Утверждаю
Ректор
_____ Л.Н.Горбатова
«26» 05. 2021 г.

ПОЛИТИКА
информационной безопасности
Федерального государственного
бюджетного образовательного
учреждения высшего образования
«Северный государственный медицинский университет»
Министерства здравоохранения Российской Федерации

Версия 2.0

Дата введения: 26.05.2021.

Архангельск
2021

	Должность	Фамилия/подпись	Дата
Разработал	Директор информационно-интеллектуального центра	Трифонов И.А.	02.04.2021.
Проверил	Начальник управления правового и кадрового обеспечения	Котлов И.А.	02.04.2021.
Согласовал	Первый проректор, проректор по учебно-воспитательной работе	Оправин А.С.	02.04.2021.
	Проректор по цифровой трансформации и инфраструктурному развитию	Халезин А.С.	02.04.2021.

1. Рассмотрено на заседании Ученого совета, протокол № 12 от «14» 04 2021 г.
2. Утверждено и введено в действие приказом Ректора, № 146 от «26» 05 2021 г.
3. Соответствует требованиям СГМУ.
4. Введено в действие взамен Политики информационной безопасности – версия 1.0.

СОДЕРЖАНИЕ

1.ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящая Политика распространяется на все структурные подразделения Университета и обязательна к исполнению всеми ее работниками и ответственными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах Университета, а также в договорах.

2.НОРМАТИВНЫЕ ССЫЛКИ

Настоящая Политика разработана с учетом следующих документов:

- Федеральный закон "Об информации, информационных технологиях и защите информации" от 27.07.2006 № 149-ФЗ;
- Федеральный закон «О коммерческой тайне» от 29.07.2004 года №98-ФЗ;
- Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ;
- Постановление правительства от 3 ноября 1994г. № 1233
- ГОСТ Р ИСО 9001-2008 Система менеджмента качества. Требования.
- Гостехкомиссия «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» 2 марта 2001 г №7.2

3.ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ,ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящей Политике используются следующие термины.

Автоматизированная система (АС): Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аудит информационной безопасности Университета: процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самим Университетм (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит) на основе рекомендаций ГОСТ Р ИСО 9001-2008 и ГОСТ Р ИСО/МЭК

17799-2005. Результаты проверки документально оформляются свидетельством аудита.

Информационная технология: совокупность правил, приемов и методов применения средств вычислительной техники для выполнения функций хранения, обработки, передачи и использования производственной, финансовой, аналитической или иной информации, связанной с функционированием Университета информации.

Информационный технологический процесс: часть производственного технологического процесса, содержащая операции над информацией, необходимой для функционирования Университета.

Информационная безопасность Университета: состояние защищенности информационных активов Университета в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т. п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов Университета. Защищенность достигается обеспечением совокупности свойств информационной безопасности - конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры Университета.

Информационные активы Университета: активы Университета, имеющие отношение к его информационной сфере и представляющие ценность для нее с точки зрения достижения уставных целей.

Инцидент информационной безопасности: действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов Университета.

Код аутентификации электронного сообщения: данные, используемые для установления подлинности и контроля целостности электронного сообщения.

Мониторинг информационной безопасности Университета: постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности Университета, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы, информационные услуги и пр.

Политика информационной безопасности Университета: комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в Университете для обеспечения информационной безопасности.

Риск: Мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

Роль в Университете: заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом в Университете. К субъектам относятся персонал Университета, его партнеры, обучающиеся, а также инициируемые от их имени действия над объектами. Объектами являются аппаратные и программные средства, информационные ресурсы, услуги и процессы, составляющие автоматизированную систему.

Угроза: Опасность, предполагающая возможность потерь (ущерба).

Управление информационной безопасностью Университета: совокупность целенаправленных действий, осуществляемых в рамках Политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость: недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности Университета при реализации угроз в информационной сфере.

АС - автоматизированная система; АСП - аналог собственноручной подписи

ИБ - информационная безопасность;

ИС - информационная система; КА - код аутентификации;

ЛВС - локальная вычислительная сеть;

НСД - несанкционированный доступ;

ОС

операционная система;

РФ - Российская Федерация;

СКЗИ - средство криптографической защиты информации;

СУБД - система управления базами данных;

ЭВМ - электронная вычислительная машина;

ЭЦП - электронная цифровая подпись.

