МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

УТВЕРЖДАЮ
Ректор ФГБОУ ВО «ДГТУ»
к.э.н., доцент
_____ Н.Л. Баламирзоев
«__» _____ 2026г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФГБОУ ВО «Дагестанский государственный технический университет»

Утверждено на заседании
Ученого совета ФГБОУ ВО «ДГТУ»
протокол № 8 от «26» 02 2026 г.

Махачкала 2026 г.

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. Политика информационной безопасности Университета определяет:

- цели и задачи системы обеспечения информационной безопасности;

- основные принципы и общие требования по обеспечению информационной безопасности;

- организацию системы обеспечения информационной безопасности.

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;

- Федеральный закон от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».

- Постановление правительства РФ ОТ 1 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

- Приказ ФСТЭК России от 18 февраля 2013г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

- Приказ ФСБ России от 10 июля 2014г. N378 «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».

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.

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.

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).

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

АС - автоматизированная система;

АИС – автоматическая идентификационная 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

УИ – управление информатизации

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. Цель обеспечения ИБ – создание и постоянное соблюдение в Университете условий , при которых риски, связанные с нарушением безопасности информационных ресурсов Университета, постоянно контролируются и исключаются, любо находятся на допустимом уровне остаточного риска.

Процессы обеспечения информационной безопасности Университета являются составной и неотъемлемой частью процессов управления информационными технологиями и сопутствующими операционными рисками и осуществляются на основе циклической модели: «планирование – реализация – проверка – совершенствование – планирование - …»

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

Объектами защиты информации в Университете являются:

- информационные ресурсы, содержащие конфиденциальную информацию, информацию ограниченного распространения, включая персональные данные физических лиц, коммерческую тайну, а также открыто распространяемую информацию, необходимую для функционирования Университета, независимо от формы и вида ее представления;

- работники и контрагенты Университета, являющиеся пользователями автоматизированных систем;

- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникаций, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы

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 управлением информатизации (далее - УИ).

9. ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ 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;

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.

9.3. Требования по обеспечению информационной безопасности средствами антивирусной защиты:

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

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

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

9.4.1. 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.

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

9.4.3. Использование электронной почты для служебной переписки допускается только через корпоративные почтовые системы. Отправка и получение сообщений, содержащих конфиденциальную информацию, через личные почтовые ящики и сторонние почтовые сервисы запрещены.

9.4.4. Запрещается открывать вложения и переходить по ссылкам в электронных письмах, полученных от неизвестных отправителей, а также в подозрительных письмах, даже если они пришли от известного адресата (в случае компрометации учётной записи).

9.4.5. При использовании интернет-ресурсов не допускается посещение сайтов, содержание которых не связано с выполнением служебных обязанностей, особенно ресурсов, распространяющих вредоносное ПО, нарушающих авторские права или содержащих противоправную информацию.

9.4.6. Загрузка файлов из интернета (программ, документов, мультимедиа) разрешается только в случае служебной необходимости и при условии проверки загружаемых файлов антивирусными средствами.

9.4.7. Использование файлообменных сервисов и облачных хранилищ, не предоставленных Университетом, для хранения или передачи служебной информации допускается только с письменного разрешения руководителя подразделения и ответственного за ИБ, при условии применения шифрования и соблюдения требований законодательства о персональных данных.

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. При использовании в ФГБОУ ВО «ДГТУ» 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 системой обеспечения информационной безопасности осуществляет руководство Университета:

— утверждение и пересмотр политики информационной безопасности Университета;

— организация процесса управления информационной безопасностью в

Университете, включая определение подразделений, ответственных за управление отдельными процессами обеспечения информационной безопасности, утверждение положений о них;

— обеспечение условий и утверждение бюджета для эффективной реализации политики информационной безопасности;

— анализ отчетов о состоянии информационной безопасности Университета.

11.2. Все подразделения Университета и их руководители отвечают за реализацию политики информационной безопасности и управление процессами её обеспечения в рамках своей компетенции.

11.3. В целях выполнения задач по обеспечению информационной безопасности, в соответствии с рекомендациями международных и российских стандартов по безопасности, обеспечения деятельности по реализации текущей политики ИБ в Университете, в соответствии с его уставными целями, (назначается ответственное лицо или функционирует подразделение), ответственное за обеспечение информационной безопасности — подразделение или ответственное лицо.

