МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«СЕВЕРНЫЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Российской Федерации

ПРИКАЗ

«06» июля 20 26 г. № 421

г. Архангельск

Об утверждении «Политики информационной безопасности» и размещении на официальном сайте

В целях обеспечения в федеральном государственном бюджетном образовательном учреждении высшего образования «Северный государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее – Университет) исполнения требований Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 11.04.2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и других законодательных актов Российской Федерации в области защиты информации,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие «Политику информационной безопасности», определяющую направление деятельности в области обеспечения информационной безопасности и систематизирующую цели и задачи информационной безопасности, которыми руководствуется Университет в своей работе по обеспечению защиты информации и персональных данных.

2. Разместить в соответствующем разделе на официальном сайте Университета в сети «Интернет» утвержденную «Политику информационной безопасности».

3. Контроль за исполнением приказа возложить на и.о. проректора по цифровой трансформации Яценко А.А.

И.о. ректора Н.А. Былова

Исп. Чернышов С. Е.
(8182) 28-57-69

Утверждаю
И.о. ректора ФГБОУ ВО СГМУ
(г. Архангельск)
Минздрава России, к.м.н.,
Н.А. Былова

«06» июля 2026 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Версия 2.0

Дата введения: 06.07. 2026 г.

Архангельск
2026

	Должность	Фамилия/подпись	Дата
Разработал	Специалист по защите информации отдела ИТС	Чернышов С. Е.	03.06.26
Проверил	Начальник управления правового и кадрового обеспечения	Сороченко Н.С.	03.06.26
Согласовал	И.о проректора по цифровой трансформации	Яценко А. А.	03.06.26

1. Рассмотрено на заседании Ученого совета, протокол № 17 от «03» 06 2026г.
2. Утверждено и введено в действие приказом и.о. ректора университета № 421 от «06» июля 2026г.
3. Соответствует требованиям вуза.

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Аудит информационной безопасности – процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самой организацией (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит).

Аутентификация – действия по проверке подлинности субъекта доступа в информационной системе.

Безопасность информации – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Государственная информационная система (ГИС) – информационная система, создаваемая в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

Доступ к информации – возможность получения информации и ее использования.

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

Защита информации от несанкционированного доступа – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

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

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

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

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

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов).

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

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

Ключевая информация - секретные ключи или пары открытых и закрытых ключей, которые позволяют зашифровать и расшифровать информацию.

Ключевой носитель – электронный носитель ключевой информации, содержащий один или несколько ключей (сертификатов, электронно-цифровых подписей), данных, используемых для аутентификации владельца.

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

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

Мониторинг информационной безопасности – постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности, 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.

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.

Объект информатизации – это совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

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

Персональные данные – это любая информация, которая прямо или косвенно относится к конкретному физическому лицу и позволяет его идентифицировать.

Пользователь – гражданин или юридическое лицо, использующее вычислительную систему или программное средство для выполнения конкретной функции.

Риск – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

Сертификат открытого ключа (сертификат электронной подписи, сертификат ключа подписи, сертификат ключа проверки электронной подписи) – электронный или бумажный документ, содержащий открытый ключ, информацию о владельце ключа, области применения ключа, подписанный выдавшим его Удостоверяющим центром и подтверждающий принадлежность открытого ключа владельцу.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на неё.

Удостоверяющий центр – это государственная организация или коммерческая компания, которая выпускает и выдаёт сертификаты ключей проверки электронных подписей.

Уязвимость – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации.

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

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место

Минцифры – Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

ФСБ России – Федеральная служба безопасности Российской Федерации

ФСТЭК России - Федеральная служба по техническому и экспортному контролю

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая политика информационной безопасности (далее – Политика) является основным документом, определяющим направления деятельности в области обеспечения информационной безопасности и представляет собой систематизированное изложение целей и задач информационной безопасности, как одно или несколько правил, процедур, практических приемов и руководящих принципов, которыми руководствуется Федеральное государственное бюджетное образовательное учреждение высшего образования «Северный государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее – Университет), а также организационных, технологических и процедурных аспектов обеспечения информационной безопасности.

Настоящая Политика разработана в соответствии с положениями и требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи», Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 11.04.2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Положения настоящей Политики не распространяются на обеспечение информационной безопасности сведений, составляющих государственную тайну.

Основной задачей в области информационной безопасности Университет признает совершенствование мер и средств обеспечения защиты информации и всех информационных ресурсов и информационных систем Университета в контексте развития законодательства Российской Федерации и норм регулирования деятельности в области сбора, обработки, классификации, хранения и передачи информации, в том числе содержащей персональные данные, в современных условиях функционирования и развития информационных технологий.

При разработке Политики учитывались основные принципы создания систем защиты информации, характеристики и возможности организационно-распорядительных и технических мер, а также современных программных и аппаратно-программных средств защиты информации.

В рамках своей деятельности Университет обязуется предпринимать все возможные меры для защиты информации от угроз безопасности информации.

Требования информационной безопасности соответствуют целям деятельности Университета и предназначены для снижения и минимизации рисков, связанных с реализацией угроз безопасности информации.

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

Политика доступна всем работникам и учащимся Университета, сторонним пользователям его ресурсов.

