

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 1 из 33
--	--	------------

СТАНДАРТ ОРГАНИЗАЦИИ

**Система менеджмента качества
ПОЛИТИКА ПО ЗАЩИТЕ ИНФОРМАЦИИ**

**СТО С.001-2025
Второе издание**




УТВЕРЖДАЮ
И.о. ректора университета
Я.Ю. Григорьев
«31» 10 2025 г.



Комсомольск-на-Амуре
2025

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 2 из 33
--	---	------------

Лист согласования

Должность	Ф.И.О.	Подпись	Дата ознакомления
Начальник ИТУ	Е.Б. Абарникова		30.10.2025
Начальник ПУ	А.В. Ременников		31.10.2025
Начальник УКД	М.А. Корякина		31.10.2025

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 3 из 33
--	--	------------

Содержание

1 Назначение и область применения.....	4
2 Нормативные ссылки.....	4
3 Термины, определения, сокращения.....	7
4 Ответственность.....	10
5 Цели, задачи и мероприятия обеспечения информационной безопасности.....	10
6 Категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия (права).....	13
7 Организация системы обеспечения информационной безопасности.....	15
8 Основные принципы обеспечения информационной безопасности.....	17
9 Категории информации и информационных систем.....	18
10 Политика информационной безопасности при использовании автоматизированного рабочего места.....	19
11 Политика информационной безопасности при использовании электронной почты и Интернет.....	20
12 Политика противодействия несанкционированному доступу.....	21
13 Политика управления доступом.....	21
14 Парольная политика.....	22
15 Политика сетевой защиты информации.....	24
16 Антивирусная политика.....	25
17 Политика использования средств криптографической защиты информации и электронной подписи.....	26
18 Политика информационной безопасности на этапах жизненного цикла информационной системы.....	27
19 Политика резервного копирования.....	27
20 Политика управления рисками информационной безопасности.....	28
21 Политика управления уязвимостями.....	29
22 Политика управления инцидентами.....	30
23 Политика повышения осведомленности сотрудников в области информационной безопасности.....	30
24 Разработчик.....	32
Лист регистрации изменений.....	33

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 4 из 33
--	---	------------

1 Назначение и область применения

1.1 Назначение

Настоящий документ описывает политику по защите информации в ФГБОУ ВО «КНАГУ».

Целью разработки данного стандарта является закрепление подходов к функционированию и совершенствованию системы обеспечения информационной безопасности в ФГБОУ ВО «КНАГУ» (далее – университет) и определяет:

- цели и задачи системы обеспечения информационной безопасности;
- основные принципы и общие требования по обеспечению информационной безопасности;
- организацию системы обеспечения информационной безопасности;
- категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия (права).

1.2 Область применения

Требования настоящего стандарта распространяются на:

- информационные системы университета, включая программные и программно-аппаратные средства, информационные ресурсы и информацию, обрабатываемую в университете, за исключением сведений, составляющих государственную тайну;
- информационно-технологическую инфраструктуру университета, включая сервисы, телекоммуникационное оборудование и каналы связи, обеспечивающие передачу информации между информационными системами и информационное взаимодействие участников информационного обмена;
- системы и подсистемы защиты информации университета, обеспечивающие реализацию и контроль мер информационной безопасности;
- персонал университета, участвующий в процессах сбора, накопления, систематизации, обработки, передачи, хранения и защиты информации.

2 Нормативные ссылки

Настоящий стандарт разработан в соответствии со следующими документами:

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 5 из 33
--	--	------------

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

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

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06 марта 1997 г. № 188.

Указ Президента РФ «О стратегии национальной безопасности Российской Федерации» от 02 июля 2021 г. № 400.

Указ Президента РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» от 30 марта 2022 г. № 166.

Указ Президента РФ «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» от 01 мая 2022 г. № 250.

Указ Президента РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» от 30 марта 2022 г. № 166.

Постановление Правительства РФ «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средства автоматизации» от 15 сентября 2008 г. № 687.

Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01 ноября 2012 г. № 1119.

Постановление Правительства РФ «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» от 08 февраля 2018 г. № 127.

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

Приказ ФСТЭК РФ «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» от 21 декабря 2017 г. № 235.

Приказ ФСТЭК РФ «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 6 из 33
--	--	------------

необходимости присвоения ему одной из таких категорий» от 22 декабря 2017 г. № 236.

Приказ ФСТЭК РФ «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25 декабря 2017 г. № 239.

Приказ ФСТЭК РФ «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» от 02 июня 2020 г. № 76.

Приказ ФСТЭК РФ «Об утверждении требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»» от 27 октября 2022 г. № 178.