11.4 Подразделение или ответственное лицо:

— разрабатывает нормативные, инструктивные и методические документы

Университета по обеспечению информационной безопасности;

— разрабатывает требования по защите информационных ресурсов в аспектах целостности и конфиденциальности на основе анализа рисков информационной безопасности;

— осуществляет контроль соответствия требованиям на всех стадиях жизненного цикла автоматизированных систем, от проектирования до снятия с эксплуатации;

— Обеспечивает управление ключевыми системами средств криптографической защиты;

— организует проведение единой антивирусной политики в Университете;

— организует работу и осуществляет взаимодействие с администраторами

автоматизированных информационных систем;

— проводит расследования инцидентов и фактов нарушений информационной безопасности и информирует руководство о результатах проведенного расследования;

— организует обучение персонала по вопросам информационной безопасности;

— осуществляет инструментальный контроль и мониторинг текущего состояния информационной безопасности;

— регулярно информирует руководство о состоянии информационной безопасности в Университете, в том числе, в составе сводных отчетов;

— Обеспечивает взаимодействие с уполномоченными государственными: органами по вопросам информационной безопасности;

— осуществляет анализ, оценку и прогноз риска, связанного с нарушением

информационной безопасности Университета.

11.5. Обеспечение разработки, актуализации и доведения до сведения работников локальных нормативных и методических документов, детализирующих требования настоящей Политики, включая:

- инструкцию по антивирусной защите;

- регламент резервного копирования и восстановления данных;

- порядок предоставления доступа к информационным системам;

- инструкцию по действиям при инцидентах ИБ;

- правила работы с персональными данными;

- памятку пользователю по безопасной работе.

Указанные документы должны быть утверждены в установленном порядке и пересматриваться по мере необходимости, но не реже одного раза в три года.

11.6. Подразделения, ответственные за обслуживание АИС, или администраторы АИС:

— обеспечивают выполнение требований информационной безопасности при

подключении и администрировании коммуникационного оборудования, операционных систем, СУБД и систем доставки;

— проводят обновление системного ПО, связанное с устранением критичных

уязвимостей; обеспечивают доступность информационных ресурсов в условиях отказов и других неблагоприятных событий в части

коммуникационного оборудования, операционных систем, СУБД и систем доставки;

— обеспечивает выполнение требований информационной безопасности при

администрировании автоматизированных информационных систем; обеспечивают хранение программной документации;

— осуществляют регистрацию информации об инцидентах, имеющих отношение к информационной безопасности.

— совместно с (подразделение, должностное лицо, ответственное за

информационную безопасность) проводят категорирование информационных ресурсов, владельцами, которых они являются, и определяют те из них, которые являются критичными;

— совместно с (подразделение, должностное лицо, ответственное за информационную безопасность) участвуют в оценке рисков реализации угроз их информационным ресурсам;

— устанавливают в пределах своей компетенции режим и порядок доступа, правила работы с информационными ресурсами, владельцами которых они являются;

— обеспечивают выполнение требований и процедур информационной безопасности при работе работников с информационными ресурсами Университета;

— Обеспечивают учет в подразделении информационных ресурсов и работников, имеющих к ним доступ;

— Обеспечивают инструктаж работников по вопросам информационной

безопасности;

— обеспечивают контроль проведения антивирусных мероприятий в подразделении и соблюдения требований информационной безопасности;

— обеспечивают взаимодействие с (подразделение, должностное лицо ответственное за информационную безопасность) при инцидентах информационной безопасности.

12. АУДИТ И САМООЦЕНКА ИБ

12.1 Порядок и периодичность проведения аудита ИБ Университета, а также

отдельных его структурных подразделений, определяется подразделением, ответственным за обеспечение ИБ на основании потребности в такой деятельности.

12.2 Внешний аудит ИБ проводится независимыми организациями (индивидуальными предпринимателями), имеющими право на

осуществление такой деятельности, с целью проверки и оценки соответствия ИБ Университета требованиям действующего законодательства Российской Федерации в области информационной безопасности, Внешний аудит ИБ проводится на основании приказа ректора Университета,

12.3 Самооценка уровня ИБ и внутренний контроль соблюдения требований ИБ проводится подразделением, ответственным за обеспечение ИБ с целью выявления и регистрации недостатков защитных мер и оценки полноты реализации положений текущей политики ИБ, инструкций и руководств по обеспечению ИБ Университета. Самооценка уровня ИБ и внутренний контроль проводится по распоряжению ректора Университета

12.4 При подготовке к вешнему аудиту ИБ рекомендуется проведение самооценки ИБ.