2. ЦЕЛИ И ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Субъекты информационных отношений

Субъектами при обеспечении информационной безопасности в Университете являются:

- работники структурных подразделений Университета (в том числе уволенные);
- абитуриенты и студенты всех форм обучения Университета;
- физические лица, работающие по договорам гражданско-правового характера;
- физические лица, получающие медицинские услуги в рамках исполнения договорных обязательств;

- физические лица, представители контрагентов в рамках исполнения договорных обязательств;

- физические и юридические лица, подавшие обращение в адрес Университета;

- юридические лица, в рамках исполнения договорных обязательств или во исполнении требований со стороны законодательства Российской Федерации;

- органы государственной власти всех уровней.

Объекты информационных отношений

Объектами при обеспечении информационной безопасности являются:

- информационные ресурсы и информационные системы Университета;

- государственные информационные системы, Оператором или Пользователем которых является Университет;

- регламенты и процедуры сбора, обработки, классификации, хранения и передачи информации;

- проектная и техническая документация содержащая описание процессов сбора, обработки, классификации, хранения и передачи информации в информационных системах Университета;

- проектная и техническая документация содержащая описание мер, средств и алгоритмов организации защиты информации в информационных системах Университета;

- процессы сбора, обработки, классификации, хранения и передачи информации в информационных системах Университета, и используемые при этом информационные технологии;

- информационная инфраструктура, включающая в себя технические средства для сбора, обработки, хранения и анализа информации, программные и программно-аппаратные средства, в том числе оборудование и каналы связи и телекоммуникации;

- системы и средства защиты информации, объекты и помещения, в которых размещены средства сбора, обработки, классификации, хранения и передачи информации.

Цели обеспечения информационной безопасности

Основной целью Университета при обеспечения информационной безопасности являются действия, направленные на достижение максимальной защиты и минимизации рисков для информационных активов и субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию персоналом,

противоправных действий злоумышленников, потенциального вреда от аварий, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации.

Штатный режим функционирования технологических и информационных процессов Университета достигается следующим путем:

- обеспечение отказоустойчивого функционирования оборудования, программных и аппаратно-программных средств Университета и предоставляемых сервисов;

- соблюдение правового режима использования информационных массивов и средств сбора, обработки, классификации, хранения и передачи информации;

- предотвращение реализации угроз безопасности информации при осуществлении деятельности Университета.

Задачи обеспечения информационной безопасности

Достижение целей обеспечения информационной безопасности Университета решается выполнением следующих задач:

- защита от несанкционированного доступа к информационным ресурсам;

- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам;

- регистрация и периодический контроль действий пользователей при обработке защищаемой информации и периодический контроль корректности их действий;

- контроль целостности среды исполнения программ и ее восстановление в случае нарушения;

- обеспечение аутентификации и идентификации пользователей, участвующих в информационном обмене;

- обеспечение исправности применяемых в информационных системах Университета средств защиты информации;

- своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;

- создание службы мониторинга и реагирования на угрозы безопасности информации и негативные последствия;

- создание условий для минимизации наносимого ущерба неправомерными действиями и устранение последствий нарушения информационной безопасности в Университете.

Решение вышеперечисленных задач в Университете осуществляется посредством:

- учета всех подлежащих защите информационных ресурсов;

- журналирования действий пользователей, допущенных к работе с информационными ресурсами и информационными системами и действий персонала, осуществляющего обслуживание и модификацию программных и программно-аппаратных средств информационных систем;

- регламентации процессов сбора, обработки, классификации, хранения и передачи информации, а также действий работников Университета, осуществляющих эксплуатацию программных и программно-аппаратных средств, на основе утвержденных организационно-распорядительных документов по защите информации;

- назначения и подготовкой работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в Университете;

- наделения каждого работника минимально необходимыми правами при работе в информационной инфраструктуре согласно их должностным обязанностям;

- соблюдения всеми пользователями информационных ресурсов и информационных систем, а также работниками, эксплуатирующими и обслуживающими программные и программно-аппаратные средства, требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

- персональной ответственностью каждого работника, участвующего в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к информационным ресурсам и информационным системам;

- реализацией технологических процессов обработки информации с использованием комплекса организационно-технических мер защиты программного обеспечения, программно-аппаратных средств;

- принятия мер по обеспечению физической целостности оборудования, программных и программно-аппаратных средств информационных систем и поддержанием необходимого уровня защищенности компонентов;

- использования программных и программно-аппаратных средств защиты информации, обрабатываемой в Университете, и административной поддержкой их использования;

- контроля соблюдения всеми пользователями информационных систем Университета требований по обеспечению информационной безопасности;

- проведения анализа эффективности принятых мер информационной безопасности и применяемых средств защиты информации в Университете;

- разработки и реализации предложений по совершенствованию систем информационной безопасности в Университете в современных условиях функционирования и развития информационных технологий.

3. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение информационной безопасности в Университете, должно осуществляться в соответствии со следующими основными принципами:

Принцип законности

При выборе мероприятий по защите информации, должно соблюдаться действующее законодательство Российской Федерации в сфере защиты информации. Все работники должны иметь представление об ответственности за правонарушения в сфере защиты информации. Аппаратные и программно-аппаратные средства, применяемые в Университете, должны иметь соответствующие лицензии, официально приобретаться у представителей разработчиков этих средств или являться интеллектуальной собственностью Университета.