Приказ ФСТЭК РФ «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» от 11 апреля 2025 г. № 117.

Приказ ФСБ РФ «Об утверждении Составы 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» от 10 июля 2014 г. № 378.

Приказ ФСБ РФ «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» от 19 июня 2019 г. № 282.

Приказ ФСБ РФ «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных» от 13 февраля 2023 г. № 77.

Приказ ФСБ РФ «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, гос-

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 7 из 33
--	--	------------

ударственных унитарных предприятий, государственных учреждений с использованием шифровальных (криптографических) средств» от 18 марта 2025 г. № 117.

Руководящий документ, утверждённый решением председателя государственной технической комиссии при Президенте РФ от 30.03.1992 «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Методический документ ФСТЭК РФ от 05.02.2021 «Методика оценки угроз безопасности информации».

Методический документ ФСТЭК РФ от 28.10.2022 «Методика тестирования обновлений безопасности программных, программно-аппаратных средств».

Методический документ ФСТЭК РФ от 17.05.2023 «Руководство по организации процесса управления уязвимостями в органе (организации)».

Методический документ ФСТЭК РФ от 30.06.2025 «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств».

3 Термины, определения, сокращения

3.1 Термины и определения

В настоящем стандарте применяются следующие термины с соответствующими определениями:

Автоматизированное рабочее место – рабочее место специалиста, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования.

Владелец информационного актива – подразделение университета, в лице его руководителя, наделенное полномочиями владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами.

Данные – информация, представленная в электронной форме.

Демилитаризованная зона – участок корпоративной сети, расположенный между внешним межсетевым экраном и внешним маршрутизатором, используемым для подключения корпоративной сети к сети провайдеров Интернет.

Доступность – обеспечение возможности легитимным пользователям за приемлемое время получать требуемую информационную услугу.

Доступ к информации – возможность получения информации и ее использования.

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 8 из 33
--	--	------------

Защита информации – это комплекс мер, направленных на обеспечение конфиденциальности, целостности и доступности информации.

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

Идентификация риска – процесс выявления и классификации рисков.

Информационная безопасность – состояние и режим эксплуатации средств хранения, доставки и автоматизированной обработки, при котором обеспечивается уровень защиты информационных ресурсов, достаточный для минимизации ущерба, вызванного возможными нарушениями безопасности.

Информационный актив – информационные системы и информационные ресурсы университета, осуществляющие обработку информации автоматизированными и не автоматизированными средствами и имеющие ценность для университета.

Информационный ресурс – различная информация университета, используемая в деятельности университета.

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

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

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Инцидент информационной безопасности – это непредвиденное или нежелательное событие, которое нарушает безопасность информации – ее конфиденциальность, целостность и доступность.

Конфиденциальность – обеспечение доступности информации только ограниченному кругу лиц, имеющих соответствующие полномочия.

Критичный информационный ресурс (критичная информация) – информация, создание, модификация и обработка которой связаны с повышенным риском информационной безопасности.

Критичные уязвимости – недостатки и ошибки системного и прикладного программного обеспечения на всех уровнях архитектуры автоматизированных информационных систем, создающие повышенные риски информационной безопасности критичным информационным ресурсам.

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 9 из 33
--	--	------------

Корпоративная сеть – объединение информационных активов, компьютерного, телекоммуникационного и офисного оборудования всех структурных подразделений университета, посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Операционный риск – риск, возникающий в результате недостатков в организации деятельности университета, используемых технологиях, функционировании информационных систем, неадекватных действий или ошибок сотрудников, а также в результате внешних событий.

Оценка риска – оценка вероятности реализации риска и величины возможных потерь при реализации конкретного вида риска и/или совокупных рисков, принимаемых на себя университетом.

Риск – возможность возникновения у университета потерь (убытков), незапланированных расходов или возможность снижения планируемых доходов.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Руководство – ректорат университета.

Система обеспечения информационной безопасности – часть общей системы управления университета, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности университета. Включает структуру, политики, совокупность мероприятий, методов и средств, обеспечивающих требуемый уровень безопасности информационных ресурсов участниками соответствующих процессов.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Угроза информационной безопасности – внешний или внутренний фактор, создающий риск информационной безопасности.

Уязвимость – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы информационной безопасности.