12.5. В целях оценки эффективности функционирования системы обеспечения информационной безопасности используются следующие метрики (показатели):

- количество зарегистрированных инцидентов за отчётный период (в динамике);

- среднее время реагирования на инциденты;

- доля критичных уязвимостей, устранённых в установленный срок;

- процент сотрудников, прошедших обучение по ИБ;

- количество успешных тестовых восстановлений из резервных копий;

- результаты внутренних аудитов и самооценок.

Анализ метрик проводится ежеквартально, результаты докладываются руководству Университета для принятия управленческих решений.

13. ПОРЯДОК ПЕРЕСМОТРА ПОЛИТИКИ

13.1. Пересмотри Политики производится не реже одного раза в три года для изменения, корректировки, либо отклонения, поставленных целей, задач и основных принципов информационной безопасности Университете.

13.2. Пересмотр Политики осуществляется специально назначаемой для этой цели комиссией по защите информации или рабочей группой пересмотру Политики.

13.3. Пересмотри Политики должен включать:

- проверку эффективности Политики, исходя из характера, числа и последствий зарегистрированных инцидентов нарушений ИБ;

- определений стоимости мероприятий по управлению информационной безопасностью и их влияние на эффективность по достижению уставных целей Университета;

- оценку влияния изменений в технологиях.

14. ОТВЕТСТВЕННОСТЬ

14.1. Все работники Университета несут ответственность за невыполнение требований настоящей политики.

14.2. Работники Университета, нарушающие требования информационной

безопасности и руководители подразделений, не обеспечивающие их выполнение, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

14.3. Контроль за выполнением требований настоящей политики возлагается на руководство Университета, руководителей всех структурных подразделений Университета.

15. УПРАВЛЕНИЕ ДОСТУПОМ И ИДЕНТИФИКАЦИЕЙ

15.1. Доступ пользователей к информационным ресурсам Университета предоставляется только после прохождения процедур идентификации, аутентификации и авторизации.

15.2. Идентификация и аутентификация осуществляются с использованием уникальных учётных записей. Запрещается использование групповых учётных записей, за исключением специально оговорённых случаев (гостевой доступ, служебные учётные записи), которые должны быть документально зафиксированы и контролироваться.

15.3. Парольная политика устанавливает следующие требования:

- длина пароля не менее 8 символов;

- пароль должен содержать символы как минимум трёх из четырёх категорий: строчные буквы, прописные буквы, цифры, специальные символы;

- смена пароля не реже одного раза в 90 дней;

- запрет на использование предыдущих паролей (не менее 3 последних значений);

- блокировка учётной записи после 5 неудачных попыток входа на время не менее 15 минут;

- обязательная смена пароля при первом входе в систему.

15.4. Передача паролей другим лицам, запись паролей на бумажных носителях, размещённых на рабочем месте, использование одинаковых паролей для служебных и личных ресурсов запрещаются.

15.5. При увольнении сотрудника или изменении его должностных обязанностей доступ к информационным ресурсам должен быть заблокирован или изменён в день наступления соответствующего события. Руководители подразделений обязаны своевременно информировать администраторов информационных систем и ответственных за ИБ о необходимости изменения прав доступа.

15.6. Для привилегированных учётных записей (администраторов, суперпользователей) применяются дополнительные меры контроля: двухфакторная аутентификация, выделенные рабочие станции, аудит всех действий.

15.7. На всех автоматизированных рабочих местах должна быть настроена автоматическая блокировка экрана при отсутствии активности пользователя в течение не более 15 минут. Разблокировка возможна только после повторного ввода пароля.

16. ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ПЕРИМЕТРА

16.1. Серверные помещения, узлы связи, кроссовые и другие помещения, где размещено критическое телекоммуникационное оборудование и носители информации, должны быть оборудованы системами контроля доступа (электронные замки, считыватели, кодовые панели) и видеонаблюдения.

16.2. Доступ в указанные помещения разрешён только сотрудникам, в должностные обязанности которых входит обслуживание размещённого там оборудования, на основании утверждённых списков. Посещение иными лицами допускается только в сопровождении ответственного сотрудника и с обязательной регистрацией в журнале учёта посещений.

16.3. Рабочие места сотрудников должны располагаться таким образом, чтобы исключить возможность визуального ознакомления посторонних лиц с информацией, отображаемой на экранах мониторов, а также с документами на столах.

16.4. Внос и вынос оборудования, съёмных носителей информации за пределы контролируемой территории Университета должен осуществляться по письменному разрешению руководителя подразделения и фиксироваться в соответствующих учётных формах.