ИСПДн - информационная система персональных данных

4. ИСХОДНАЯ КОНЦЕПТУАЛЬНАЯ СХЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УНИВЕРСИТЕТА

4.1. Концептуальная схема информационной безопасности Университета направлена на защиту ее информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

4.2. Наибольшими возможностями для нанесения ущерба Университета обладает ее собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне Университета), либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

4.3. Для противодействия угрозам информационной безопасности в Университете на основе имеющегося опыта составляется модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ Университета при минимальных ресурсных затратах.

4.4. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

4.5. Стратегия обеспечения ИБ Университета заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала Университета и других пользователей АС.

5. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИБ

Основными принципами обеспечения ИБ являются следующие:

5.1. Постоянный и всесторонний анализ АС и информационных технологий с целью выявления уязвимостей информационных активов Университета.

5.2. Своевременное обнаружение проблем, потенциально способных повлиять на ИБ Университета, корректировка моделей угроз и нарушителя.

5.3. Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию и совместимости этих мер с действующим технологическим процессом. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей Университета, а также повышать трудоемкость технологических процессов обработки информации и создавать дополнительные сложности для клиентов Университета.

5.4. Контроль эффективности принимаемых защитных мер.

5.5. Персонификация и адекватное разделение ролей и ответственности между сотрудниками Университета, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

5.6. Знание сотрудниками Университета своих работников.

6. ЦЕЛИ И ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УНИВЕРСИТЕТА

6.1. Основными целями защиты информации Университета являются:

- повышение стабильности функционирования Университета в целом;
- достижение адекватности мер по защите от реальных угроз ИБ;
- предотвращение или снижение ущерба от инцидентов ИБ.

6.2. Основными задачами деятельности по обеспечению ИБ Университета являются:

- выполнение требований законодательства по обеспечению ИБ;

- контроль выполнения установленных требований по обеспечению ИБ;
- повышение эффективности мероприятий по обеспечению и поддержанию информационной безопасности с учетом требований системы менеджмента качества;
- разработка и совершенствование регламентирующих документов Университета в области обеспечения информационной безопасности;
- выявление, оценка и прогнозирование угроз информационной безопасности;
- выработка рекомендаций по устранению уязвимостей;
- организация антивирусной защиты информационных активов;
- защита информации от НСД и утечки по техническим каналам связи.

7. ОБЪЕКТЫ ЗАЩИТЫ

7.1. Объектами защиты информации в Университете являются:
- производственный процесс;
- финансовая информация;
- информационный технологический процесс;
- персональные данные
- различного рода носители защищаемой информации, в том числе информационные ресурсы, документы на бумажных и машинных носителях, определенные как защищаемые нормативно-распорядительными документами Университета.

7.2. Защищаемая информация делится на следующие виды:
- информация, составляющая коммерческую тайну, научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой

обладателем такой информации введен режим коммерческой тайны (определяется Перечнем защищаемых сведений, составляющих коммерческую тайну Университета в соответствии с Федеральным Законом «О коммерческой тайне»).

- персональные данные - сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (в соответствии с Трудовым кодексом и другими законодательными актами Российской Федерации).
- иная информация, не относящаяся ни к одному из указанных выше видов, которая определена как защищаемая Приказами и распоряжениями руководства Университета.

8. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ

8.1. Модели угроз и нарушителей (прогноз ИБ) являются определяющими при развертывании, поддержании и совершенствовании системы обеспечения ИБ Университета.

8.2. Источники угроз, уязвимости и объекты нападений, пригодные для реализации угрозы, типы возможных потерь, масштабы потенциального ущерба определяются документом «Модели угроз и нарушителей», разрабатываемым работниками ответственными за информационную безопасность и отделом информатизации (далее - ОИ).