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 10 из 33
--	--	-------------

Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

3.2 Сокращения

В настоящем стандарте применяются следующие сокращения:

АРМ – автоматизированное рабочее место;

ГИС – государственная информационная система и иные информационные системы государственных учреждений;

ДМЗ – демилитаризованная зона;

ИТ – информационные технологии;

ИС – информационные системы;

ИБ – информационная безопасность;

ИСПДн – информационная система персональных данных;

НСД – несанкционированный доступ;

ОС – операционная система;

ПДн – персональные данные;

ПО – программное обеспечение;

СЗИ – средства защиты информации;

СКЗИ – средства криптографической защиты информации;

СУБД – система управления базами данных;

ЭП – электронная подпись;

ПЭП – простая электронная подпись;

НЭП – усиленная неквалифицированная электронная подпись;

КЭП – усиленная квалифицированная электронная подпись.

4 Ответственность

4.1 Все сотрудники университета несут ответственность за выполнение требований настоящей политики.

4.2 Сотрудники 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.

4.3 Контроль за выполнением требований настоящей политики возлагается на руководство университета и руководителей всех структурных подразделений университета.

5 Цели, задачи и мероприятия обеспечения информационной безопасности

5.1 Основными целями защиты информации являются:

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 11 из 33
--	--	-------------

- недопущение (исключение, снижение возможности) наступления негативных последствий (событий) от нарушения конфиденциальности, целостности, доступности информации;

- недопущение (исключение, снижение возможности) наступления негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации.

5.2 Мероприятия и меры по защите информации должны быть направлены на решение следующих задач:

- исключение утечки информации ограниченного доступа и иной конфиденциальной информации;

- предотвращение несанкционированного доступа к информационным активам и содержащейся в них информации, обнаружение фактов несанкционированного доступа и реагирование на них;

- предотвращение несанкционированной модификации информации, обнаружение фактов несанкционированной модификации и реагирование на них;

- предотвращение несанкционированной подмены информации, обнаружение фактов несанкционированной подмены и реагирование на них;

- предотвращение несанкционированного удаления информации и программного обеспечения, обнаружение фактов несанкционированного удаления и реагирование на них;

- исключение или существенное затруднение отказа в обслуживании авторизованным пользователям информационных активов;

- недопущение использования информационных активов и содержащейся в них информации не по назначению;

- исключение или существенное затруднение нарушения функционирования (работоспособности) информационных систем;

- недопущение распространения с использованием информационных активов противоправной информации;

- обеспечение возможности восстановления доступа авторизованных пользователей к информационным активам и содержащейся в них информации, заблокированной вследствие реализации (возникновения) угроз безопасности информации;

- обеспечение возможности восстановления информации, модифицированной или уничтоженной вследствие реализации (возникновения) угроз безопасности информации.

5.3 Мероприятия и меры для достижения целей и решения задач защиты информации должны реализовываться в соответствии с п. 5.4-5.5. адаптированные с учетом разработанных моделей угроз информационных активов.

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 12 из 33
--	--	-------------

5.4 Для достижения целей и решения задач защиты информации должны проводиться следующие мероприятия:

- выявление и оценка угроз безопасности информации;
- контроль конфигураций информационных систем;
- управление уязвимостями;
- управление обновлениями;
- обеспечение защиты информации при обработке, хранении и обращении с информацией ограниченного доступа;
- обеспечение защиты информации при применении конечных устройств;
- обеспечение защиты информации при применении мобильных устройств;
- обеспечение защиты информации при удаленном доступе пользователей к информационным системам;
- обеспечение защиты информации при беспроводном доступе пользователей к информационным системам;
- обеспечение защиты информации при предоставлении пользователям привилегированного доступа к информационным активам;
- обеспечение мониторинга информационной безопасности;
- обеспечение разработки безопасного программного обеспечения;
- обеспечение физической защиты информационных систем;
- обеспечение непрерывности функционирования информационных систем при возникновении нештатных ситуаций;
- повышение уровня знаний и информированности пользователей по вопросам защиты информации;
- обеспечение защиты информации при взаимодействии с подрядными организациями;
- обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании;
- обеспечение защиты информации при использовании искусственного интеллекта;
- реализация в информационных системах мер по их защите и защите содержащейся в них информации;
- проведение контроля уровня защищенности информации, содержащейся в информационных системах.

5.5 Для достижения целей и решения задач защиты информации должны быть реализованы следующие базовые меры защиты:

- идентификация и аутентификация;
- управление доступом;
- регистрация событий безопасности;
- защита виртуализации и облачных вычислений;

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 13 из 33
--	--	-------------

- защита технологий контейнерных сред и их оркестрации;
- защита сервисов электронной почты;
- защита веб-технологий;
- защита программных интерфейсов взаимодействия приложений;
- защита конечных устройств;
- защита мобильных устройств;
- защита технологий интернета вещей;
- защита точек беспроводного доступа;
- антивирусная защита;
- обнаружение и предотвращение вторжений на сетевом уровне;
- сегментация и межсетевое экранирование;
- защита от компьютерных атак, направленных на отказ в обслуживании;
- защита каналов передачи данных и сетевого взаимодействия.

