

**МИНОБРНАУКИ РОССИИ**  
**федеральное государственное бюджетное**  
**образовательное учреждение высшего образования**  
**«Череповецкий государственный университет»**

УТВЕРЖДЕНО  
приказом ректора  
№ 05-02-41 от 21.06.2021

**Система менеджмента качества**  
**ПОЛОЖЕНИЕ О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ РАБОТ ПО ЗАЩИТЕ**  
**КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ**

---

наименование документа

**Используемые сокращения:**

|       |   |
|-------|---|
| АРМ   | Автоматизированное рабочее место                          |
| АС    | Автоматизированная система                                |
| БД    | Базы данных   |
| ГИС   | Государственная информационная система                    |
| ЗИ    | Защита информации   |
| ИСПДн | Информационная система персональных данных                |
| КС    | Корпоративная сеть  |
| КЗ    | Класс защищенности  |
| ЛВС   | Локальная вычислительная сеть                             |
| МЭ    | Межсетевой экран  |
| НСД   | Несанкционированный доступ                                |
| ОС    | Операционная система                                      |
| ПО    | Программное обеспечение                                   |
| ПЭМИН | Побочные электромагнитные излучения и наводки             |
| РД    | Руководящий документ                                      |
| РИС   | Региональная информационная система                       |
| СВТ   | Средства вычислительной техники                           |
| СЗИ   | Система защиты информации                                 |
| СКЗИ  | Средства криптографической защиты информации              |
| СКУД  | Система контроля управления доступом                      |
| ФСТЭК | Федеральная служба по техническому и экспортному контролю |
| ЧС    | Чрезвычайная ситуация                                     |
| ЭВМ   | Электронная вычислительная машина                         |
| ЭК    | Экспертная комиссия                                       |

**Термины и определения**

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

**Автоматизированное рабочее место** - программно-технический комплекс, предназначенный для автоматизации определенного вида деятельности.

**Аттестация автоматизированной системы** - процесс комплексной проверки выполнения заданных функций автоматизированной системы по обработке защищаемой информации на

|  |                  |
|--|------------------|
| <b>Система менеджмента качества</b><br><b>ПОЛОЖЕНИЕ О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ РАБОТ ПО ЗАЩИТЕ</b><br><b>КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ</b> | Страница 2 из 25 |
|--|------------------|

соответствие требованиям стандартов и/или нормативных документов в области защиты информации и оформления документов о ее соответствии требованиям безопасности информации.

**Аутентификация** - проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение его подлинности.

**Безопасность информации** - состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних и внешних угроз.

**Государственная информационная система** - федеральная информационная система и региональная информационная система, созданная на основании соответственно федерального закона, закона субъекта Российской Федерации, на основании правовых актов государственных органов.

**Доступность информации** - состояние информации, характеризующееся способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

**Защита информации** - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

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

**Информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Информационная система персональных данных** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

**Класс защищенности автоматизированной системы** - определенная совокупность требований по защите автоматизированной системы от несанкционированного доступа к информации.

**Коммерческая тайна** - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

**Конфиденциальная информация** - информация с ограниченным доступом, не содержащая сведений составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации или обладателем информации.

**Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

**Несанкционированный доступ** - Получение защищаемой информации заинтересованным субъектом с нарушением установленных нормативными правовыми документами или обладателем информации прав или правил доступа к защищаемой информации.

**Обработка информации** - совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией.

|  |                  |
|--|------------------|
| <b>Система менеджмента качества</b><br><b>ПОЛОЖЕНИЕ О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ РАБОТ ПО ЗАЩИТЕ</b><br><b>КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ</b> | Страница 3 из 25 |
|--|------------------|

**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 информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

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

**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 и другая информация.

**Система защиты информации в автоматизированной** - системе совокупность технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации

**Система обеспечения безопасности информации** - совокупность органов и (или) исполнителей, используемых ими средств защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

**Средство защиты информации** - техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

**Техническая защита конфиденциальной информации** - комплекс мероприятий и (или) услуг по ее защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

**Целостность информации** - состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

## **1 ОБЩИЕ ПОЛОЖЕНИЯ**

Настоящий документ «Положение о порядке организации и проведения работ по защите конфиденциальной информации» (далее по тексту - Положение) определяет цели, задачи и основные мероприятия по обеспечению безопасности информации в федеральном государственном бюджетном образовательном учреждении высшего образования «Череповецкий государственный университет» (далее по тексту - Учреждение).

Согласно Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», в Положении под конфиденциальной понимается следующая информация (далее конфиденциальная информация - КИ):

- персональные данные граждан;
- служебная тайна;
- коммерческая тайна;
- иные сведения конфиденциального характера.

Положение разработано применительно к информации, подлежащей защите, средствам ее обработки, хранения и передачи, а также к информационным ресурсам общего пользования, неправомерное использование которых может представлять собой угрозы безопасности информации Учреждения.

Положение разработано в соответствии с действующим законодательством РФ в области безопасности информации, а также ГОСТ и руководящими документами (РД) ФСТЭК (Гостехкомиссии) России, перечень которых приведен в Разделе 9.

Положение является основой для разработки локальных нормативных актов Учреждения по обеспечению безопасности информации.

Положение распространяется на всех сотрудников Учреждения, включая сотрудников, работающих по договору подряда, а также на сотрудников сторонних организаций, взаимодействующих с Учреждением на основании соответствующих нормативных, правовых и организационно-распорядительных документов.

Положение применимо ко всем средствам вычислительной техники и автоматизированным системам (АС) Учреждения, в том числе серверам, активному сетевому оборудованию, автоматизированным рабочим местам (АРМ) локальных вычислительных сетей (ЛВС) в составе корпоративной сети (КС) Учреждения, а также персональным компьютерам в пределах среды автоматизированной системы (АС) Учреждения.

## **2 ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

Под безопасностью информации понимается состояние защищенности информационной среды Учреждения, обеспечивающее удовлетворение информационных потребностей пользователей информации (т.е. предоставление им полной, достоверной и своевременной информации) и обеспечение безопасности такой информации.

Обеспечение безопасности информации Учреждения осуществляется путем реализации деятельности по защите информации, т.е. деятельности по предотвращению утечки и утраты информации. При этом в понятие утрата входит хищение, потеря информации, а также блокирование (временная утрата) и искажение (частичная утрата), а в понятие утечка информации - неправомерный выход информации за пределы защищаемой зоны ее функционирования или установленного круга лиц, результатом которого является получение информации лицами, не имеющими к ней санкционированного доступа. Утечка и утрата информации могут происходить в результате несанкционированного доступа (НСД) к информации, несанкционированных и непреднамеренных воздействий на нее или средства ее

|  |                  |
|--|------------------|
| <b>Система менеджмента качества</b><br><b>ПОЛОЖЕНИЕ О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ РАБОТ ПО ЗАЩИТЕ</b><br><b>КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ</b> | Страница 5 из 25 |
|--|------------------|

обработки и передачи.

