении.

2.3.1. Информация, представляемая сотрудником, при поступлении на работу в Департамент, должна иметь документальную форму. При заключении служебного контракта, или трудового договора, сотрудник предъявляет представителю нанимателя:

– паспорт или иной документ, удостоверяющий личность;

– трудовую книжку, за исключением случаев, когда трудовой договор или служебный контракт заключается впервые, или сотрудник поступает на работу на условиях совместительства, либо трудовая книжка у сотрудника отсутствует в связи с ее утратой или по другим причинам;

– страховое свидетельство государственного пенсионного страхования;

– документы воинского учета — для военнообязанных и лиц, подлежащих воинскому учету;

– документ об образовании, о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;

– свидетельство о присвоении ИНН (при его наличии у сотрудника).

2.3.2. При оформлении сотрудника в Департамент, сотрудником отдела кадров заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные сотрудника:

– общие сведения (Ф.И.О. сотрудника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

– сведения о воинском учете;

– данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

– сведения о переводах на другую работу;

– сведения об аттестации;

– сведения о повышении квалификации;

– сведения о профессиональной переподготовке;

– сведения о наградах (поощрениях), почетных званиях;

– сведения об отпусках;

– сведения о социальных гарантиях;

– сведения о месте жительства и контактных телефонах.

2.3.3. В отделе кадров Департамента создаются и хранятся следующие группы документов, содержащие данные о сотрудниках в единичном или сводном виде:

2.3.3.1. Документы, содержащие персональные данные сотрудников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки сотрудников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации сотрудников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Департамента, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

2.3.3.2. Документация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции сотрудников, приказы, распоряжения, указания руководства Департамента); документы по планированию, учету, анализу и отчетности в части работы с персоналом Департамента.

III. Сбор, обработка и защита персональных данных

3.1. Порядок получения персональных данных.

3.1.1. Все персональные данные сотрудников Департамента следует получать у него самого. Если персональные данные сотрудника, возможно, получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо представителя нанимателя должно сообщить сотруднику Департамента о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа сотрудника дать письменное согласие на их получение.

3.1.2. Представитель нанимателя не имеет права получать и обрабатывать персональные данные сотрудника Департамента о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

Обработка указанных персональных данных сотрудников представителем нанимателя возможна только с их согласия (приложение №1), либо без их согласия в следующих случаях:

– персональные данные являются общедоступными;

– персональные данные относятся к состоянию здоровья сотрудника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия сотрудника невозможно;

– по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

IV. Передача и хранение персональных данных

4.1. При передаче персональных данных сотрудника, представитель нанимателя должен соблюдать следующие требования:

4.1.1. Не сообщать персональные данные сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом.

4.1.2. Не сообщать персональные данные сотрудника в коммерческих целях без его письменного согласия. Обработка персональных данных работников в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, допускается только с его предварительного согласия.

4.1.3. Предупредить лиц, получивших персональные данные сотрудника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные сотрудника, обязаны соблюдать режим секретности (конфиденциальности) (приложение №2). Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

4.1.4. Осуществлять передачу персональных данных сотрудников в пределах Департамента в соответствии с настоящим Положением.

4.1.5. Разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь

право получать только те персональные данные работника, которые необходимы для выполнения конкретной функции.

4.1.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции.

4.2. Хранение и использование персональных данных сотрудников:

4.2.1. Персональные данные сотрудников обрабатываются и хранятся в отделе кадров.

4.2.2. Персональные данные сотрудников могут быть получены, проходить дальнейшую обработку и передаваться на, хранение, как на бумажных носителях, так и в электронном виде.

4.3. При получении персональных данных не от сотрудника (за исключением случаев, если персональные данные были предоставлены представителю нанимателя на основании федерального закона или если персональные данные являются общедоступными) представитель нанимателя до начала обработки таких персональных данных обязан предоставить сотруднику следующую информацию:

– наименование (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.

V. Доступ к персональным данным работников

5.1. Право доступа к персональным данным сотрудников имеют:

– представитель нанимателя, заместители представителя нанимателя;

– сотрудники отдела кадров;

– сотрудники бухгалтерии;

- лица, ответственные за защиту и обработку персональных данных.

5.2. Сотрудник Департамента имеет право:

5.2.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные сотрудника.

5.2.2. Требовать от представителя нанимателя уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми, для представителя нанимателя персональных данных.

5.2.3. Получать от представителя нанимателя

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

5.2.3. Требовать извещения представителем нанимателя всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия представителя нанимателя при обработке и защите его персональных данных.

5.3. Копировать и делать выписки персональных данных сотрудника разрешается исключительно в служебных целях с письменного разрешения начальника отдела кадров.

5.4. Передача информации третьей стороне возможна только при письменном согласии работников.

VI. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

6.1. Сотрудники Департамента, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

11. Положение о хранении и уничтожении носителей персональных данных в Департаменте промышленности и торговли Смоленской области

Носителями персональных данных являются:

а) бумажные носители (документы);

б) машинные носители:

-накопители на жестких магнитных дисках (НЖМД), установленные в системных блоках автоматизированных рабочих мест обработки персональных данных;

-съемные носители (дискеты, CD-DVD диски, USB-носители, съемные НЖМД).

Носители уничтожаются в случаях:

- истек срок хранения носителя;
- носитель пришел в негодность.

Для уничтожения носителей приказом руководителя назначается комиссия.

Бумажные носители персональных данных, CD-DVD диски и дискеты уничтожаются путем сожжения или измельчения шредером (уничтожителем бумаги).

НЖМД и USB-носители уничтожаются при помощи специальных устройств или физического повреждения, исключающего возможность восстановления носителя.

В том случае, если необходимо уничтожить персональные данные на машинном носителе и сохранить носитель для последующего использования необходимо произвести 3 цикла полного форматирования носителя.