16.5. По окончании рабочего дня сотрудники обязаны запирать шкафы и сейфы с документами, а также обеспечивать отключение оргтехники, если это не противоречит технологическому процессу.

16.6. Помещения, в которых обрабатываются персональные данные и конфиденциальная информация, должны быть оснащены замками, исключающими несанкционированное проникновение, и находиться под охраной в нерабочее время.

17. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

17.1. Под инцидентом информационной безопасности понимается любое событие, которое может привести к нарушению конфиденциальности, целостности или доступности информационных активов Университета, либо к несоблюдению требований законодательства и внутренних нормативных документов.

17.2. Все сотрудники Университета обязаны незамедлительно сообщать о замеченных фактах или подозрениях на инциденты информационной безопасности лицу, ответственному за обеспечение ИБ, или своему непосредственному руководителю.

17.3. Порядок реагирования на инциденты включает следующие этапы:

- регистрация инцидента (дата, время, обстоятельства, заявитель);

- первичная оценка критичности и принятие мер по локализации и минимизации ущерба;

- расследование причин и обстоятельств инцидента;

- устранение последствий и восстановление штатного режима работы;

- анализ инцидента, разработка и реализация мер по предотвращению повторения.

17.4. Для каждого инцидента, связанного с нарушением безопасности персональных данных, должно быть организовано взаимодействие с уполномоченными органами в порядке, установленном законодательством Российской Федерации.

17.5. Информация обо всех инцидентах фиксируется в журнале учёта инцидентов, ведение которого возлагается на подразделение (лицо), ответственное за информационную безопасность. На основе накопленных данных не реже одного раза в квартал проводится анализ динамики и эффективности принятых мер.

18. ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ ДЕЯТЕЛЬНОСТИ И ВОССТАНОВЛЕНИЕ ПОСЛЕ СБОЕВ

18.1. В Университете должны быть определены критически важные информационные процессы и ресурсы, нарушение функционирования которых может привести к значительному ущербу или остановке

деятельности. Для них разрабатываются планы обеспечения непрерывности и восстановления.

18.2. Обязательным требованием является организация резервного копирования данных, содержащихся на серверах, в базах данных и на рабочих станциях, где хранится критическая информация.

18.3. Резервное копирование должно выполняться с установленной периодичностью:

- для критичных систем – ежедневно;

- для прочих информационных систем – не реже одного раза в неделю.

18.4. Резервные копии должны храниться как локально (для оперативного восстановления), так и на удалённых (внеплощадочных) носителях, защищённых от несанкционированного доступа и воздействия факторов, способных повредить оригиналы.

18.5. Не реже одного раза в полгода должно проводиться тестирование восстановления из резервных копий для подтверждения их работоспособности и целостности данных. Результаты тестирования оформляются актом.

18.6. В случае возникновения аварийных ситуаций (пожар, затопление, отключение электроэнергии, аппаратные сбои и т.п.) сотрудники обязаны действовать в соответствии с утверждёнными инструкциями по действиям в нештатных ситуациях, которые должны находиться на каждом рабочем месте.

19. УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И УЯЗВИМОСТЯМИ

19.1. Все изменения в программном и аппаратном обеспечении, а также в конфигурации информационных систем должны производиться только после согласования с подразделением (лицом), ответственным за информационную безопасность, и документироваться.

19.2. Изменения, способные повлиять на уровень защищенности (установка обновлений, смена настроек доступа, подключение нового оборудования и т.п.), должны быть протестированы в тестовой среде, если это технически возможно, перед внедрением в продуктивную среду.

19.3. С целью своевременного устранения уязвимостей в Университете организуется мониторинг обновлений безопасности для используемого системного и прикладного программного обеспечения. Критичные обновления, устраняющие уязвимости с высоким уровнем риска, должны устанавливаться в кратчайшие сроки (не более 3 рабочих дней) после выхода.

19.4. Периодически (не реже одного раза в квартал) должно проводиться сканирование информационных систем на наличие известных уязвимостей с использованием специализированных средств. Результаты сканирования

анализируются, и по ним разрабатывается план устранения выявленных недостатков.

19.5. Запрещается использование нелицензионного или неподдерживаемого (снятого с сопровождения) программного обеспечения, поскольку оно может содержать неустранимые уязвимости.