Таким образом, целью реализации различных мер и мероприятий по защите информации является, в конечном итоге, обеспечение безопасности информации Учреждения, а это, в свою очередь, позволяет защитить интересы Учреждения в экономической сфере, обеспечить ему более выгодное положение на конкурентном рынке.

Задачами, которые необходимо решить для достижения поставленной цели являются:

- своевременное выявление потенциальных угроз защищаемой информации и средствам ее обработки и передачи;
- выявление причин, обстоятельств и условий, способствующих реализации выявленных угроз и выработка мероприятий по их нейтрализации;
- предотвращение НСД к информации и средствам ее обработки и передачи;
- предотвращение непреднамеренных воздействий на информацию и средства ее обработки и передачи;
- предотвращение утечки информации по техническим каналам;
- контроль эффективности защитных мер и мероприятий.

### **3 ЗАЩИЩАЕМЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ**

К защищаемым информационным ресурсам Учреждения относятся:

- информация, зафиксированная на различных носителях;
- средства обработки, хранения, передачи информации и средства связи, в том числе программное обеспечение указанных средств (при его наличии).

#### **3.1 Информация, подлежащая защите**

Защите подлежит информация, касающаяся различных направлений деятельности, неправомерное обращение с которой может нанести ущерб интересам Учреждения или иному физическому или юридическому лицу, доверившему свою информацию Учреждению.

В рамках деятельности Учреждения ведется обработка следующих категорий информации:

- конфиденциальная информация (информация, составляющая служебную тайну, коммерческую тайну и персональные данные и иные сведения конфиденциального характера (см. абз.2 раздел 1);
- открытая информация (подлежит защите от ее утраты).

Конкретный состав информации, относимой к каждой из названных категорий, определяется в установленном действующим законодательством порядке и закрепляется в соответствующих документах: в части касающейся конфиденциальной информации - в положении о коммерческой тайне и конфиденциальности информации в Череповецком государственном университете. Указанный перечень разрабатывается в соответствии с действующим законодательством, в том числе, в части определения сведений, которые не могут быть отнесены к категории конфиденциальной информации. Защищаемые информационные ресурсы могут быть представлены в виде отдельных документов (массивов документов) на бумажных носителях, а также в виде документов (файлов) и массивов документов в ЛВС и/или на машинных носителях информации.

### **3.2 Средства обработки информации**

Состав средств обработки, хранения и передачи информации, а также средств связи, используемых для обработки конфиденциальной информации, закрепляется в «Техническом паспорте».

Средства вычислительной техники, используемые для обработки информации в Учреждении, объединены в ЛВС.

На физическом уровне ЛВС Учреждения представляет собой совокупность нескольких сегментов. ЛВС включает в себя сетевые и файловые серверы, серверы баз данных (БД) и подключенные к ним через коммутаторы рабочие станции (АРМ пользователей), осуществляющие с серверами обмен информацией по стеку протоколов ТСР/ІР.

Программное обеспечение представлено серверными операционными системами (ОС), а также клиентскими ОС для рабочих станций. Стандартный пакет ПО, устанавливаемый на рабочих станциях, включает также пакет офисных приложений, программы для архивирования (сжатия) файлов, программы оболочки и антивирусное ПО. Иное программное обеспечение, необходимое сотрудникам для выполнения своих функциональных обязанностей, устанавливается на АРМ после подачи соответствующей заявки в Управление информационных технологий Учреждения.

Подключение к сети Интернет на АРМ Учреждения обрабатывающих ПДн осуществляется через проху-сервер. В качестве средств защиты и связи между территориальными площадками используется оборудование межсетевого экранирования.

## **4 УГРОЗЫ ЗАЩИЩАЕМЫМ ИНФОРМАЦИОННЫМ РЕСУРСАМ**

Дестабилизирующее воздействие на информацию и/или средства ее обработки, хранения и передачи может привести к реализации следующих групп угроз.

### **Угрозы целостности:**

- несанкционированное уничтожение информации;
- несанкционированная модификация информации;
- фальсификация (подделка) информации и/или ее носителя.

### **Угрозы доступности:**

- блокирование информации;
- атаки типа «отказ в обслуживании».

### **Угрозы конфиденциальности:**

- НСД к информации;
- разглашение информации;
- утечки по техническим каналам;
- хищение информации и/или ее носителя;
- потеря носителя информации.

Данные виды угроз могут реализовываться различными способами, в зависимости от источника угроз, его возможностей, целей, причин и условий оказания дестабилизирующего воздействия.

К источникам угроз относятся:

- человек;
- технические средства обработки, хранения и передачи информации;
- системы обеспечения жизнедеятельности (водоснабжение, электроснабжение, отопление);
- природные явления и стихийные бедствия.

Различные источники угроз могут оказывать как непосредственное воздействие, так и опосредованное, через другие источники, в том числе различные группы людей (как источники угроз) могут действовать совместно и/или согласованно.

#### **4.1 Угрозы со стороны человека**

##### **4.1.1 Модель нарушителя**

Для людей, как источника угроз, необходимо построение модели вероятного нарушителя, которая бы описывала цели, устремления и возможности различных групп злоумышленников, могущих оказывать негативное воздействие на защищаемую информацию.

Классы нарушителей выделяются исходя из:

- отношения нарушителя к системе - внутренний или внешний;
- оснащенности нарушителя - высокооснащенный, среднего уровня оснащенности или неподготовленный;
- характера воздействия - преднамеренное или непреднамеренное, непосредственное или опосредованное;
- периодичности воздействия - постоянное воздействие, эпизодическое или случайное.

В соответствии с этим выделяется 2 класса потенциальных нарушителей - «Внутренние» и «Внешние».

##### **Внутренние нарушители**

К данной категории относятся лица (в зависимости от уровня доступа):

- работники Учреждения, в том числе, администраторы и пользователи ЛВС Учреждения;
- лица, получившие санкционированный доступ к определенной части защищаемых информационных ресурсов в силу служебной и деловой необходимости (контрагенты, представители органов власти, правоохранительных органов и т.п.);
- технический и обслуживающий персонал;
- лица, имеющие право физического доступа в помещения Учреждения.

Такие нарушители могут оказывать как преднамеренное (постоянное или эпизодическое) воздействие, так и (в большей степени) непреднамеренное (случайное) воздействие.