6 Категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия (права)

6.1 Защиту информации организует ректор или по его решению назначенное ответственное лицо в должности не ниже проректора.

6.2 Ректор либо назначенное ответственное лицо определяет структурное подразделение или назначает отдельных специалистов, на которых возлагаются обязанности (функции) по защите информации.

Обязанности (функции) и полномочия (права) ответственного лица по организации деятельности по защите информации, управлению защитой информации, организации контроля за данной деятельностью и обязанности (функции) и полномочия (права) специалистов по защите информации по проведению мероприятий и принятию мер по защите информации определяются в их должностных инструкциях. Состав обязанностей (функций) и полномочий (прав) специалистов по защите информации должен быть достаточен для проведения мероприятий и принятия мер по защите информации.

6.3 Требуемый уровень информационной безопасности обеспечивается проведением мероприятий всеми лицами взаимодействующими с информационными активами. Защиту информации для каждого информационного актива обеспечивают:

- специалисты по защите информации;
- сотрудники, использующие информационные активы;
- сотрудники, обеспечивающие эксплуатацию информационных активов.

6.4 Подразделения (работники), использующие информационные активы, должны участвовать в проведении мероприятий и принятии мер по

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 14 из 33
--	--	-------------

защите информации в объеме, установленном в локальных нормативных актах университета.

6.5 Подразделения, обеспечивающие эксплуатацию и развитие информационных активов, должны проводить мероприятия и принимать меры по защите информации в ходе сопровождения, обслуживания, развития информационных активов, поставки комплектующих, отладки информационных активов и иных видов эксплуатационных работ объеме, установленном в локальных нормативных актах университета.

6.6 Специалистами по защите информации должны применяться программные, программно-аппаратные средства, обеспечивающие выполнение возложенных на них обязанностей (функций) по защите информации, в том числе по выявлению угроз безопасности информации, обнаружению и предотвращению вторжений, проведению контроля уровня защищенности информации, содержащейся в информационных системах, мониторингу информационной безопасности информационных систем, выявлению уязвимостей, контролю настроек и конфигураций информационных систем, а также средства и системы, предназначенные для автоматизации и аналитической поддержки деятельности по защите информации. Состав программных и программно-аппаратных средств, необходимых специалистам по защите информации для выполнения возложенных на них обязанностей (функций), определяется во внутренних регламентах по защите информации.

6.7 По решению ректора или ответственного лица для проведения мероприятий и принятия мер по защите информации могут привлекаться организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации. Состав проводимых организациями-лицензиатами мероприятий и принимаемых ими мер по защите информации, используемых при этом программных, программно-аппаратных средств, предназначенных для защиты информации, определяется в договорах или иных документах, на основании которых такие организации-лицензиаты привлекаются к защите информации.

Специалисты по защите информации должны осуществлять контроль проводимых организациями-лицензиатами мероприятий и принимаемых ими мер по защите информации.

6.8 Специалисты по защите информации должны разрабатывать и представлять ректору или ответственному лицу обоснованные предложения по организационным, материально-техническим и иным обеспечивающим ресурсам, необходимым для проведения мероприятий и принятия мер по защите информации, с указанием сведений о целях защиты информации, на достижение которых требуются ресурсы, и

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 15 из 33
--	--	-------------

перечня негативных последствий (событий), наступление которых прогнозируется в случае отсутствия ресурсов.

Ректор или ответственное лицо на основе представленных предложений и в пределах имеющихся средств предусматривает выделение организационных, материально-технических и иных обеспечивающих ресурсов для проведения мероприятий и принятия мер по защите информации, привлечения при необходимости дополнительных сил и средств для защиты информации.

7 Организация системы обеспечения информационной безопасности

7.1 Общее руководство системой обеспечения информационной безопасности осуществляет руководство университета по следующим направлениям:

- 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.

7.2 Управление деятельностью по защите информации должно включать:

- а) разработку и планирование мероприятий и мер по защите информации;
- б) проведение мероприятий и принятие мер по защите информации;
- в) проведение оценки состояния защиты информации;
- г) совершенствование мероприятий и мер по защите информации.