9. ТРЕБОВАНИЯ ПО ИНФОРМАТИОННОЙ БЕЗОПАСНОСТИ

9.1. Общие требования по обеспечению информационной безопасности

Требования ИБ формулируются для следующих областей:

- назначение и распределение ролей и доверия к персоналу;
- стадий жизненного цикла АС;
- защиты от НСД, управления доступом и регистрацией в АС;

- антивирусной защиты;
- использования ресурсов Интернет;
- использования средств криптографической защиты информации;
- защиты информационных технологических процессов;
- защита от аварийных сбоев в электроснабжении и телекоммуникационных каналах связи.

9.2. Требования по обеспечению информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу Университета:

9.2.1. Для эффективного выполнения целей Университета и задач по управлению активами определяются соответствующие роли персонала Университета. Роли определяются исходя из задач, функциональных и процедурных требований, и обеспечиваются соответствующими ресурсами. Роли персонифицируются с установлением ответственности за их исполнение. Ответственность фиксируется в должностных инструкциях.

9.2.2. С целью снижения рисков нарушения ИБ не рекомендуется, чтобы в рамках одной роли совмещались следующие функции: разработки и сопровождения системы или программного обеспечения, их разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора ИБ, выполнения операций в системе и контроля их выполнения.

9.2.3. Контроль за исполнением требований ИБ осуществляется работниками ответственными за информационную безопасность.

9.2.4. Персонал Университета, а также лица, принимаемые на работу по срочным трудовым договорам и для прохождения практики, (стажировки) подписывают обязательство о неразглашении конфиденциальной информации.

9.2.5. Компетентность персонала Университета в области обеспечения ИБ достигается обучением правилам безопасной (с точки зрения ИБ) работы, изучением соответствующих регламентирующих документов, осведомленности персонала об источниках потенциальных угроз и уязвимостях и периодическими проверками его знаний и навыков.

9.2.6. Обязанности персонала по выполнению требований ИБ включаются в трудовые контракты (соглашения, договоры, должностные инструкции).

9.3. Требования по обеспечению информационной безопасности автоматизированных систем Университета на стадиях жизненного цикла:

9.3.1. ИБ АС должна обеспечиваться на всех стадиях жизненного цикла (ЖЦ) АС, автоматизирующих технологические процессы Университета, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений Университета).

9.3.2. Ввод в действие и снятие с эксплуатации систем защиты АС осуществляются при участии работников ответственных информационную безопасность.

9.4. Требования по обеспечению информационной безопасности при управлении доступом и регистрации:

9.4.1. Права доступа персонала и клиентов к активам Университета распределяются в соответствии с Положением об управлении доступом к информации, обрабатываемой средствами вычислительной техники.

9.4.2. Требуется использовать в составе АС сертифицированные или разрешенные к применению средства защиты информации от НСД.

9.4.3. В Университете должна обеспечиваться авторизация, контроль и управление доступом к информационным активам, в том числе:

- функционирование системы парольной защиты ЭВМ и ЛВС, определенной в Инструкции по организации парольной защиты;

- регистрация действий персонала и пользователей в журналах событий системного программного обеспечения. Данные электронные журналы доступны для чтения, анализа и резервного копирования только администратору соответствующего ПО, который несет персональную ответственность за полноту и точность отражения в журнале имевших место событий;
- аудит действий пользователей автоматизированной системы.

9.5. Требования по обеспечению информационной безопасности средствами антивирусной защиты:

9.5.1. Установка и регулярное обновление средств антивирусной защиты на автоматизированных рабочих местах осуществляется ответственным сотрудником ОИ. На всех ЭВМ Университета настраивается автоматическая установка обновлений антивирусного программного обеспечения.

9.5.2. Ответственность за неисполнение или ненадлежащее исполнение требований Инструкций по антивирусной защите возлагается на каждого работника Университета, имеющего доступ к ПЭВМ.

9.6. Требования по обеспечению информационной безопасности при использовании ресурсов международной сети Интернет:

9.6.1. Ресурсы сети Интернет в Университете используются для получения и распространения информации, связанной с деятельностью Университета, информационно-аналитической работы в интересах Университета, обмена почтовыми сообщениями с внешними организациями, а также ведения собственной хозяйственной деятельности. Любое иное использование ресурсов сети Интернет, решение о котором не принято руководством Университета в установленном порядке, рассматривается как нарушение ИБ.