Внутренние нарушители имеют следующую квалификацию:

- являются высококвалифицированными специалистами в области эксплуатации (а в некоторых случаях и разработки) программного обеспечения (ПО) и технических средств обработки информации;
- знают специфику задач, решаемых Учреждением;
- знают специфику построения системы защиты информации, особенности применяемых в целях обеспечения безопасности информации средств, методов и мероприятий

по защите информации.

#### **Внешние нарушители**

К ним относятся лица, не получающие в установленном порядке права доступа к защищаемым информационным ресурсам Учреждения.

Такие нарушители могут оказывать как преднамеренное, так и непреднамеренное воздействие, обладать различным уровнем квалификации и периодичность такого воздействия может быть различной, в зависимости от целей и устремления нарушителей.

При создании эффективной системы защиты информации учитывается, что внешние нарушители:

- знают специфику задач, решаемых Учреждением;
- знают функциональные особенности работы Учреждения и закономерности хранения, обработки и передачи информации;
- знают сетевое оборудование, а также протоколы передачи данных, используемые в корпоративной сети Учреждения;
- знают особенности системного и прикладного ПО, а также технических средств, используемых при работе с защищаемой информацией в ЛВС Учреждения;
- являются высококвалифицированными специалистами в области использования технических средств перехвата и НСД к информации;
- могут использовать специальное оборудование, предназначенное для съема информации с кабельных линий связи и по радиоканалам.

#### **4.1.2 Возможности нарушителей**

Основными видами воздействия нарушителей на защищаемую информацию Учреждения являются:

##### **Со стороны внутренних нарушителей:**

- разглашение информации, к которой имеется правомерный доступ;
- хищение (кража) носителей защищаемой информации и/или технических средств ее обработки;
- уничтожение носителя или информации на нем, фальсификация носителей информации, размагничивание магнитных носителей информации и т.п.;
- модификация ПО, установка программных закладок, заражение ЭВМ компьютерными вирусами;
- невыполнение установленных правил работы с информацией и средствами ее обработки, внесение несанкционированных изменений в процедуры обработки информации, в порядок подготовки документов, неправильная настройка оборудования, считывание данных из файлов других пользователей и т.п.;
- блокирование работы ЛВС Учреждения и/или ее сегментов.

##### **Со стороны внешних нарушителей:**

- изучение системы защиты информации, методов и механизмов обеспечения информационной безопасности с целью выявления уязвимостей;
- получение НСД к информации и средствам ее обработки, как физического (непосредственное проникновение), так и логического, с использованием штатных технических средств обработки и передачи информации;
- применение средств несанкционированного съема (перехвата) защищаемой информации (в том числе подслушивание, визуальное наблюдение);
- получение НСД к информации через лиц, имеющих санкционированный доступ к защищаемой информации;
- сбор сведений о структуре, топологии ЛВС Учреждения, составе, функциях программно-аппаратных средств обработки информации и выявление их уязвимостей;
- модификация программного обеспечения путем добавления новых функций или



использование программно-аппаратных средств, реализующих недеklarированные возможности;

- использование учетных записей зарегистрированных пользователей с целью получения доступа к информационным ресурсам или дискредитации зарегистрированных пользователей;

- подключение к каналам связи с целью перехвата, анализа, модификации или уничтожения информации, а также с целью блокирования данных каналов связи.

#### **4.2 Угрозы со стороны технических средств обработки, хранения и передачи информации**

Угрозы со стороны технических средств имеют отношение к информации, обрабатываемой, хранимой и передаваемой с помощью данных технических средств. Вывод из строя технических средств обработки информации и нарушение режима их работы со стороны нарушителей относится к видам воздействия со стороны человека, как источника угрозы. В данном контексте рассматриваются случайно возникшие аварийные ситуации.

К таким угрозам относятся:

- выход из строя технических средств обработки информации;
- сбои в работе технических средств обработки информации;
- возникновение ПЭМИН, сопровождающих функционирование технических средств.

#### **4.3 Угрозы со стороны систем обеспечения жизнедеятельности Учреждения**

К системам обеспечения жизнедеятельности относятся системы водоснабжения, энергоснабжения, отопления, вентиляции и кондиционирования.

Угрозы со стороны таких систем опосредовано могут привести к оказанию дестабилизирующего воздействия на защищаемые информационные ресурсы.

К таким угрозам относятся:

- выход из строя системы обеспечения жизнедеятельности Учреждения;
- сбои в работе систем обеспечения жизнедеятельности Учреждения.

#### **4.4 Угрозы со стороны природных явлений**

К данному источнику относятся природные факторы и стихийные бедствия различного происхождения. Угрозы со стороны данного источника носят различный характер и приводят к широкому спектру дестабилизирующих воздействий на защищаемые информационные ресурсы. В основе дестабилизирующего воздействия, в этом случае, лежат объективные причины, неподконтрольные человеку, поэтому здесь, в первую очередь, имеет значение ликвидация последствий и снижение ущерба от реализации подобных угроз. Реализация угроз со стороны данных источников возникает в условиях возникновения чрезвычайных ситуаций (ЧС). Действия персонала Учреждения в условиях ЧС должны быть описаны в соответствующем документе («Положение по действиям при угрозе или возникновении чрезвычайных ситуаций»).

## **5 МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

Всю совокупность мер по обеспечению безопасности информации, наличие которых необходимо для построения системы защиты информации (СЗИ) Учреждения, условно можно разделить на:

- законодательные (правовые);
- организационные (административные);
- технические (программные и аппаратные);
- физические.

### **5.1 Законодательные (правовые) меры**

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с конфиденциальной информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию конфиденциальной информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

### **5.2 Организационные и административные меры**

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности конфиденциальной информации или снизить размер потерь в случае их реализации.

Главная цель организационных мер, предпринимаемых на высшем управленческом уровне - сформировать политику информационной безопасности Учреждения (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация политики информационной безопасности КИ в ИСПДн состоит из мер административного уровня и организационных мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Примером таких решений могут быть:

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности КИ, определение ответственных за ее реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области безопасности КИ;
- принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне Учреждения в целом;
- обеспечение нормативной (правовой) базы по безопасности и т.п.

Политика административного уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности КИ, определить какими ресурсами

(материальные, персонал) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и стоимостью проводимых мероприятий по защите КИ в ИСПДн.

На уровне процедурных мер защиты определяются процедуры и правила достижения целей и решения задач политики информационной безопасности КИ. Эти правила определяют:

- какова область применения политики безопасности КИ;
- каковы роли и обязанности должностных лиц, отвечающих за проведение политики безопасности КИ, а также их ответственность;
- кто имеет права доступа к КИ;
- какими мерами и средствами обеспечивается защита КИ;
- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- определять коалиционные и иерархические принципы и методы разграничения доступа к КИ;
- определять порядок работы с программно-математическими и техническими (аппаратными) средствами защиты и криптозащиты.