20. ВЗАИМОДЕЙСТВИЕ С ТРЕТЬИМИ СТОРОНАМИ

20.1. Привлечение сторонних организаций (подрядчиков, консультантов, аутсорсеров) для выполнения работ, связанных с доступом к информационным ресурсам Университета или их обработкой, допускается только при наличии в договоре (контракте) условий, обязывающих третью сторону соблюдать требования информационной безопасности не ниже установленных в Университете.

20.2. В договорах должны быть оговорены:

- обязательства по сохранению конфиденциальности полученной информации;

- перечень разрешённых действий с информацией;

- порядок уведомления об инцидентах;

- ответственность за нарушение требований безопасности;

- право Университета на проведение проверок соблюдения условий договора в части ИБ.

20.3. При использовании облачных сервисов и внешних хранилищ данных необходимо убедиться в соответствии провайдера требованиям законодательства о персональных данных (в частности, о хранении персональных данных граждан РФ на территории РФ) и наличии у него необходимых лицензий и сертификатов.

20.4. Доступ сторонних специалистов к информационным системам Университета должен предоставляться на минимально необходимый срок и объём, строго в рамках выполняемых работ, с обязательным контролем со стороны ответственного сотрудника Университета.

20.5. Передача информации, содержащей персональные данные или коммерческую тайну, третьим лицам осуществляется только при наличии согласия субъектов персональных данных (если это требуется по закону) и с разрешения руководства Университета.

21. ПРАВИЛА ИСПОЛЬЗОВАНИЯ МОБИЛЬНЫХ УСТРОЙСТВ И УДАЛЁННОЙ РАБОТЫ

21.1. Использование личных мобильных устройств (ноутбуков, планшетов, смартфонов) для выполнения служебных задач допускается только с

разрешения руководителя подразделения и после установки на них необходимых средств защиты (антивирус, шифрование, VPN-клиент) и проведения инструктажа.

21.2. При удалённом доступе к информационным ресурсам Университета обязательно использование защищённых каналов связи (VPN) с аутентификацией.

21.3. На мобильных устройствах, используемых в служебных целях, должно быть настроено:

- блокировка экрана паролем или биометрией;

- шифрование данных устройства (если поддерживается);

- удалённое управление (возможность очистки данных при утере или краже).

21.4. Запрещается хранение на мобильных устройствах нешифрованных копий документов, содержащих персональные данные или иную конфиденциальную информацию, а также передача таких данных через незащищённые каналы связи (мессенджеры, открытая электронная почта).

21.5. При утере или краже мобильного устройства, содержащего служебную информацию, сотрудник обязан немедленно сообщить об этом ответственному за ИБ и руководителю для принятия мер по блокировке доступа и удалению данных.

22. ОБУЧЕНИЕ И ПОВЫШЕНИЕ ОСВЕДОМЛЁННОСТИ ПЕРСОНАЛА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

22.1. Все сотрудники Университета при приёме на работу должны быть ознакомлены с настоящей Политикой и другими нормативными документами по информационной безопасности под роспись.

22.2. Вновь принятые сотрудники, а также сотрудники, меняющие должностные обязанности, связанные с доступом к информационным системам, обязаны пройти вводный инструктаж по информационной безопасности у ответственного лица.

22.3. Не реже одного раза в год для всех сотрудников должно проводиться периодическое обучение (в форме лекций, семинаров, рассылки информационных материалов) по актуальным угрозам и правилам безопасной работы.

22.4. Для сотрудников, имеющих доступ к персональным данным, а также для администраторов информационных систем, организуются специализированные тренинги с учётом специфики их работы и требований законодательства.

22.5. Проверка знаний требований информационной безопасности может проводиться в форме тестирования или собеседования. Результаты проверок учитываются при аттестации сотрудников.

22.6. Руководители подразделений несут ответственность за своевременное доведение до подчинённых изменений в политиках и процедурах ИБ.

23. УПРАВЛЕНИЕ АКТИВАМИ И КЛАССИФИКАЦИЯ ИНФОРМАЦИИ

23.1. Все информационные активы Университета (оборудование, программное обеспечение, базы данных, документы, съёмные носители) подлежат инвентаризации. Ответственность за ведение реестра активов возлагается на подразделение (лицо), ответственное за ИБ, совместно с владельцами активов.

23.2. Для каждого актива должны быть определены:

- владелец (ответственный за сохранность и правильное использование);

- категория конфиденциальности;

- требования по защите (доступность, целостность, конфиденциальность);

- срок хранения и порядок уничтожения.

23.3. Информация, обрабатываемая в Университете, подразделяется на следующие категории:

Общедоступная информация – не требует специальных мер защиты.