9.6.2. Порядок подключения и использования ресурсов сети Интернет регламентируется соответствующим Положением.

9.7. Требования по обеспечению информационной безопасности при использовании средств криптографической защиты информации:

9.7.1. Внутренний порядок применения СКЗИ в технологических процессах Университета должны определяться Положением по использованию средств криптографической защиты информации.

9.7.2. Порядок обращения с носителями ключевой информации определяется Порядком по учету и хранению носителей ключевой информации.

9.7.3. Разработка документов по применению СКЗИ и по обращению и хранению носителей ключевой информации, их своевременное обновление осуществляется администратором информационной безопасности Университета. Контроль за исполнением данных документов должен выполняться ответственным за ИБ.

9.8. Требования по обеспечению информационной безопасности технологических процессов Университета:

9.8.1. Система обеспечения информационной безопасности технологического процесса Университета строится в соответствии с требованиями пунктов 11.2 - 9.7 настоящей Политики и иных нормативных документов по вопросам ИБ.

9.8.2. Информационный технологический процесс Университета определяется в Положениях, Регламентах и других нормативно-методических документах Университета.

9.8.3. Работники Университета, в том числе администраторы информационных систем и средств защиты информации, не должны обладать всей полнотой полномочий для бесконтрольного создания, авторизации, уничтожения и изменения информации, а также проведения операций по изменению состояния записей в базах данных.

9.8.4. Результаты технологических операций по обработке информации контролируются и удостоверяются должностными лицами или автоматизированными процессами. Ответственные лица или

автоматизированные процессы, осуществляющие обработку информации и контроль (проверку) результатов обработки, не зависят друг от друга.

9.8.5. При работе с информацией должны проводиться авторизация и контроль целостности данной информации.

9.8.6. Подготовленная партнерами Университета информация, на основании которой совершаются расчетные, учетные и кассовые операции, предназначена для внутреннего использования в Университете и может быть передана иным организациям только в соответствии с действующим законодательством Российской Федерации.

9.8.7. Безопасность информации, отнесенной к коммерческой тайне, обеспечивается в соответствии с требованиями Федерального закона «О коммерческой тайне».

9.8.8. Обязанности по администрированию доступа пользователей к информации, передаваемой по электронным каналам связи, возлагаются приказом по Университету на администраторов соответствующих ИС с отражением этих функций в их должностных обязанностях.

9.8.9. Комплекс мер по обеспечению информационной безопасности технологического процесса Университета должен предусматривать:

- защиту информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации документов;
- минимально необходимый, гарантированный доступ работника Университета только к тем ресурсам информационного технологического процесса, которые необходимы ему для исполнения служебных обязанностей или реализации прав, предусмотренных технологией обработки информации;
- контроль исполнения установленной технологии подготовки, обработки, передачи и хранения информации;
- аутентификацию обрабатываемой информации;

- восстановление информации в случае ее умышленного или случайного разрушения (искажения) или выхода из строя средств вычислительной техники;
- гарантированную доставку сообщений участникам информационного обмена.

9.9. Требования по обеспечению информационной безопасности информационных технологических процессов Университета:

9.9.1. Система обеспечения ИБ информационного технологического процесса Университета должна соответствовать требованиям пунктов 11.2 -11.7 настоящей Политики и иных нормативных документов по вопросам ИБ, действие которых распространяется на производственные процессы.

9.9.2. В Университете информация классифицируется как:
- открытая информация, предназначенная для официальной передачи во внешние организации и средства массовой информации;
- внутренняя информация, предназначенная для использования исключительно сотрудниками Университета при выполнении ими своих служебных обязанностей;
- информация, содержащая сведения ограниченного распространения в соответствии с утвержденным в Университете Перечнем защищаемых сведений и подлежащая защите в соответствии с законодательством РФ.