#### **5.2.1 Регламентация состава и содержания защищаемой информации**

Состав информации, относимой к конфиденциальной, а также порядок такого отнесения определяется «Перечнем сведений конфиденциального характера» (далее Перечень).

Любая иная информация, не указанная в данном Перечне, не должна относиться к категории конфиденциальной.

Если выявляется необходимость отнесения к конфиденциальным сведений, не подходящих ни под одну категорию из названного Перечня, то вносятся предложения по его пересмотру. Пересмотр перечня осуществляется в порядке, установленном для его утверждения.

#### **5.2.2 Определение полномочий доступа сотрудников к защищаемым информационным ресурсам и их реализация**

Порядок доступа сотрудников к защищаемым информационным ресурсам университета определяется в соответствии с действующим положением о разрешительной система доступа работников к защищаемым информационным ресурсам информационной системы персональных данных.

Защищаемые информационные ресурсы, доступ пользователей к которым ограничен, определяются в документе «Перечень защищаемых информационных ресурсов информационной системы персональных данных».

Каждый сотрудник Учреждения должен иметь права доступа только к той части конфиденциальной информации, которая действительно необходима ему для выполнения своих трудовых обязанностей.

Необоснованное служебной необходимостью ознакомление сотрудников с конфиденциальной информацией Учреждения не допускается.

#### **5.2.3 Технология обработки конфиденциальных документов**

Технология обработки конфиденциальных документов включает в себя определение правил учета, хранения и выдачи носителей конфиденциальной информации (в том числе съемных машинных носителей) и правил работы сотрудников с защищаемой информацией.

При разработке конфиденциальных документов гриф должен определять сам разработчик. Гриф проставляется в правом верхнем углу с указанием количества экземпляров

документа.

Полученные извне документы грифуются на основе «Перечня сведений конфиденциального характера». Грифованные документы должны храниться в сейфах или шкафах, обеспечивающих отсутствие возможности несанкционированного к ним доступа посторонних лиц. Учет, хранение и выдача документов осуществляется специально назначаемым сотрудником.

Для уничтожения таких документов приказом по Учреждению назначается комиссия по их уничтожению, которая составляет и подписывает Акт уничтожения конфиденциальных документов.

Запрещается работа с конфиденциальными документами вне помещений Учреждения (кроме случаев служебных командировок).

#### **5.2.4 Организационное сопровождение функционирования технических и программно-аппаратных средств обработки и защиты информации**

Порядок работы с техническими и программно-аппаратными средствами защиты информации определяется соответствующими руководителями для всех категорий пользователей, которые должны быть ознакомлены с содержанием данных документов и строго выполнять содержащиеся в них требования.

АРМ сотрудников Учреждения должны быть оборудованы необходимыми программными или программно-аппаратными средствами защиты информации - система парольной защиты, средства защиты информации от НСД, антивирусы, криптографические средства (при необходимости), и т.п.

Сотрудники обязаны использовать технические и программно-аппаратные средства защиты информации, установленные на их рабочих местах и/или использующиеся совместно со средствами обработки, передачи информации и средствами связи.

Не допускается обработка КИ на ЭВМ, включая портативные персональные компьютеры, без установленных программных или программно-аппаратных средств защиты информации.

Не допускается передача КИ по открытым каналам связи без использования специальных технических средств защиты информации.

Не допускается использование незащищенных личных средств мобильной связи для обсуждения вопросов, содержащих сведения конфиденциального характера.

В Учреждении должно проводиться обучение сотрудников правилам работы с используемыми техническими и программно-аппаратными средствами защиты информации.

Все, используемые в Учреждении технические и программно-аппаратные средства защиты информации должны быть сертифицированы в установленном порядке.

#### **5.2.5 Организация технического обслуживания оборудования, используемого для обработки защищаемой информации**

Оборудование, предназначенное для обработки защищаемой информации Учреждения, должно эксплуатироваться в условиях (температура, влажность, электромагнитный режим) в соответствии с инструкциями производителя и/или соответствующих нормативных документов. Техническое обслуживание оборудования должно обеспечивать его постоянную работоспособность.

Сотрудниками, ответственными за поддержание оборудования в работоспособном состоянии, ведется Журнал технического обслуживания и учета неисправностей оборудования, в котором отмечаются все работы по техническому обслуживанию и регистрируются неполадки, возникающие в процессе работы.

Проводить ремонт и техническое обслуживание оборудования могут только организации, обладающие в соответствии с действующим законодательством правом на осуществление указанного вида деятельности, привлекаемые Учреждением для оказания данных услуг на основании договора.

### **5.2.6 Организация пропускного и внутри объектового режима в Учреждении**

Доступ сотрудников на территорию Учреждения и во внутренние рабочие помещения, где обрабатывается КИ, осуществляется с использованием журнала учета посещений, с обязательной регистрацией входа и выхода.

Для каждого помещения должен быть составлен список сотрудников, имеющих право доступа в данное помещение. Список должен своевременно корректироваться по мере увольнения сотрудников Учреждения, приема на работу новых сотрудников или перевода сотрудника на другую работу. Сотрудники, не указанные в данном списке, не имеют права находиться в помещении без сопровождения сотрудника, имеющего право такого доступа, кроме случаев экстренной необходимости при чрезвычайных обстоятельствах. В данном случае с разрешения администрации Учреждения помещение снимается с охраны и производится доступ в данное помещение в присутствии лица, ответственного за него, или представителя администрации Учреждения.

Доступ посетителей на территорию Учреждения осуществляется по предварительной договоренности с конкретным сотрудником Учреждения, который сообщает в пропускной пункт, необходимые для временного пропуска - ФИО посетителя, день, цель и место визита.

Временный пропуск посетителя возможен при предъявлении им в пропускном пункте одного из трех типов установленных документов, а именно Паспорта, Водительского удостоверения или Военного билета.

Все посетители регистрируются в пропускном пункте в журнале учета посещений с записью паспортных или иных данных в соответствии с предъявляемым типом документа. Посетители, пришедшие без предварительной договоренности (курьеры и др.), не имеют права доступа во внутренние помещения Учреждения.

Доступ приглашенного технического и обслуживающего персонала осуществляется в соответствии с необходимыми письменными распоряжениями администрации Учреждения. Доступ технического и обслуживающего персонала в защищаемые помещения без сопровождения сотрудника Учреждения не допускается.

На посту охраны при входе в здание должен находиться список сотрудников, имеющих доступ в помещения Учреждения, в соответствии с которым осуществляется проход сотрудников в здание по предъявлении паспорта при отсутствии у них пропуска. Список должен своевременно корректироваться по мере увольнения сотрудников Учреждения или приема на работу новых сотрудников.

