Утверждаю
Ректор
_____ Н.Л. Баламирзоев
«31» 05 2024 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Федерального государственного бюджетного
образовательного учреждения высшего образования
"Дагестанский Государственный Технический Университет"

Дата введения: _____

Махачкала 2024

1. Рассмотрено на заседании Ученого совета, протокол № __ от «__» _____ 2024 г.
2. Утверждено и введено в действие приказом Ректора, № __ от «__» _____ 2024 г.
3. Соответствует требованиям ДГТУ

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. № 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».

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 взаимосвязанных 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 внештатной 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, либо 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 «Модель угроз безопасности персональных данных при их обработке в ИСПДн», 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.

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. № 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. 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;

— обеспечивают 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 отделом ИБ проводят категорирование информационных ресурсов, владельцами, которых они являются, и определяют те из них, которые являются критичными;

— совместно с отделом ИБ 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 соблюдение требований информационной безопасности;

— обеспечивают взаимодействие с отделом ИБ 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.

13. ПОРЯДОК ПЕРЕСМОТРА ПОЛИТИКИ

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

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

13.3. Пересмотр Политики должен включать:

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

СОГЛАСОВАНО:

Проректор по ЭиАД	М.С. Алибеков
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 ОК	А.Э. Магомедрагимова
Начальник ЮО	М.Н. Гарунова
Начальник отдела ИБ	К.М. Шахбанов