Принцип системности

При создании системы защиты должны учитываться актуальные угрозы безопасности информации, возможные объекты и направления атак на неё со стороны нарушителей. Система защиты должна строиться с учетом не только известных каналов утечки информации, но и с учетом возможности появления новых уязвимостей в программном обеспечении.

Принцип комплексности

Комплексное использование средств защиты информации предполагает согласованное применение при построении целостной системы защиты, перекрывающей

все существенные угрозы безопасности информации. Защита должна строиться эшелонировано.

Физическая защита и контроль доступа должны обеспечиваться физическими средствами защиты, автоматизированными средствами контроля и организационно-распорядительными мерами. Информационная защита должна обеспечиваться совокупностью организационно-технических мер и современных сертифицированных программных и аппаратно-программных средств защиты информации.

При построении, внедрении и эксплуатации системы защиты информации руководство Университета обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

Принцип своевременности

Разработка системы защиты информации должна вестись параллельно с разработкой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные информационные системы, обладающие достаточным уровнем защищенности.

Принцип преемственности

Постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, анализа функционирования информационных систем и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите информации.

Принцип достаточности

При планировании системы защиты следует учитывать соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величину возможного ущерба от их разглашения, уничтожения и искажения.

На выбор уровня достаточности влияет гибкость системы защиты, так как внешние условия и требования меняются со временем, и принятые меры и установленные средства защиты могут обеспечивать как чрезмерный, так и недостаточный уровень защиты.

Принцип ответственности

Возложение ответственности за обеспечение безопасности информации и ее обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения был известен нарушитель.

Принцип обоснованности и технической реализуемости

Информационные технологии, программные и программно-аппаратные средства, организационно-распорядительные меры защиты информации должны быть реализованы по современным решениям, обоснованы с точки зрения достижения заданного уровня защищенности информации и экономической целесообразности, а также соответствовать установленным нормам и требованиям по безопасности информации.

Принцип профессионализма

Реализация мер защиты информации и эксплуатация средств защиты информации должна осуществляться профессиональными специалистами. Привлечение специализированных организаций к разработке средств и реализации мер защиты информации, подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и лицензии на право оказания услуг в этой области.

Принцип минимизации привилегий пользователей

Обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих должностных обязанностей в Университете.

4. ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ОБРАБОТКЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Система защиты информации должна предусматривать комплекс организационных, программных и программно-аппаратных средств и мер по защите информации в процессе ее обработки.

Выполнение требований достигается за счет реализации на объектах информатизации следующих мер по защите информации:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей с информацией ограниченного доступа, в т.ч. персональных данных;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение вторжений;

- контроль (анализ) защищенности информации ограниченного доступа, в т.ч. персональных данных;

- обеспечение целостности информационной системы и персональных данных;

- обеспечение доступности информации ограниченного доступа, в т.ч. персональных данных;

- защита среды виртуализации;

- защита технических средств;

- защита информационной системы, ее средств, систем связи и передачи данных;

- выявление инцидентов и реагирование на них;

- управление конфигурацией информационной системы и системы защиты информации ограниченного доступа, в т.ч. персональных данных.

Университет, как обладатель информации ограниченного доступа, в т.ч. персональных данных при осуществлении своих прав обязан:

- соблюдать права и законные интересы иных лиц;

- принимать необходимые меры по защите информации;

- ограничивать доступ к информации, если такая обязанность установлена законодательством Российской Федерации.

В том числе Университет, вправе, если иное не предусмотрено законодательством Российской Федерации:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

- использовать информацию, в том числе распространять ее, по своему усмотрению;

- передавать информацию другим лицам на установленном законодательством Российской Федерации основании;

- защищать установленными законодательством Российской Федерации способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

- осуществлять иные действия с информацией или разрешать осуществление таких действий, если эти действия не противоречат федеральным законам и другим нормативно-правовым актам Российской Федерации.

Защита информации ограниченного доступа в т.ч. персональных данных представляет собой принятие организационных и технических мер, направленных на:

- соблюдение конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);

- обеспечение целостности информации (исключение неправомерного уничтожения или модифицирования информации);

- реализацию права на доступ к информации (исключение неправомерного блокирования информации).

Средства защиты информации внедряются по результатам проведения оценки рисков информационной безопасности.

Организация защиты информации

При организации в Университете защиты информации, должны выполняться требования Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», которые регулируют отношения, связанные с установлением, изменением и прекращением режима обработки защищаемой информации. В том числе требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах утвержденные приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» для государственных информационных систем по которым Университет является Оператором.

Для организации защиты информации, Университет вправе применять средства и методы технической защиты, а также предпринимать другие, не противоречащие законодательству Российской Федерации, меры.

В Университете помимо реализации основных мер защиты информации должны осуществляться:

- регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками;

- информирование, обучение и повышение квалификации работников Университета в сфере информационной безопасности;

- методическая помощь работникам в вопросах обеспечения информационной безопасности;

- анализ и поиск возможностей по повышению уровня защищенности информации.

В контексте обеспечения защиты информации, при оформлении трудовых отношений необходимо ознакомить под роспись работников, доступ которых к информации ограниченного доступа необходим для выполнения ими своих должностных обязанностей, с перечнем информации ограниченного доступа, нормативно-правовыми актами в сфере информационной безопасности и мерами защиты информации, принятыми в Университете, а также ограничениями, связанными с распространением данной информации.