### **5.2.7 Разработка организационно-распорядительной и нормативной документации**

В Учреждении должны быть разработаны и введены в действие все организационно-распорядительные и иные нормативные документы, на которые имеются ссылки в данном Положении. Одним из основных документов является «Перечень сведений конфиденциального характера».

В ходе подготовки Перечня должностные лица Учреждения должны провести анализ всех сторон его деятельности с целью определения конкретных сведений, разглашение которых может нанести ущерб.

Сведения, составляющие конфиденциальную информацию о деятельности Учреждения, должны разделяться на сведения, составляющие персональные данные, коммерческую тайну, служебную тайну и иные сведения конфиденциального характера.

Для работы по составлению Перечня должен привлекаться широкий круг экспертов и должностных лиц отделов, служб Учреждения с тем, чтобы ни одно из возможных направлений деятельности не было упущено при его разработке.

Перечень вводится в действие приказом ректора Учреждения.

### **5.2.8 Контроль соблюдения требований по обеспечению безопасности информации**

Контроль соблюдения требований по обеспечению безопасности информации в Учреждении возлагается на администрацию Учреждения и специально назначенные проверочные комиссии.

В Учреждении должна быть введена должность администратора информационной безопасности, который осуществляет организацию деятельности по защите конфиденциальной информации Учреждения, установку, настройку и администрирование программных и программно-аппаратных средств защиты информации в КС, контроль за выполнением требований по обеспечению безопасности информации.

Допускается совмещение выполнения указанных функций с другими обязанностями. При этом совмещение в одном лице функций системного администратора и администратора информационной безопасности **не допускается**.

Каждый сотрудник несет персональную ответственность за соблюдение правил настоящего Положения и иных нормативных документов по вопросам обеспечения безопасности информации.

## **5.3 Технические (программные и аппаратные) меры**

Данные меры предполагают обеспечение защиты конфиденциальной информации от утечки по техническим каналам, а также от НСД.

### **5.3.1 Общие меры по защите КИ от НСД**

Установка и настройка программно-аппаратных средств защиты информации в ЛВС осуществляется только администратором информационной безопасности.

Установка и настройка программных и программно-аппаратных средств обработки информации в ЛВС осуществляется лицом, выполняющим функции системного администратора (далее системный администратор).

Все действия системного администратора по настройке программных и программно-аппаратных средств обработки информации в ЛВС не должны нарушать состояние защищенности обрабатываемой информации. Контроль соблюдения требований безопасности при работах в ЛВС должен осуществляться администратором информационной безопасности.

Доступ к конфигурации программно-аппаратных средств защиты информации для иных пользователей, кроме администратора информационной безопасности, должен быть заблокирован.

На АРМ пользователей должно быть установлено прикладное программное обеспечение (ПО), только действительно необходимое пользователю для выполнения им своих трудовых обязанностей. Неиспользуемое пользователем ПО АРМ должно быть отключено или удалено.

Должна быть обеспечена синхронизация времени между АРМ и сервером.

Должно проводиться своевременное обновление ПО АРМ.

Установку нового ПО на АРМ и обновление ПО должен осуществлять только системный администратор или сотрудники службы, осуществляющие обслуживание и техническое сопровождение СВТ Учреждения.

АРМ должно эксплуатироваться тем сотрудником, за которым оно закреплено. Этот сотрудник несет персональную ответственность за работу своего АРМ и выполнение требований данного Положения по безопасности для своего АРМ.

Доступ к установке и конфигурированию серверного ПО имеют только системный администратор и администратор безопасности.

Из операционной системы и ПО сервера удаляются (отключаются) все неиспользуемые сервисы и протоколы, регулярно устанавливаются пакеты обновлений для

создания более безопасной конфигурации операционной системы (ОС).

Для анализа работы ЛВС должны использоваться системы обнаружения вторжений (атак) и средства анализа и контроля трафика.

Должно быть обеспечено в обязательном порядке наличие источников бесперебойного питания для сетевого и серверного оборудования Учреждения и, желательно, для АРМ пользователей.

Съемные машинные носители конфиденциальной информации должны быть учтены в подразделении, выполняющем функции службы конфиденциального делопроизводства, в установленном порядке.

### **5.3.2 Контроль доступа пользователей к АРМ и ресурсам ЛВС**

В ЛВС Учреждения должны обеспечиваться: идентификация, аутентификация, авторизация; управление доступом; контроль целостности; регистрация, включая:

- функционирование системы парольной защиты АРМ и ЛВС;
- контроль доступа пользователей к ресурсам АРМ и/или ЛВС. Оперативный контроль доступа пользователей осуществляется администратором информационной безопасности;
- непротиворечивая и прозрачная административно-техническая поддержка задач управления доступом к ресурсам АРМ и/или ЛВС. Назначение/лишение полномочий по доступу сотрудников к ресурсам АРМ и/или ЛВС санкционируется руководителем структурного подразделения Учреждения, несущего персональную ответственность за обеспечение безопасности информации в данном подразделении.

Системный администратор не должен иметь служебных полномочий (а при возможности и технических средств) по настройке параметров системы, влияющих на полномочия пользователей по доступу к информации. Однако, он должен иметь право добавить в систему нового пользователя без всяких полномочий по доступу к информации, а также удалить из системы такого пользователя.

Администратор информационной безопасности должен иметь служебные полномочия и технические возможности по контролю действий соответствующих системных администраторов (без вмешательства в их действия) и пользователей, а также полномочия (а при возможности и технические средства) по настройке для каждого пользователя параметров системы, которые определяют права доступа к информации.

Администратор информационной безопасности не должен иметь права добавить нового пользователя в домен, а также удалить из него существующего пользователя.

В случае отсутствия у администратора информационной безопасности технических возможностей по настройке параметров ЛВС, влияющих на полномочия пользователей по доступу к информации, эти настройки выполняются системным администратором, но с обязательным предварительным согласованием устанавливаемых прав доступа пользователей к информации с администратором информационной безопасности.

Права доступа пользователей к ресурсам ЛВС назначаются администратором информационной безопасности в соответствии с положением о разрешительной системе доступа работников к защищаемым информационным ресурсам информационной системы персональных данных.

Для каждого пользователя заводится отдельная учетная запись, которая должна содержать фамилию и инициалы пользователя.

Учетные записи должны быть распределены по группам, к которым относятся пользователи.

Учетные записи пользователей делятся на 2 категории: администраторы и пользователи.

#### **Администраторы:**

- учетная запись используется сотрудниками службы, осуществляющей поддержку функционирования оборудования ЛВС и средств ее защиты;
- администраторы имеют доступ ко всем штатным средствам настройки программно-аппаратного комплекса ЛВС.