Информация для служебного пользования – доступна только сотрудникам Университета в рамках выполнения должностных обязанностей.

Конфиденциальная информация – включает персональные данные, коммерческую тайну, служебную тайну. Доступ строго ограничен, требуется применение организационных и технических мер защиты.

Секретная информация – при наличии государственной тайны (обрабатывается в соответствии с законодательством о государственной тайне).

23.4. Все носители информации (бумажные, электронные) должны иметь соответствующую маркировку, указывающую на категорию конфиденциальности.

23.5. При выводе из эксплуатации оборудования или носителей, содержащих конфиденциальную информацию, должно проводиться их гарантированное уничтожение (физическое разрушение или программное затирание) с составлением акта.

24. СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

24.1. Деятельность Университета по обработке информации должна соответствовать требованиям законодательства Российской Федерации, в том числе в области персональных данных, коммерческой тайны, электронной подписи, авторских прав.

24.2. Регулярно (не реже одного раза в год) проводится анализ изменений законодательства и оценка их влияния на действующую систему обеспечения информационной безопасности. По результатам вносятся необходимые коррективы в локальные нормативные акты.

24.3. Лица, ответственные за обработку персональных данных, обязаны обеспечивать выполнение требований Федерального закона № 152-ФЗ, включая получение согласий субъектов, уведомление Роскомнадзора (при необходимости), организацию взаимодействия с субъектами по вопросам обработки их данных.

24.4. Использование программного обеспечения должно осуществляться исключительно на законных основаниях (лицензионное ПО, свободное ПО с соблюдением условий лицензий). Контроль за соблюдением авторских прав возлагается на руководителей подразделений и администраторов информационных систем.

24.5. Внутренние проверки соблюдения требований проводятся в рамках аудита и самооценки (раздел 12 настоящей Политики). По выявленным несоответствиям разрабатываются корректирующие мероприятия.

25. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

25.1. Для обеспечения конфиденциальности и целостности информации при её передаче по каналам связи, а также при хранении на съёмных носителях, применяются сертифицированные средства криптографической защиты информации (СКЗИ) в соответствии с требованиями ФСБ России.

25.2. Использование криптографии обязательно в следующих случаях:

- передача персональных данных и конфиденциальной информации по открытым каналам связи (включая Интернет);

- организация удалённого доступа к информационным ресурсам Университета (VPN);

- создание электронной подписи при юридически значимом документообороте;

- хранение резервных копий, содержащих конфиденциальную информацию, на внешних носителях.

25.3. Применение СКЗИ должно осуществляться в соответствии с эксплуатационной документацией. Запрещается вносить изменения в

настройки СКЗИ, не предусмотренные документацией, или использовать средства, не прошедшие сертификацию.

25.4. Управление ключевыми носителями (генерация, хранение, замена, уничтожение ключей) осуществляется лицами, ответственными за криптографическую защиту, с соблюдением мер, исключающих компрометацию ключей.

25.5. Компрометация ключей (утрата носителей, подозрение на копирование и т.п.) должна быть немедленно зафиксирована, после чего производится замена ключей и, при необходимости, информирование взаимодействующих сторон.

26. ПРАВИЛА ЧИСТОГО СТОЛА И ЧИСТОГО ЭКРАНА

26.1. В конце рабочего дня сотрудники обязаны убирать со столов все документы, съёмные носители и другие материалы, содержащие конфиденциальную информацию, в запираемые шкафы или сейфы.

26.2. На рабочих столах не допускается оставление без присмотра документов, содержащих персональные данные или иную ограниченную информацию.

26.3. При временном отсутствии на рабочем месте (перерыв, совещание и т.п.) сотрудник обязан заблокировать компьютер (перевести в режим ожидания или заблокировать экран) с использованием пароля или иных средств аутентификации.

26.4. Запрещается оставлять открытыми на экране монитора документы, содержащие конфиденциальную информацию, если за монитором никто не наблюдает.

26.5. Печатные устройства (принтеры, МФУ) должны размещаться таким образом, чтобы исключить доступ посторонних лиц к выведенным на печать документам.

Согласовано:

Проректор по ЦТиИБ	Р.Г. Махмудов
Проректор по НиИД	Ш.А. Юсуфов
Проректор по УР	А.Ф. Демирова
Проректор по ВиСР	Р.К. Ашуралиева

Начальник УИ	Н.М. Джанатлиев
Начальник отдела ИБ	Ш.М. Абдуллаев
Начальник ЮО	М.Н. Гарунова
Начальник ОК	З.Г. Керимова