Особенности защиты персональных данных

При организации обработки в Университете персональных данных необходимо руководствоваться требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Перечень мер, выполнение которых обеспечивает Университет в качестве Оператора персональных данных, должен включать:

- назначение в Университете ответственного за организацию обработки персональных данных;

- разработку документов, определяющих правила в отношении обработки персональных данных в Университете, локальных актов по вопросам обработки персональных данных;

- применение организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- выполнение требований нормативно-правовых актов по составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушений, соотношение указанного вреда и принимаемых оператором мер,

направленных на обеспечение выполнения обязанностей, предусмотренных законодательством;

- ознакомление под роспись работников Университета, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, требованиями к защите персональных данных, ответственности за разглашение, а также документами, определяющими требования Университета в отношении обработки персональных данных. При необходимости провести внутреннее обучение указанных работников методам работы с персональными данными и организации защиты информации.

Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз и нарушителей безопасности персональных данных при их обработке в информационных системах персональных данных;

- определением уровня защищенности персональных данных в соответствии с требованиями нормативно-правовых актов;

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценкой эффективности принимаемых мер по защите персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- восстановлением персональных данных, вследствие получения несанкционированного доступа к ним;

- установлением правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;

- контролем за принимаемыми мерами по защите персональных данных и определенного уровня защищенности информационных системах персональных данных в процессе ее эксплуатации.

5. ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ответственным за методическое руководство, разработку решений по защите информации, согласование выбора технических, программных и программно-аппаратных

средств защиты информации, организацию работ по выявлению возможностей и предупреждению утечки и свойств защищаемой информации, аттестацию объектов информатизации является проректор по цифровой трансформации Университета.

Структурные подразделения Университета, в чьих интересах выполняются мероприятия по защите информации не должны препятствовать ответственным за организацию защиты информации работникам Университета в получении информации о выполняемых ролях, регламентах процессов, итоговых результатах работы информационной системы.

Физическая безопасность

Существуют определённые риски, связанные с прямым или косвенным физическим вмешательством в процесс сбора, обработки, классификации, хранения и передачи информации, в т.ч. информации ограниченного доступа и персональных данных.

Принятые организационные и технические решения по защите помещений, серверного и коммутационного оборудования, автоматизированных рабочих мест пользователей информационных систем Университета призваны минимизировать или в целом исключить риски прямого или косвенного физического вмешательства путем реализации следующих мер:

- организация пропускного режима на территорию и в помещения Университета;
- разграничение доступа работников в помещения Университета в соответствии с их полномочиями и должностными обязанностями;
- регистрация фактов входа/выхода работников в помещения в которых ведется обработка персональных данных;
- контролируемое пребывание посторонних лиц в помещениях Университета, в т.ч. в которых ведется обработка информации ограниченного доступа, персональных данных и размещены аппаратные средства информационных систем;
- организация режима контролируемого вноса/выноса средств обработки информации.

Помещения Университета должны быть оборудованы детекторами огня и дыма, огнетушителями, системами кондиционирования воздуха, средствами охранно-пожарной сигнализации.

Основное серверное и коммутационное оборудование Университета должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с

применением источников бесперебойного питания. Источники бесперебойного питания необходимо регулярно тестировать и проверять уполномоченным работникам Университета в соответствии с рекомендациями производителя.

При организации мероприятий с использованием автоматизированных рабочих мест, портативных (мобильных) технических средств за пределами контролируемой зоны Университета, технические средства не должны оставаться без постоянного контроля со стороны ответственных работников Университета.

Безопасность на рабочем месте

Запрещается вести запись паролей в открытом виде на материальных носителях, а также их хранение на рабочем месте Пользователя, за исключением случаев, регламентированных организационно-руководящими документами и предусмотренных ими методов хранения.

При уходе с рабочего места все документы и носители с информацией ограниченного доступа должны убираться в запираемые и опечатываемые места (сейфы, шкафы и т.п.). На время отсутствия Пользователя и прекращения работы на автоматизированном рабочем месте рабочая сессия должна быть прервана, рабочий стол заблокирован. Автоматизированное рабочее место должно быть настроено на автоматическую блокировку через определённое время, но не более 5 минут, при бездействии Пользователя. Вход пользователя в систему не должен выполняться автоматически.

Документы, содержащие информацию ограниченного доступа, должны сразу изыматься из печатающих устройств. Для утилизации документов, содержащих информацию ограниченного доступа, должны использоваться уничтожители документов не ниже 4 уровня по стандарту безопасности, применяемому к уничтожителям документов.

Размещение технических средств вывода информации в помещениях Университета производится с учетом исключения возможности визуального просмотра информации посторонними лицами и работниками, не допущенным к работе с данной информацией.

Технические средства (автоматизированные рабочие места, мобильные технические средства, сервера, оргтехника и т.д.) размещаемые на рабочем месте в обязательном порядке закрепляются за работником Университета, который несёт ответственность за их физическую сохранность, работоспособность и обеспечение защиты информации.

Хранение и размещение технических средств должно быть организовано таким образом, чтобы сократить возможный риск повреждения и угрозы несанкционированного доступа.

Техническое обслуживание и ремонт оборудования

Технические средства Университета должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.

Ремонт и техническое (сервисное) обслуживание оборудования должны выполняться только квалифицированными специалистами.

Текущий (модульный) ремонт технических средств может выполняться силами уполномоченного структурного подразделения Университета с использованием имеющейся ремонтной базы. Сложные ремонты и гарантийное техническое (сервисное) обслуживание осуществляется специализированными сторонними организациями.