9.9.3. Для защиты информации, обрабатываемой в ИС, могут назначаться администраторы (ответственные) ИС (далее - Администраторы т.е. лица, наделенные конкретными полномочиями). Функции, права и обязанности администратора ИБ каждого приложения определяются соответствующим приказом. Допускается назначение одного администратора ИБ на несколько компонентов ИС, а также совмещение выполнения указанных функций с другими обязанностями.

9.9.4. Процессы подготовки, ввода, обработки и хранения информации, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств должны быть регламентированы и обеспечены инструктивными и методическими материалами, согласованными с ответственными по информационной безопасности.

9.9.5. На Предприятии должны быть разработаны процедуры восстановления системы обеспечения ИБ после технических сбоев или преднамеренных атак.

10. ОБЩИЕ ТРЕБОВАНИЯ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. В Университете должен быть определен и документально зафиксирован перечень ИСПДн. В перечень ИСПДн должна быть включена, как минимум, бухгалтерская информационная система (далее - БИС), целью создания и использования которой является обработка персональных данных.

10.2. Для каждой ИСПДн Университета должны быть определены и документально зафиксированы:

- цель обработки персональных данных в ИСПДн;
- объем и содержание персональных данных, обрабатываемых в ИСПДн;
- перечень действий с персональными данными и способы обработки персональных данных в ИСПДн.

Объем и содержание персональных данных, а также перечень действий и способы обработки персональных данных должны соответствовать целям обработки. В том случае, если для выполнения информационного технологического процесса, реализацию которого поддерживает ИСПДн, нет необходимости в обработке определенных персональных данных, эти персональные данные должны быть удалены.

10.3. Информационные технологические процессы, в рамках которых обрабатываются персональные данные в ИСПДн, должны быть документированы.

10.4. В Университете должен быть определен и документально зафиксирован перечень (список) работников, осуществляющих обработку персональных данных в ИСПДн, либо имеющих доступ к персональным данным. Доступ работников к персональным данным и обработка персональных данных работниками Университета должны осуществляться только для выполнения их должностных обязанностей.

10.5. Работники Университета, осуществляющие обработку персональных данных в ИСПДн, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также должны быть ознакомлены под роспись со всей совокупностью требований по обработке и обеспечению безопасности персональных данных в части касающейся их должностных обязанностей.

10.6. В Университете должен быть определен и документально зафиксирован порядок доступа работников в помещения, в которых ведется обработка персональных данных.

10.7. В Университете должен быть определен и документально зафиксирован порядок хранения материальных носителей персональных данных, устанавливающий:

- места хранения материальных носителей персональных данных;
- требования по обеспечению безопасности персональных данных;
- работников, ответственных за реализацию требований по обеспечению безопасности персональных данных;
- порядок контроля выполнения требований по обеспечению безопасности персональных данных.

10.8. При использовании в ФГБОУ ВО СГМУ (Г. Архангельск) Минздрава России типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться требования установленные «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15 сентября 2008 г. N 687

11. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, РАСПРЕДЕЛЕНИЕ ФУНКЦИЙ ПО ОБЕСПЕЧЕНИЮ ИБ МЕЖДУ ПОДРАЗДЕЛЕНИЯМИ И ОТВЕТСТВЕННЫМИ ЛИЦАМИ УНИВЕРСИТЕТА

11.1. Управление информационной безопасностью Университета:

11.1.1.Управление ИБ Университета включает в себя:

- разработку политики информационной безопасности;
- разработку регламентирующих и методических документов обеспечения ИБ;
- обеспечение штатного функционирования комплекса средств ИБ Университета;
- осуществление контроля (мониторинга) функционирования системы ИБ;
- обучение с целью поддержки (повышения) квалификации персонала Университета;
- оценку рисков, связанных с нарушениями ИБ.