**Пользователи:**

- учетная запись используется для всех сотрудников, АРМ которых подключены к ЛВС Учреждения;
- пользователи имеют доступ на сервере к папке своей службы, общим папкам и при необходимости, к иным ресурсам в соответствии с назначенными администратором информационной безопасности правами;
- пользователи имеют право на использование ПО, установленного на АРМ;
- пользователи не имеют права установки дополнительного ПО без согласования с администратором информационной безопасности и системным администратором.

Учетные записи сотрудников, которые прекратили работу в Учреждении, должны блокироваться. Удаление таких учетных записей должно осуществляться не ранее, чем через 6 месяцев.

Доступ пользователей к АРМ и ЛВС осуществляется с использованием средств парольной защиты.

Пароль пользователя назначается администратором информационной безопасности при создании учетной записи пользователя и в дальнейшем может изменяться только им с соблюдением следующих условий:

- должен состоять не менее, чем из 6 символов;
- должен содержать хотя бы по одной строчной, прописной букве и цифре;
- должен быть известен только владельцу и администратору информационной безопасности;
- не должен использоваться для доступа к другим информационным системам и сервисам вне Учреждения;
- не должен содержать устойчивых выражений, словосочетаний, аббревиатур и т.п.;
- не должен содержать любых персональных данных;
- не должен содержать повторений или простых последовательностей букв и цифр.

В целях обеспечения доступа к системе в случае, когда пользователь забыл пароль, список паролей хранится у администратора информационной безопасности.

Смена пароля должна проводиться периодически, как установлено в Учреждении, или при его компрометации.

Должна быть предусмотрена возможность ручной блокировки экрана на случай оставления пользователем рабочего места.

Снятие блокировки осуществляется вводом пароля пользователя.

Контроль доступа (как локального, так и удаленного) к АРМ администратора информационной безопасности и системного администратора должен дополнительно обеспечиваться с помощью средств аутентификации.

### **5.3.3 Мониторинг системы защиты информации**

Мониторинг СЗИ должен проводиться администратором информационной безопасности с целью обнаружения и регистрации отклонений защитных мер от требований обеспечения безопасности информации и оценки полноты реализации требований данного



Положения.

Основной целью мониторинга СЗИ является оперативное и постоянное наблюдение, сбор, анализ и обработка данных, необходимых для решения следующих задач:

- контроль за реализацией положений нормативных актов по обеспечению безопасности информации на Учреждения;
- выявление нештатных (или злоумышленных) действий в ЛВС Учреждения;
- выявление потенциальных нарушений безопасности информации.

Для целей оперативного и постоянного наблюдения объектов мониторинга могут использоваться как специализированные (например, программные) средства, так и штатные (входящие в коммерческие продукты и системы) средства регистрации действий пользователей, процессов и т.п.

В СЗИ должен вестись журнал регистрации действий пользователей. Журнал ведется в электронной форме, при необходимости, с использованием штатных средств ОС.

Должна осуществляться регистрация попыток входа пользователей в систему.

Регистрируются следующие параметры:

- дата и время попытки;
- результат попытки входа (успешная, неуспешная);
- идентификатор пользователя, предъявленный при попытке;
- пароль, предъявленный при неуспешной попытке;

Должна осуществляться регистрация попыток доступа к защищаемым файлам данных.

Регистрируются следующие параметры:

- дата и время попытки доступа;
- результат попытки (успешная, неуспешная);
- идентификатор пользователя - субъекта доступа;

Действия пользователей с полномочиями администраторов также должны подвергаться регистрации. Следующие действия администраторов должны протоколироваться:

- создание, модификация, удаление объектов;
- модификация прав доступа и привилегий пользователей;
- модификация правил доступа к информационным ресурсам;
- запуск (остановка) сетевых сервисов;
- изменение параметров аудита.

События, дополнительно подлежащие регистрации, устанавливаются отдельно для различных пользователей, групп пользователей, информационных ресурсов.

Журнал регистрации должен быть защищен от несанкционированного доступа и изменений.

Должно осуществляться резервное копирование данных журнала регистрации.

Должно быть настроено оперативное оповещение администратора информационной безопасности при регистрации критических событий нарушения безопасности.

Администратор безопасности должен регулярно просматривать и анализировать данные журнала регистрации.

#### **5.3.4 Антивирусная защита**

На серверах и каждом АРМ должны использоваться официально приобретенные (лицензионные) средства антивирусной защиты.

Обязателен автоматический запуск антивирусного средства при загрузке ОС и обязательное автоматическое обновление антивирусных баз не реже, чем раз в сутки.

Любые файлы, полученные из сети Интернет, должны автоматически проверяться на наличие вирусов и открываться только в случае подтверждения отсутствия вирусной опасности.

Устанавливаемое или изменяемое программное обеспечение серверов и АРМ должно быть предварительно проверено на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена полная антивирусная проверка.

При обнаружении компьютерного вируса необходимо принять меры по устранению последствий вирусной атаки, проинформировать администратора информационной безопасности и, при необходимости, приостановить работу (на период устранения последствий вирусной атаки). В случае обнаружения вирусной атаки должно проводиться «лечение» зараженных файлов (без запроса действия у пользователя). В случае невозможности лечения - должно выдаваться сообщение администратору для дальнейшего принятия им требуемых мер.

Не должно допускаться самостоятельное удаление пользователями зараженных файлов.

Отключение или отказ от обновления антивирусных средств не допускается. Установка и обновление антивирусных средств в Учреждении должны контролироваться администратором информационной безопасности и системным администратором.

Ответственность за выполнение требований по антивирусной защите должна быть возложена на руководителя подразделения информационных технологий Учреждения, а обязанности по выполнению мер антивирусной защиты должны быть возложены на каждого сотрудника Учреждения, имеющего доступ к АРМ и ЛВС.

Должны проводиться периодические антивирусные проверки АРМ в соответствии с «Регламентом периодического тестирования СЗИ в ЛВС Учреждения».

#### **5.3.5 Межсетевое экранирование**

Подключение к сети Интернет должно осуществляться по выделенному каналу, защищенному межсетевым экраном (МЭ).

МЭ администрируется администратором безопасности локально или удаленно (только из ЛВС с АРМ администратора информационной безопасности).

Должна обеспечиваться идентификация и аутентификация администратора информационной безопасности при его запросах на доступ.

Должна обеспечиваться регистрация загрузки, инициализации системы и остановки работы МЭ.

Межсетевой экран должен быть корректно настроен, чтобы обеспечивать:

- фильтрацию трафика, поступающего со стороны внешней сети на сетевом, транспортном и прикладном уровне;
- трансляцию сетевых адресов при взаимодействии с внешней сетью;
- противодействие попыткам определения топологии ЛВС, активности оборудования, запущенных сетевых служб;
- противодействие атакам типа «отказ в обслуживании»;
- блокировку иных дестабилизирующих воздействий со стороны внешней сети;
- регистрацию попыток подключения со стороны внешней сети и регистрацию этих данных в своем журнале аудита.