Техническое (сервисное) обслуживание оборудования сторонними организациями не должно приводить к риску нарушения конфиденциальности защищаемой информации. При передаче оборудования сторонним организациям для выполнения технического (сервисного) обслуживания с носителей информации находящихся в оборудовании, в случае невозможности их изъятия, в обязательном порядке должна быть удалена вся служебная и защищаемая информация.

Взаимодействие с третьими лицами

В целях обеспечения информационной безопасности Университета при взаимодействии с третьими лицами должны выполняться следующие мероприятия:

- заключение соглашения о неразглашении служебной информации и информации ограниченного доступа полученной в ходе исполнения договорных обязательств;

- осуществление контроля за действиями представителей контрагентов в пределах контролируемой зоны Университета;

- в договорах с третьими лицами предусматривать право Университета на проведение аудита обеспечения безопасности той информации, которая получена в ходе исполнения договорных обязательств.

Нахождение представителей юридических лиц в рамках исполнения договорных обязательств в помещениях в которых ведется обработка информации ограниченного доступа, размещены сервера информационной системы, возможно только в сопровождении работника Университета, допущенного до обработки такой информации.

Управление жизненным циклом информационных систем

Мероприятия по защите информации в процессе жизненного цикла информационных систем Университета должны выполняться при вводе в эксплуатацию, в период эксплуатации, сопровождения, модернизации и вывода из эксплуатации.

Основанием при разработке информационных систем должны являться современные решения принятые на стадии формирования требований к архитектуре, быстродействию, масштабированию, интеграции, а также к системе защиты информации.

Любое планируемое к внедрению изменение информационной системы предварительно должно быть проанализировано на совместимость и отсутствие нарушений работоспособности системных компонентов в том числе средств защиты информации.

Работы по модернизации информационной системы, в том числе по установке программного обеспечения и обновлений, должны проводиться в нерабочее время или время наименьшей рабочей нагрузки.

При выводе из эксплуатации информационных систем должно обеспечиваться гарантированное удаление обрабатываемой и хранимой в них информации с использованием средств гарантированного уничтожения информации или путем физического уничтожения носителей информации.

Все процедуры обеспечения защиты информации, установленные в Университете в отношении информационных систем, должны выполняться и контролироваться ответственными лицами за организацию работ по защите информации.

Контроль доступа к информационным ресурсам и системам

Все работники Университета, допущенные к работе с информационными ресурсами и информационными системами, несут персональную ответственность за нарушения установленного порядка обработки информации.

Уровень доступа и полномочий работника при работе с информационными ресурсами и информационными системами Университета должен определяться в соответствии с его должностными обязанностями. Руководитель структурного подразделения в соответствии с выполняемыми работником должностными обязанностями указывает требуемый уровень доступа к информационным ресурсам и полномочий в информационных системах.

Уровень доступа к информационным ресурсам и полномочий в информационных системах пользователей контролируется администратором информационных ресурсов и/или информационной системы.

Изменение уровня доступа и полномочий или прекращение доступа работника к информационными ресурсами и информационным системами Университета производится в случаях перевода на другую должность с изменением должностных обязанностей или увольнении.

Ответственные лица за организацию работ по защите информации должны регулярно проводить контроль выполнения организационно-распорядительных документов, касающихся регламентации допуска работников Университета к информационным системам. Осуществлять проверку блокировки доступа к информационным ресурсам и информационным системами Университета уволенных работников.

Идентификация и аутентификация

Доступ пользователей к информационным ресурсам и информационным системам Университета должен предоставляться только после успешного прохождения идентификации и аутентификации.

Создание учетной записи пользователя и получение имени и пароля для доступа к информационным ресурсам, а также имени и пароля для работы в информационной системе должно осуществляться по представлению руководителя структурного подразделения.

Управление доступом

Управление доступом должно осуществляться посредством набора процессов и технологий, направленных на контроль и управление тем, кто и каким образом имеет доступ к информационным ресурсам и информационным системам Университета.

Системы управления доступом могут быть:

- на основе ролей (RBAC) — права доступа определяются на основе ролей, которые исполняют пользователи;

- на основе атрибутов (ABAC) — доступ определяется на основе атрибутов пользователя, ресурса и окружающей среды;

- на основе списков контроля доступа (ACL) — доступ определяется на основе предварительно заданных списков, содержащих разрешения для пользователя или группы.

Для достижения оптимального уровня безопасности информации возможно комбинированное использование данных методов управления доступом.

Система управления доступом должна в том числе предусматривать возможность обеспечения защищённого удалённого доступа через внешние информационно-телекоммуникационные сети к информационным ресурсам и информационным системам Университета, т.к. Университет имеет распределённую территориально информационную инфраструктуру.

Безопасность при работе со съемными машинными носителями информации

Работники Университета допущенные в рамках выполнения своих должностных обязанностей к информационным ресурсам и информационным системам со служебной информацией ограниченного доступа и/или персональными данными, в своей работе должны использовать только учтенные съемные машинные носители информации.

Использование иных съемных машинных носителей информации в целях сбора, обработки, классификации, хранения и передачи служебной информацией ограниченного доступа и/или персональных данных в Университете строго запрещено.

Учтенные съемные машинные носители информации должны хранится в опечатываемых шкафах, в помещениях в которых предусмотрена обработка служебной информации ограниченного доступа и/или персональных данных.