7.3 Все подразделения университета и их руководители отвечают за реализацию политики информационной безопасности и управление процессами ее обеспечения в рамках своих компетенций:

7.3.1 ИТ-Управление (далее – ИТУ):

- разрабатывает нормативные, инструктивные и методические документы университета по обеспечению информационной безопасности;
- разрабатывает требования по защите информационных активов в аспектах целостности и конфиденциальности на основе анализа рисков информационной безопасности;

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 16 из 33
--	--	-------------

- 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;
- осуществляет регистрацию информации об инцидентах, имеющих отношение к информационной безопасности;
- проводит расследования инцидентов и фактов нарушений информационной безопасности и информирует руководство о результатах проведенного расследования;
- обеспечивает выполнение требований информационной безопасности при администрировании автоматизированных информационных систем;
- 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.
- проводит обновление системного ПО, связанное с устранением критичных уязвимостей;
- обеспечивает доступность информационных ресурсов;
- обеспечивает хранение документации на информационные системы;
- организует обучение персонала по вопросам информационной безопасности;
- оценивает риски реализации угроз в информационных активах.

7.3.2 Все подразделения университета

- обеспечивают выполнение требований и процедур информационной безопасности при работе с информационными ресурсами и информационными активами.
- обеспечивают выполнение требований информационной безопасности при работе со средствами криптографической защиты, в том числе со средствами электронной подписи;
- обеспечивают взаимодействие с ответственными сотрудниками ИТУ при инцидентах информационной безопасности.

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 17 из 33
--	---	-------------

8 Основные принципы обеспечения информационной безопасности

Университет определяет следующие основные принципы обеспечения информационной безопасности:

Осведомленность о риске информационной безопасности. Процессы обеспечения информационной безопасности затрагивают каждого сотрудника университета, использующего его информационные активы, и накладывают на него соответствующие обязанности и ограничения.

Персональная ответственность. Ответственность за нарушения требований информационной безопасности возлагается непосредственно на сотрудников, допустивших нарушения, и руководителя подразделения, в котором нарушения допущены.

Минимальность полномочий. Любому сотруднику университета доступ к информационным ресурсам предоставляется только в том объеме, который необходим ему для выполнения служебных обязанностей. Все операции по предоставлению доступа или назначению полномочий осуществляются строго в соответствии с установленными процедурами.

Комплексность защиты. Меры по обеспечению безопасности информационных активов\ресурсов принимаются по всем идентифицированным видам угроз с учетом результатов оценки рисков информационной безопасности.

Адекватность защиты. Принимаемые меры обеспечения информационной безопасности эффективны и соразмерны имеющим место рискам информационной безопасности.

Эргономичность защиты. Средства защиты должны быть максимально “прозрачными” и удобными для пользователей и администраторов автоматизированных систем.

Документированность. Документирование обеспечивает закрепление достигнутого текущего состояния системы обеспечения информационной безопасности. Любые изменения этого состояния оформляются документально.

Непрерывность процессов контроля и совершенствования системы обеспечения информационной безопасности. В университете осуществляется постоянный мониторинг и аудит системы обеспечения информационной безопасности, по результатам которых осуществляется анализ эффективности принятых мер обеспечения информационной безопасности с учетом изменений среды функционирования информационного актива\ресурса, появления новых угроз, инцидентов и проблем, планируются и внедряются дополнительные меры защиты.

Контроль со стороны руководства. Руководство на регулярной основе рассматривают отчеты о состоянии информационной безопасности

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 18 из 33
--	--	-------------

в подразделениях университета и фактах нарушений установленных требований, а также общие и частные вопросы информационной безопасности, связанные с использованием технологий повышенного риска или существенно влияющие на бизнес-процессы. Политика информационной безопасности и предложения по ее актуализации рассматриваются Руководством на периодической основе.

Целевое финансирование мероприятий по обеспечению информационной безопасности. Ежегодный бюджет университета предусматривает специальные статьи расходов на обеспечение информационной безопасности.

9 Категории информации и информационных систем

9.1 Устанавливаются следующие категории информации:

– Общедоступная информация – открытая информация, находящаяся в публичном доступе.

– Открытая информация – информация для которой нет запрета на распространение и/или обработку.

– Конфиденциальная информация – сведения конфиденциального характера, указанные в Указе Президента РФ от 06.03.1997 г. № 188, а также персональные данные.

– Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации в соответствии с Федеральным законом от 21.07.1993 № 5485-1 «О государственной тайне» (*настоящим Стандартом защита государственной тайны не регулируется*).

– Иная информация для внутреннего пользования, не подпадающая под иные категории и подлежащая защите.

9.2 Устанавливаются следующие категории ИС:

– Открытые ИС – ИС, обрабатывающие общедоступную и/или открытую информацию.

– ИС, обрабатывающие сведения конфиденциального характера – ИС, предназначенные для обработки конфиденциальной информации, за исключением персональных данных.

– ИС персональных данных – ИС, предназначенные и/или осуществляющие обработку персональных данных.