МЭ должен содержать средства контроля за целостностью своей программной и информационной части.

МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление заданных свойств.

МЭ должен обеспечивать достаточную пропускную способность и отказоустойчивость.

Настройка МЭ должна осуществляться в соответствии с действующими правилами регламентации трафика. Данные правила должны быть изложены в соответствующем документе («Регламент настройки межсетевого экрана»).

Нерегламентированный трафик должен блокироваться.

Межсетевое экранирование должно применяться при организации защиты периметра КС и серверного сегмента (внутренних серверов).

### **5.3.6 Электронная почта, web-сервер**

Ресурсы сети Интернет в Учреждении могут использоваться для ведения деловой переписки, получения и распространения информации, связанной с деятельностью Учреждения (путем создания информационных web-сайтов), информационно-аналитической работы в интересах Учреждения, обмена почтовыми сообщениями, обусловленного служебной необходимостью. Иное использование ресурсов сети Интернет, решение о котором не принято руководством Учреждения в установленном порядке, должно рассматриваться как нарушение безопасности информации.

При взаимодействии с сетью Интернет обязательно должны применяться соответствующие сертифицированные средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации (СКЗИ) и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

Запрещается передавать конфиденциальную информацию через открытые соединения с сетью Интернет, в том числе по электронной почте без шифрования такой информации.

В Учреждении должна быть одна точка почтового обмена с сетью Интернет, состоящая из внешнего (подключенного к сети Интернет) и внутреннего (подключенного к внутренним сетям организации) почтовых серверов с безопасной системой репликации почтовых сообщений между ними.

Почтовый сервер должен обеспечивать реализацию следующих функций:

- входящие Интернет-соединения;
- соединения от пользователей ЛВС к почтовым сервисам.

Запрещены к передаче/приему по электронной почте файлы больше установленного системным администратором объема и файлы exe- и com- форматов.

Электронная почта должна архивироваться. Архив должен быть доступен только администратору информационной безопасности. Изменения в архиве не допускаются. Доступ к информации архива должен быть ограничен.

Порядок подключения и использования ресурсов сети Интернет в Учреждении должен контролироваться администратором информационной безопасности.

Удаленный доступ к ЛВС Учреждения с использованием сети Интернет запрещен.

Web-сервер должен поддерживать входящие соединения из Интернет к данному серверу.

### **5.3.7 Резервное копирование данных**

Системный администратор должен осуществлять резервирование данных на файловом и почтовом серверах Учреждения.

Пользователи должны хранить критически важные файлы в специально отведенных для этой цели для каждого подразделения выделенных папках на файловом сервере. Вся

информация должна храниться на серверах и должным образом резервироваться. Для этого все производственные серверы должны иметь горячий резерв.

Резервные копии наиболее важной производственной информации необходимо периодически сохранять на съемных носителях и хранить их в закрытых сейфах в помещениях, отличных от мест расположения файловых серверов.

### **5.3.8 Криптографическая защита**

КИ высокого уровня конфиденциальности должна храниться на АРМ пользователей и в ЛВС Учреждения в зашифрованном виде.

Средства криптографической защиты информации:

- должны допускать встраивание в действующую технологическую схему обработки электронных сообщений, обеспечивать взаимодействие с прикладным ПО на уровне обработки запросов на криптографические преобразования и выдачи результатов;
- должны поставляться разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;
- должны быть реализованы на основе алгоритмов, соответствующих национальным стандартам РФ, условиям договора с контрагентом и (или) стандартам Учреждения;
- должны иметь строгий регламент использования ключей, предполагающий контроль со стороны администратора информационной безопасности за действиями пользователя на всех этапах работы с ключевой информацией (получение ключевого носителя, ввод ключей, использование ключей и сдача ключевого носителя);
- не должны содержать требований к ЭВМ по специальной проверке на отсутствие закладных устройств, если иное не оговорено в технической документации на конкретное средство защиты;
- не должны требовать дополнительной защиты от утечки по ПЭМИН.

При применении СКЗИ должны поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности ПО.

Безопасность процессов изготовления ключевых документов СКЗИ должна обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты.

Внутренний порядок применения СКЗИ определяется руководством Учреждения и 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.

### **5.3.9 Организация взаимодействия между удаленными сегментами корпоративной сети**

Взаимодействие между удаленными сегментами КС должно осуществляться с использованием VPN-соединения, построенного на основе используемой в качестве транспортной среды телекоммуникационной сети провайдера.

Организация VPN-сети обеспечивает защиту информации передаваемой при взаимодействии между сегментами корпоративной сети с помощью следующих механизмов:

- организация шифрованного логического соединения на основе криптоалгоритмов, сертифицированных ФСБ РФ;
- использование надежных с точки зрения безопасности информации методов аутентификации и средств организации VPN-сетей.

Должен быть организован мониторинг за установленными VPN-соединениями.

В каждом сегменте должен быть регламентирован перечень объектов доступа, доступных для пользователей внешних сегментов корпоративной сети.

Применение сертифицированных средств криптографической защиты необходимо в случаях, когда этого требует законодательство (то есть только для случая передачи ПДн).

#### **5.4 Физические меры**

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключаящими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

##### **5.4.1 Установка и использование средств охранно-пожарной сигнализации**

В помещениях Учреждения должны быть установлены необходимые элементы системы охранно-пожарной сигнализации: дымовые и/или тепловые пожарные датчики, датчики охранной сигнализации, извещатели, а также средства пожаротушения.

Должен проводиться периодический профилактический осмотр указанных средств на предмет своевременного выявления неисправностей.

##### **5.4.2 Установка и использование средств физической защиты**

Помещения Учреждения должны быть оборудованы запирающими конструкциями (электромеханическими замками).

Помещения, в которых ведется обработка конфиденциальной информации, должны быть оборудованы дополнительными средствами ограничения доступа.

В отделах и службах Учреждения при необходимости должны быть установлены сейфы для хранения носителей конфиденциальной информации и материальных ценностей.

### **6 КОНТРОЛЬ ЭФФЕКТИВНОСТИ ЗАЩИТЫ**

Эффективность защиты информации - это степень соответствия реального функционирования и состояния СЗИ поставленным целям.

Основным принципом оценки эффективности является постоянный контроль выполнения требований действующих законодательных, нормативно-методических и организационно-распорядительных документов по данной проблеме.

Для оценки эффективности используются показатели, определяемые действующими нормами, установленными нормативными документами ФСТЭК, ФСБ, Мининформсвязи РФ и

документами Учреждения.