В случае кражи или потери учтенного съемного машинного носителя информации, а также иных инцидентов, которые могут привести к нарушению свойств служебной информации ограниченного доступа и/или персональных данных, должны проводиться мероприятия по расследованию таких инцидентов.

При выводе из эксплуатации съемного машинного носителя информации, все данные, хранящиеся на нем, должны быть удалены определенной комиссией из числа работников, средством гарантированного уничтожения информации.

Факт уничтожения информации на съемном машинном носителе информации фиксируется в акте об уничтожении информации со съемного машинного носителя информации.

Регистрация событий

Все события безопасности на всех компонентах информационных ресурсов и информационных систем Университета должны регистрироваться встроенными или внешними средствами регистрации событий безопасности.

Средства регистрации событий безопасности должны предоставлять следующие возможности:

- включения и исключения событий безопасности в совокупность событий, подвергающихся регистрации;

- обеспечения непрерывности и невозможность остановки или блокировки процесса регистрации событий безопасности;

- обеспечения непрерывности процесса регистрации при превышении журналом регистрации определенного размера;

- предоставления регистрируемой информации в понятном и защищенном от несанкционированного доступа виде;

- выборочного просмотра, поиска, сортировки и упорядочения регистрируемой информации;

- изготовления соответствующих отчетов и др.

Антивирусная защита

В целях обнаружения и устранения вредоносных программ в Университете должны использоваться сертифицированные ФСТЭК России средства антивирусной защиты информации.

Обязательному и постоянному контролю средствами антивирусной защиты подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по локальной вычислительной сети и сетям общего пользования, полученная посредством электронной почты или иным способом, а также информация, хранимая и передаваемая на съемных машинных носителях информации.

При установке программного обеспечения или его обновления на средствах вычислительной техники, в том числе на северном оборудовании, должна автоматически выполняться предварительная проверка устанавливаемого программного обеспечения на отсутствие вредоносного программного обеспечения.

Обновление баз сигнатур для средства антивирусной защиты информации должно проводится ежедневно и только из проверенных источников распространения, указанных производителем средства антивирусной защиты.

Настройки безопасности средств антивирусной защиты должны блокировать доступ к конфигурации средств антивирусной защиты или возможности отключения Пользователем без прав администратора информационной системы.

Программное обеспечение

Выбор используемого системного, прикладного и специализированного программного обеспечения для установки на автоматизированные рабочие места и серверное оборудование информационных систем Университета должен производиться в приоритете к отечественным разработкам, внесенным в «Единый реестр российских программ для электронных вычислительных машин и баз данных». В случае отсутствия аналога системного и прикладного программного обеспечения в «Едином реестре российских программ для электронных вычислительных машин и баз данных» допускается использовать программного обеспечение импортного производства.

В целях исключения фактов нарушения безопасности информации путем эксплуатации уязвимостей программного обеспечения, используемого в информационных системах содержащих служебную информацию ограниченного доступа и/или персональные данные, следует использовать только прошедшее сертификацию и входящее в «Государственный реестр сертифицированных средств защиты информации» ФСТЭК России программное обеспечение.

Резервное копирование и восстановление данных

В целях недопущения потери критический важной информации и остановки работы информационных систем Университета в случаях, связанных с нарушением безопасности информации требуется иметь настроенную и работающую систему резервного копирования данных.

Резервное копирование данных должно осуществляться в автоматическом режиме с применением отечественного специализированного средства резервного копирования, входящего в «Государственный реестр сертифицированных средств защиты информации» ФСТЭК России и действующим сертификатом соответствия.

Резервное копирование должно осуществляться для:

- информации хранимой и обрабатываемой на файловом сервере и сервере приложений;
- файлов и данных информационной системы;
- рабочих мест администраторов информационной системы.

Частота и режим резервного копирования устанавливаются таким образом, чтобы обеспечить минимальную потерю данных и оперативное восстановление.

Настройка резервного копирования и восстановления ресурсов информационных систем Университета должны проводить уполномоченные работники.

Средства криптографической защиты информации

В случаях передачи служебной информации ограниченного доступа, в том числе персональных данных по открытым каналам связи, имеющим выход за пределы контролируемой зоны, должна быть организована защита от раскрытия, модификации и навязывания (ввода ложной информации), которая обеспечивается применением средств криптографической защиты информации.

Существующие информационные системы, в ходе эксплуатации которых выявилась необходимость передачи служебной информации ограниченного доступа, в том числе персональных данных по открытым каналам связи, имеющим выход за пределы контролируемой зоны, требуют доработки системы защиты информации. В имеющуюся систему защиты информации необходимо включить средства криптографической защиты информации.

У вновь разрабатываемых информационных систем на стадии формирования требований к системе защиты информации обязательно должен быть проработан вопрос о необходимости передачи служебной информации ограниченного доступа, в том числе персональных данных по открытым каналам связи, имеющим выход за пределы контролируемой зоны и необходимости включении в состав системы защиты информации средств криптографической защиты информации.

Используемые в составе информационных систем средства криптографической защиты информации должны входить в «Государственный реестр сертифицированных средств защиты информации» ФСТЭК России и поставляться для нужд Университета на основании договоров и контрактов с юридическими лицами имеющими действующую лицензию ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием

шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Электронная почта

Электронная почта используется в Университете с целью организации взаимодействия посредством электронных сообщений между работниками, обучающимися, контрагентами и органами государственной власти.