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 19 из 33
--	---	-------------

– Иные ИС – ИС, предназначенные для оборотки информации, не относящийся к категориям общедоступных, открытых, конфиденциальных или персональных данных.

– Гибридные ИС – ИС одновременно обрабатывающие не менее 2-х категорий информации, указанных в п. 9.1.

10 Политика информационной безопасности при использовании автоматизированного рабочего места

10.1 Подключение компьютеров к корпоративной сети университета, установка и удаление программного обеспечения, осуществление настроек системного и прикладного программного обеспечения, в том числе служб и протоколов, настройка сетевых настроек осуществляется только уполномоченными сотрудниками ИТУ, за исключением настроек, не требующих привилегированных прав.

10.2 Запрещается обрабатывать сведения конфиденциального характера на АРМ, не предназначенных для такой обработки.

10.3 Обработка конфиденциальной информации в присутствии лиц, не допущенных к ней возможна только при соблюдении мер, исключающих неправомерное ознакомление с такой информацией.

10.4 На АРМ используется только лицензионное программное обеспечение либо свободно распространяемое программное обеспечение в соответствии с функциональными обязанностями пользователя.

10.5 Съёмные носители информации, разрешенные для использования, подлежат учету и контролю использования. Для работы со съёмными носителями информации они должны быть предварительно проверены антивирусным программным средством. Запрещается использовать съёмные носители информации на АРМ с отсутствующей или выключенной антивирусной защитой, а также в случаях установки на АРМ не актуальных антивирусных баз (допускается отклонение даты антивирусных баз от текущей даты не более 3 календарных дней).

10.6 На АРМ должна быть настроена автоматическая блокировка при отсутствии активности более 20 минут. На время своего отсутствия пользователь должен блокировать свой АРМ независимо от времени своего отсутствия. Под данное требование попадает любой случай, когда АРМ не находится в зоне видимости пользователя.

10.7 При выводе из эксплуатации или перемещении машинных носителей информации, используемых для обработки конфиденциальной информации, должно быть обеспечено гарантированное уничтожение данной конфиденциальной информации.

10.8 Должна обеспечиваться своевременная установка обновлений безопасности операционных систем, прикладного программного обеспече-

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 20 из 33
--	--	-------------

ния и средств защиты информации с проведением предварительной проверки подлинности и целостности обновлений программных, программно-аппаратных средств и тестирования обновлений до их эксплуатации в информационных активах. В случаях снятия с поддержки программного обеспечения и отсутствия возможности перехода на иное программное обеспечения для выполнения производственных задач, необходимо предусмотреть компенсирующие меры для исключения реализации потенциальных угроз.

11 Политика информационной безопасности при использовании электронной почты и Интернет

11.1 Запрещено передавать по электронной почте и через Интернет сведения конфиденциального характера без использования средств защиты информации, прошедших оценку соответствия требованиям законодательства РФ в области обеспечения безопасности информации.

11.2 Запрещено использовать корпоративную электронную почту для осуществления рассылки сообщений не связанных с рабочими целями, сообщения рекламного и агитационного характера, сообщения нарушающие требования действующего законодательства Российской Федерации, нормы корпоративной этики и культуры, а также авторские и смежные права других лиц.

11.3 Запрещено переходить по ссылкам и открывать вложения в письмах, полученных от неизвестных адресатов.

11.4 Запрещено использовать почтовые учетные записи других пользователей для отправки сообщений от их имени.

11.5 Доступ сотрудников в Интернет должен быть контролируемым.

11.6 Запрещено использовать Интернет в целях нанесения репутационного вреда университету, в целях противоречащих законодательству Российской Федерации, в личных целях для получения коммерческой выгоды.

11.7 Запрещено обсуждать служебные вопросы в социальных сетях, форумах, веб-ресурсах и иных средствах масс-медиа.

11.8 Запрещено использовать ресурсы Интернет, не имеющие отношения к выполнению должностных обязанностей.

11.9 Максимально исключить использование интернет-ресурсов не поддерживающих протоколы защиты интернет-трафика (SSL, TLS) и использовать ресурсы адрес которых начинается с префикса `https://` с обязательным символом «s» после «http».

11.20 На узлах доступа в Интернет должны быть предусмотрены меры противодействия компьютерным атакам.

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 21 из 33
--	---	-------------

12 Политика противодействия несанкционированному доступу

12.1 Защита от НСД должна обеспечить эшелонированную защиту информационных активов за счет использования средств защиты информации на различных уровнях.

12.2 Защита от НСД осуществляется комплексом организационных, технических и компенсирующих мер, направленных на нейтрализации угроз безопасности информации.

12.3 Исключение использования программного обеспечения без подтверждения отсутствия недокументированных (недекларированных) возможностей.