Контроль эффективности проводимых мероприятий по защите информации и выполнения требований Положения осуществляется лицами, ответственными за безопасность информации в Учреждении, с докладом руководству Учреждения. Состав сотрудников, ответственных за проведение контрольных мероприятий, определяется в соответствии с Положением.

Непосредственный контроль за выполнением требований Положения при обработке информации в ЛВС Учреждения осуществляется администратором информационной безопасности.

Контроль может проводиться как открытый - в ходе различных проверок на рабочих местах, так и негласный (по сети) - с рабочего места администратора информационной безопасности.

Необходимо отслеживать состояние работы всех элементов СЗИ, входящих в состав защитных механизмов и соответствующих мер и мероприятий, корректность выполнения ими своих функций и соответствия результатов их выполнения заданным показателям. В целях оценки эффективности действующей СЗИ проводится ее аудит.

Аудит СЗИ Учреждения может быть внутренним или внешним. Порядок и периодичность проведения внутреннего аудита в целом или отдельных структурных подразделений, а также ЛВС определяется руководством Учреждения на основе потребностей в такой деятельности. Внешний аудит СЗИ проводится независимыми аудиторами.

Цель аудита СЗИ состоит в проверке и оценке ее соответствия требованиям настоящего Положения и других принятых в организации нормативных актов по защите информации. Аудит СЗИ должен проводиться периодически.

При проведении аудита СЗИ должны использоваться стандартные процедуры документальной проверки, опрос и интервью с руководством и персоналом Учреждения. При необходимости уточнения результатов документальной проверки, опросов и интервью в рамках внутреннего аудита СЗИ в качестве дополнительного способа может применяться «проверка на месте», которая проводится для обеспечения уверенности в том, что конкретные защитные меры реализуются, правильно используются и проверяются с помощью тестирования. Обстоятельства, при которых требуется дополнительный способ в рамках внутреннего аудита СЗИ, должны быть определены и согласованы в плане проведения аудита.

При проведении внутреннего аудита СЗИ могут использоваться журналы регистрации событий, ведущиеся администраторами информационной безопасности Учреждения и формируемые на основе данных мониторинга СЗИ.

При проведении внешнего аудита СЗИ руководство Учреждения должно обеспечить документальное и, если это необходимо, техническое подтверждение того, что:

- Положение отражает требования и цели Учреждения;
- организационная структура управления СЗИ создана;
- процессы выполнения требований по защите информации реализуются и удовлетворяют поставленным целям;
- защитные меры (например, межсетевые экраны, средства управления физическим доступом) настроены и используются правильно;
- остаточные риски оценены и остаются приемлемыми для организации;
- рекомендации предшествующих аудитов СЗИ реализованы.

Аудиторский отчет должен храниться в Учреждении в течение установленного

времени. Доступ к аудиторскому отчету должен быть разрешен только руководству организации и руководителям подразделения (лицам), ответственным за безопасность информации в Учреждении.

Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам.

Несоответствие принимаемых мер установленным требованиям или нормам является нарушением.

## **7 ОТВЕТСТВЕННОСТЬ**

Все сотрудники Учреждения, допущенные в установленном порядке к работе с защищаемой информацией, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности такой информации и соблюдение правил работы с ней, установленных данным Положением и иными организационно-распорядительными документами Учреждения, разработанными на его основе.

Ответственность за доведение требований настоящего Положения до сотрудников Учреждения и обеспечение мероприятий по их реализации несет руководство Учреждения.

Все сотрудники Учреждения обязаны неукоснительно соблюдать относящиеся к ним требования настоящего Положения.

Отказ соблюдать настоящее Положение может подвергнуть защищаемую информацию Учреждения недопустимому риску потери целостности, доступности, актуальности или конфиденциальности при ее хранении, обработке или передаче.

Нарушения сотрудниками Учреждения положений, инструкций, руководств и иных организационно-распорядительных документов, поддерживающих данное Положение, будут рассматриваться руководством Учреждения в административном порядке и лица-нарушители будут привлекаться к ответственности в установленном действующим законодательством порядке.

## **8 МЕРОПРИЯТИЯ ПО РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ПОЛОЖЕНИЯ**

Состав, порядок, сроки исполнения указанных мероприятий, а также лица ответственные за их проведение, указываются в разрабатываемых на основании данного Положения документах.

В состав данных мероприятий должны быть включены следующие меры:

### **Организационные:**

- разработка соответствующего комплекса организационно-распорядительной документации, включающей различные инструкции, руководства, положения и прочие документы;
- ознакомление с Положением и соответствующими инструкциями и руководствами сотрудников Учреждения;
- обучение сотрудников Учреждения основам обеспечения безопасности информации, в случае необходимости;
- контроль за выполнением требований организационно-распорядительной документации.

### **Технические:**

- мониторинг угроз безопасности информации;
- внедрение технических и программно-аппаратных средств защиты;

- поддержание указанных средств в работоспособном состоянии, их техническая поддержка и обслуживание;
- технический контроль за соблюдением требований Положения и поддерживающих его документов;
- осуществление соответствующих мероприятий по ЗИ.

## **9 ЗАКОНОДАТЕЛЬНАЯ И НОРМАТИВНАЯ БАЗА**

Указ Президента РФ от 5 декабря 2016 г. N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»

Федеральный закон Российской Федерации от 9 февраля 2009 №8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»

Федеральный Закон Российской Федерации от 29.07.2004 № 98-ФЗ «О коммерческой тайне»

Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями)

Федеральный закон Российской Федерации от 27.12.2002 № 184-ФЗ «О техническом регулировании».

Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

Указ Президента Российской Федерации от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера».

Указ Президента РФ от 17.03.2008 года N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена ».

Указ Президента РФ от 3 апреля 1995 года N 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».

Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Постановление Правительства Российской Федерации от 22 сентября 2009 г. №754 «Об утверждении Положения о системе межведомственного электронного документооборота».

Приказ ФСТЭК России от 18 февраля 2013г. №21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена Федеральной службой по техническому и экспортному контролю 15 февраля 2008 г.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена Федеральной службой по техническому и экспортному контролю 14 февраля 2008 г.

Нормативно-методический документ Государственной технической комиссии при Президенте Российской Федерации «Специальные требования и рекомендации по



|  |                   |
|--|-------------------|
| <b>Система менеджмента качества</b><br><b>ПОЛОЖЕНИЕ О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ РАБОТ ПО ЗАЩИТЕ</b><br><b>КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ</b> | Страница 25 из 25 |
|--|-------------------|

технической защите конфиденциальной информации (СТР-К)», утвержденный приказом Гостехкомиссии России от 30.08.2002 года № 282.