Сотрудники получают адрес служебной электронной почты в домене Университета – nsmu.ru. Использование в служебных целях других адресов электронной почты, зарегистрированных вне данного домена, запрещается,

При использовании служебной электронной почты запрещается:

- обмен информацией для служебного пользования, а также информацией ограниченного доступа, в том числе содержащей персональные данные;

- предоставление доступа к электронной почте с использованием данных своей учетной записи третьим лицам;

- публикация своего служебного адреса электронной почты в электронных каталогах, на поисковых машинах и других ресурсах сети Интернет в целях, не связанных с исполнением своих должностных обязанностей;

- подписка по электронной почте на различные рекламные материалы, листы рассылки, электронные журналы и т.д., не связанные с выполнением должностных обязанностей;

- открытие (запуск на выполнение) файлов, полученных по электронной почте без предварительной проверки их антивирусным программным обеспечением;

- рассылка по электронной почте различных рекламных материалов, электронных журналов, анкет и т.д., не связанных с выполнением должностных обязанностей.

Электронная подпись

В целях обеспечения идентичности и правомерного статуса электронных документов, подтверждения транзакций и цифровых сообщений, защиты передаваемой информации от фальсификаций в ходе электронного документооборота с контрагентами, организациями и учреждениями, а также органами государственной власти всех уровней, и

внутреннем электронном документообороте Университета, применяется электронная подпись.

Электронная подпись, в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», может выдаваться исключительно на ключевых носителях, которые, должны быть сертифицированы в соответствии с приказом ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра» и/или «Требованиями по безопасности информации, устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденными приказом ФСТЭК России от 02.06.2020 № 76.

Законодательством Российской Федерации предусмотрено и признается несколько видов электронных подписей:

простая – это последовательность символов, зашифрованная с помощью разных алгоритмов и защищенная паролем. Простая ЭЦП указывает на лицо, подписавшее документ, но не дает возможности определить неизменность подписи и подписанных данных. Она не предполагает использование сертификата ключа электронной подписи, что повышает вероятность её подделки.

неквалифицированная – электронная подпись, использующая сертификат ключа электронной подписи, ассоциируемая с владельцем и имеющая юридическую силу равную традиционной подписи. Она защищается специальным ключом и позволяет сохранить неизменность подписанной информации или обнаружить факт ее изменения.

квалифицированная – соответствует признакам неквалифицированной электронной подписи и при этом имеет специальный сертификат, выданный аккредитованным Удостоверяющим центром. Удостоверяющий центр в соответствии с законодательством Российской Федерации должен иметь лицензию ФСБ России осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание

шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) и пройти обязательную аккредитацию Минцифры.

Работники Университета использующие электронную подпись в рамках выполнения своих должностных обязанностей несут персональную ответственность за сохранность ключевого носителя и конфиденциальность личных ключей электронной подписи. Ключевые носители должны хранится в запираемых шкафах, ящиках или опечатываемых хранилищах, в помещениях в которых предусмотрено ограничение доступа посторонним лицам.

Запрещается передавать ключевой носитель и коды доступа к контейнеру с ключевой информацией третьим лицам.

В случае кражи или потери ключевого носителя, а также иных инцидентах, которые могут привести к компрометации электронной подписи, должны проводиться мероприятия по расследованию таких инцидентов и аннулированию электронной подписи работника.

Сертификаты ключей электронной подписи и ключевые носители с ними подлежат учету.

При окончании срока действия сертификатов ключей электронной подписи, с ключевого носителя все данные, хранящиеся на нем, должны быть удалены специальным программным обеспечением, применяемым для работы с электронной подписью. Факт записи и уничтожения информации на ключевой носитель фиксируется в журнале.

Работа в сетях общего пользования

Университет оставляет за собой право блокировать или ограничивать доступ работникам и студентам к сетям связи общего пользования, в том числе сети Интернет, и к размещённым в ней информационным ресурсам, содержание которых не имеет отношения к исполнению должностных обязанностей и программам обучения по специальности, а также к информационным ресурсам, содержание и направленность которых запрещены законодательством Российской Федерации.

Информация о посещаемых работниками и студентами Университета информационных ресурсах протоколируется для последующего анализа и, при необходимости, может быть представлена руководителям структурных подразделений

(кафедр) для контроля, а также по запросу может быть предоставлена правоохранительным органам.

При использовании сети Интернет запрещено:

- использовать предоставленный доступ в сеть Интернет в личных целях не связанных с выполнением должностных обязанностей или учебных целей;

- использовать несанкционированные программные и программно-аппаратные средства, позволяющие получить несанкционированный доступ к сети Интернет, а также фальсифицировать свой IP-адрес;

- публиковать, загружать и распространять материалы содержащие недостоверную информацию о деятельности Университета;

- публиковать, загружать и распространять материалы содержание и направленность которых запрещены законодательством Российской Федерации.

6. ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мониторинг информационной безопасности

На постоянной основе должен проводиться комплексный анализ функционирования информационных систем Университета и возникающих в них событий информационной безопасности.

Процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических мер по защите информации, анализ параметров конфигурации и настройки средств защиты информации.