13 Политика управления доступом

13.1 Все информационные активы университета идентифицируются, категорируются и имеют своих владельцев.

13.2 Доступ к информационным активам всем сотрудникам университета предоставляется на основании матрицы доступа в соответствии с занимаемой должностью. Для предоставления дополнительного доступа необходимо согласование начальника ИТУ на основании предоставленной докладной записке.

13.3 В случае увольнения сотрудника блокировка доступа к информационным активам учетной записи осуществляется в автоматическом режиме. В случае изменения обязанностей сотрудника, в связи с изменением его должности, доступы к информационным активам изменяются в соответствии с матрицей доступа.

13.4 Доступ к информационным активам предоставляется с минимально необходимым набором прав, достаточным для выполнения функциональных обязанностей.

13.5 Каждому пользователю, допущенному к работе с информационным активом, не связанным с образовательной деятельностью, предоставляется персонифицированная учетная запись. Запрещено использовать одну учетную запись различным пользователям, за исключением, а также административных и технологических учетных записей без возможности персонификации.

13.6 Прямой доступ пользователей к базам данных не предоставляется.

13.7 Журналы аудита действий пользователей и администраторов информационных систем должны быть информативны, защищены от модификации и храниться в течение срока, потенциально необходимого для использования при расследовании возможных инцидентов, связанных с нарушением информационной безопасности.

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 22 из 33
--	---	-------------

13.8 Удаленный доступ к информационным активам допускается только на основании докладной записки на имя ректора университета с согласующей визой начальника ИТУ при условии применения сертифицированных средств обеспечения безопасной дистанционной работы, средств антивирусной защиты и иных средств защиты информации, исключающих угрозы безопасности информации, связанные с удаленным доступом.

13.9 Привилегированный доступ должен осуществляться с применением строгой аутентификации, а в случае технической невозможности применения строгой аутентификации — с использованием усиленной многофакторной аутентификации.

Не допускается объединение в рамках одной привилегированной учетной записи или одной группы привилегированных учетных записей ролей по системному администрированию, ролей по разработке и тестированию программных, программно-аппаратных средств, ролей администраторов безопасности.

13.10 Необходимо осуществлять периодический пересмотр прав доступа к информационным активам с целью определения не актуальных прав доступа.

14 Парольная политика

14.1 Пароли в информационные системы должны удовлетворять следующим требованиям:

- максимальный срок действия пароля составляет 90 (девяносто) дней, если иной срок не указан в утвержденной документации на систему;
- минимальный срок действия пароля составляет 1 (один) день;
- пароль должен содержать символы, относящиеся к 3 (трем) из перечисленных категорий: латинские заглавные буквы (A–Z), латинские строчные буквы (a–z), цифры (0–9), отличные от букв и цифр символы (например, !, \$, #);
- пароль пользователя должен состоять из не менее, чем 8 (восьми) символов при отсутствии технических ограничений информационной системы на установление такой длины;
- пароль привилегированного пользователя должен состоять из не менее, чем 12 (двенадцати) символов при отсутствии технических ограничений информационной системы на установление такой длины;
- пароль не предполагающий свое изменение со временем и пароли не персонифицированных учетных записей привилегированного пользователя должны состоять из не менее, чем 16 (шестнадцати) символов при отсутствии технических ограничений информационной системы на установление такой длины, при этом такой пароль обязательно резервируется и

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 23 из 33
--	--	-------------

хранится в запечатанном конверте в сейфе сопровождающего систему подразделения;

- пароль не должен совпадать с 10 (десятью) последними паролями;
- пароль должен иметь отличие от предыдущего пароля минимум в 1 символе;
- пароль не должен содержать имя учетной записи пользователя или фрагменты имени пользователя длиной больше 2 (двух) символов;
- пароль не должен содержать легко угадываемые последовательно-сти символов (123456, aaabbb, qwerty, q1w2e3 и т. п.);
- в случае 10 (десяти) подряд неудачных попыток ввода пароля в течение 30 (тридцати) минут доступ должен быть заблокирован.

14.2 Первичный пароль, формируемый при создании учетной записи или смене забытого пароля, сообщается исключительно пользователю, являющемуся владельцем данной учетной записи.

14.3 Срок действия первичного пароля не должен превышать 3 (трех) рабочих дней.

14.4 Пароль должен быть изменен в следующих случаях:

- при первичном обращении к объекту доступа;
- при истечении срока действия пароля;
- при подозрении в компрометации пароля;
- при изменении состава группы, использующей общий пароль.

14.5 Пользователь должен быть извещен об истечении срока действия пароля и необходимости его смены за 14 (четырнадцать) календарных дней до окончания указанного срока.