11.2. Распределение функций по обеспечению ИБ между подразделениями и ответственными работниками:

11.2.1. Основными функциями по обеспечению информационной безопасности, выполняемыми ответственными по информационной безопасности, являются:

- разработка политики информационной безопасности;
- разработка технических, организационных и административных планов реализации политики ИБ;
- методическое обеспечение при разработке регламентирующих и методических документов обеспечения ИБ;
- согласование проектов всех внутренних документов, затрагивающих вопросы безопасности технологий, используемых в Университете;
- подготовка рекомендаций по выбору средств защиты информации;
- администрирование средств защиты информации Университета в части обеспечения работоспособности прикладного программного обеспечения и их обновления;
- осуществление методического руководства структурными подразделениями Университета по вопросам информационной безопасности;
- участие в обеспечении бесперебойной работы автоматизированных систем Университета и восстановлении её работы после сбоев;
- осуществление централизованного учета носителей ключевой информации;
- обучение пользователей безопасной работе с информационными активами;
- контроль соблюдения требований по использованию антивирусных средств;
- участвовать в расследовании событий, связанных с инцидентами ИБ, и в случае необходимости выходить с предложениями по применению санкций в отношении лиц, осуществивших НСД, например, нарушивших требования инструкций, руководств и т. п. по обеспечению ИБ Университета.

11.2.2. Ряд функций по обеспечению информационной безопасности выполняют следующие структурные подразделения и работники Университета:

11.2.2.1. Ответственные за информационную безопасность:
- участвует в проведении проверок по соблюдению требований ИБ;
- определение и оценка рисков, связанных с нарушениями ИБ;

11.2.2.2. Общий отдел:

- осуществляет регистрацию и рассылку в сторонние организации защищаемой информации на бумажных носителях.

11.2.2.3. Руководители структурных подразделений Университета:

- контролируют безопасность работы с информацией подчиненными работниками,
- обеспечивают соблюдение положений настоящей Политики, и иных документов по защите информации в подразделении.

12. АУДИТ И САМООЦЕНКА ИБ

12.1. Порядок и периодичность проведения аудита ИБ Университета в целом (или отдельных структурных подразделений) определяется руководителем Университета на основании потребности в такой деятельности.

12.2. Внешний аудит ИБ проводится независимыми аудиторами. Цель аудита ИБ Университета состоит в проверке и оценке ее соответствия требованиям настоящей Политики и других нормативных актов. Внешний аудит ИБ проводится по отдельному решению руководителя.

12.3. Мониторинг ИБ проводится ответственными за обеспечение информационной безопасности совместно с ОИ с целью обнаружения и регистрации отклонений защитных мер от требований ИБ и оценки полноты реализации положений Политики ИБ, инструкций и руководств по обеспечению информационной безопасности Университета.

12.4. При проведении внешнего аудита ИБ руководство Университета обеспечивает документальное и, если это необходимо, техническое подтверждение того, что:

- политика ИБ отражает требования бизнеса и цели Университета;
- организационная структура управления ИБ создана;

- процессы выполнения требований ИБ исполняются и удовлетворяют поставленным целям;
- защитные меры (например, межсетевые экраны, средства управления физическим доступом) настроены и используются правильно;
- риски оценены и остаются приемлемыми для Университета;
- система управления ИБ соответствует требованиям защиты;

12.5. При подготовке к аудиту ИБ рекомендуется проведение самооценки ИБ. Самооценка ИБ проводится собственными силами и по инициативе руководства Университета.

13. ПОРЯДОК ПЕРЕСМОТРА ПОЛИТИКИ

13.1. Пересмотр Политики информационной безопасности производится не реже одного раза в три года и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.

13.2. Пересмотр Политики осуществляется специально назначаемой для этой цели постоянно действующей комиссией по защите информации или создается рабочая группа по пересмотру Политики.

13.3. С момента утверждения Политики руководителем, утрачивает силу предыдущая Политика информационной безопасности ФГБОУ ВО СГМУ (г.Архангельск) Минздрава России.

14. УТВЕРЖДЕНИЕ И ИЗМЕНЕНИЕ ПОЛОЖЕНИЯ

14.1. Настоящее Положение вводится в действие с момента подписания приказа Ректором.

14.2. Ответственность за соблюдение требований, изложенных в данном Положении, несет Директор ИИЦ.

14.3 Изменения и дополнения в Положение вносятся по инициативе:

- ректора СГМУ;
- первого проректора, проректора по учебно-воспитательной работе;
- проректор по инфраструктурному развитию
- директор ИИЦ;
- начальника управления правового и кадрового обеспечения;