При проведении контрольных мероприятий, связанных с оценкой реализации мер по защите информации в Университете, уполномоченные работники должны придерживаться следующих принципов:

- не нарушать функционирование и деятельность Университета;

- действовать в соответствии с утвержденными организационно-распорядительными документами по защите информации;

- не скрывать факты выявленных нарушений и событий информационной безопасности;

- оформлять отчеты, подтверждающие выполнение мероприятий по защите информации.

Информация, полученная в ходе проведения контролирующих мероприятий о действиях, событиях и параметрах, имеющих отношение к реализации мер по защите информации, должна консолидироваться и храниться в местах, исключающих получение к ней несанкционированного доступа.

Мониторинг данных о зарегистрированных событиях информационной безопасности должен проводиться, по возможности, с использованием системы мониторинга инцидентов информационной безопасности или встроенных механизмов настройки и аудита событий в программных и программно-аппаратных средствах, используемых в информационной инфраструктуре Университета.

Управление рисками

Определение внутренних требований по защите информации, должны основываться на результатах проведения анализа рисков нарушения основных свойств безопасности для информационных ресурсов Университета.

Основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения целостности, конфиденциальности и доступности информационных ресурсов.

Результатом проведения анализа рисков должен быть разработанный комплекс мер, направленных на снижение возможного негативного влияния на основную деятельность Университета при реализации той или иной угрозы безопасности информации и обеспечивающих в дальнейшем достаточный уровень защищенности информационных ресурсов и информационных систем.

Управление инцидентами информационной безопасности

Для обеспечения эффективного разрешения инцидентов информационной безопасности, минимизации потерь и уменьшения риска возникновения повторных инцидентов в Университете должно осуществляться управление инцидентами информационной безопасности.

Управление инцидентами информационной безопасности, может осуществлять специально созданная служба мониторинга и реагирования на инциденты информационной безопасности или назначенный ответственный сотрудник.

Задача управление инцидентами информационной безопасности решается посредством комплекса средств и мероприятий для сбора и консолидации информации об инцидентах. В отношении каждого вновь произошедшего инцидента должен выполняться

его анализ, и применение существующих или разработка новых эффективных мер реагирования на данный инцидент.

Аудит системы обеспечения информационной безопасности

В целях оценки текущего уровня информационной безопасности, в Университете на регулярной основе должен проводиться аудит информационной безопасности. Внутренний аудит информационной безопасности должен выполняться уполномоченными работниками Университета.

В ходе подготовки к внутреннему аудиту необходимо подготовить внутренний документ, в котором по шагам будет расписан весь процесс проверки: перечень информационных систем и процессов информационной безопасности, перечень организационно-распорядительных документов, содержание итоговых отчетов и расписание следующих аудитов.

В число задач, решаемых при проведении внутреннего аудита информационной безопасности, входят:

- сбор и анализ исходных данных об организационной и функциональной структуре информационных систем, необходимых для оценки состояния системы защиты информации;

- анализ утвержденных организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их доработке или разработки новых;

- обоснование финансовой эффективности вновь приобретаемых средств защиты информации;

- проверка правильности выбора и настройки средств защиты информации, формирование предложений по использованию имеющихся средств защиты информации для повышения уровня надёжности и безопасности информационных систем;

- анализ отчетов по произошедшим инцидентам информационной безопасности и принятым мерам по их разрешению

Кроме внутреннего аудита Университет может инициировать проведение внешнего аудита, который призван оценить состояние системы защиты информации, принятые меры по организации защиты информации и выявить возможные неучтенные риски и факторы, приводящие к инцидентам информационной безопасности.

Результат внешнего аудита должен быть оформлен в виде подробного отчета с информацией о защищенности информационной инфраструктуры, состоянии процессов информационной безопасности и соответствии (или несоответствии) требованиям.

Внешний аудит информационной безопасности Университета проводится на основании договора или контракта со сторонней организацией, имеющей действующую лицензию ФСТЭК на техническую защиту конфиденциальной информации.

Повышение осведомленности работников

Человеческий фактор является во многих случаях основной угрозой безопасности информации. В связи с чем в рамках организации комплексного противодействия угрозам безопасности информации должно постоянно проводится повышение осведомленности работников Университета в области защиты информации, в т.ч. об основных киберугрозах и их последствиях для Университета, правовых аспектах защиты информации, ответственности за нарушения законодательства Российской Федерации в области информационных технологий и защиты информации.

Повышение осведомленности работников осуществляется путем:

- проведения инструктажей по информации безопасности;
- ознакомления с существующими в Университете организационно-распорядительным документам по информационной безопасности;
- издания и доведения инструкций и методических материалов по использованию средств защиты информации и средств антивирусной защиты на рабочем месте;
- рассылки информационных материалов о новых видах киберугроз с указанием способов противодействия им;
- размещения на рабочих местах пользователей памятки по защите информации;
- проведения периодического тестирования знаний по безопасности информации.

7. ПОРЯДОК ПЕРЕСМОТРА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

При изменении действующего законодательства Российской Федерации в области защиты информации, а также организационно-распорядительных документов Университета, настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также внутренним документам.

Все требования, установленные действующим законодательством Российской Федерации, подзаконными актами и договорными отношениями, а также подход Университета к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.

Пересмотр и внесение изменений в настоящую Политику производится на периодической и внеплановой основе и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.

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

С момента утверждения изменённой и пересмотренной Политики руководителем, утрачивает силу предыдущая Политика информационной безопасности Университета.