14.6 Пароли, предустановленные производителями компонентов информационно-технологической инфраструктуры и СЗИ, должны сменяться до начала его эксплуатации.

14.7 Ввод пароля должен обязательно маскироваться специальным символом.

14.8 При хранении пароли должны быть защищены от НСД.

14.9 Владельцы паролей обязаны обеспечить исключение компрометации паролей, в то числе запрещается:

- сообщать свой персональный пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме случаев сохранения паролей ключевых учетных записей владельцем информационного актива);
- сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода.

14.10 При обнаружения факта компрометации пароля, сотрудником ИТУ составляется акт данного обнаружения, докладная записка на имя начальника ИТУ с отражением обстоятельств выявленного факта и бес-

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 24 из 33
--	--	-------------

печивается выполнение мероприятия по блокировке учетной записи до выяснения обстоятельств выявленного нарушения. По результатам расследования обстоятельств, начальник ИТУ составляет докладную записку – отчет о происшествии на имя ректора университета. Решение о разблокировке учетной записи и наказании принимает ректор.

14.11 Запрещено применение функции запоминания пароля используемыми на АРМе программными средствами, в том числе интернет-браузерами.

15 Политика сетевой защиты информации

15.1 Сегменты доступа пользователей должны быть отделены от серверных сегментов.

15.2 Серверные сегменты рекомендуется разделять по функциональному назначению и/или в зависимости от категорий ИС, размещенных в них. Различные категории ИС рекомендовано размещать в различных сегментах сети.

15.3 Сегменты доступа пользователей должны быть разделены на основе функциональных обязанностей работников.

15.4 Средства межсетевого экранирования обязательно должны контролироваться взаимодействия между:

- сегментами ДМЗ и сетью Интернет;
- сегментами ДМЗ и доверенными сегментами сети;
- пользовательскими и серверными сегментами;
- серверными сегментами различного функционального назначения и/или серверными сегментами, содержащими ИС различных категорий;
- пользовательскими сегментами с различными функциональными обязанностями работников.

15.5 Средства межсетевого экранирования должны реализовывать фильтрацию входящих и исходящих пакетов (данных) коммуникационных протоколов сетевого уровня на основе заданных правил фильтрации.

15.6 Должно осуществляться резервное копирование конфигураций средств межсетевого экранирования с заданной периодичностью.

15.7 Необходимо периодически осуществлять пересмотр правил межсетевого экранирования для выявления неиспользуемых разрешающих правил.

15.8 Должен быть определен список лиц, имеющих право удаленного доступа в корпоративную сеть университета.

15.9 При удаленном доступе необходимо:

- использовать двухфакторную аутентификацию удаленных пользователей;

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 25 из 33
--	--	-------------

- обеспечить безопасность передаваемой информации от НСД криптографическими методами;
- регистрировать все подключения удаленных пользователей;
- удаленному пользователю обеспечить установку на удаленном рабочем месте актуальных обновлений операционной системы и актуальных баз антивирусного программного обеспечения.

16 Антивирусная политика

16.1 Вся хранимая, обрабатываемая и полученная извне информация подлежит антивирусному контролю.

16.2 Средства антивирусной защиты информации должны быть установлены на всех АРМ пользователей и серверах.

16.3 Должна быть настроена автоматическая установка обновлений антивирусных баз.

16.4 С заданной периодичностью должна проводиться полная проверка АРМ пользователей и серверов на наличие вредоносного ПО.

16.5 Антивирусное программное обеспечение не должно препятствовать нормальному функционированию АРМ и серверов

16.6 Каждый сотрудник университета обязан выполнять правила эксплуатации антивирусного ПО и требования антивирусной безопасности в отношении внешних источников и носителей информации, а также сети Интернет, немедленно прекращать работу и информировать службу информационной безопасности при подозрениях на вирусное заражение.

16.7 Пользователи АРМ не должны иметь возможность отключать средства антивирусной защиты и препятствовать их работе.

16.8 Техническая возможность подключения пользователями к рабочим станциям внешних накопителей информации, модемов, мобильных телефонов, беспроводных интерфейсов, использование CD-/DVD-дисководов должна максимально ограничиваться.

16.9 Контроль и управление антивирусным программным обеспечением, а также устранение выявленных уязвимостей в системном программном обеспечении, должен производиться централизованно в автоматизированном режиме.

16.10 При невозможности централизованного обновления антивирусного и системного ПО периодичность, сроки и порядок проведения соответствующих мероприятий определяются оценкой имеющихся рисков вирусного заражения критичных информационных ресурсов и техническими возможностями такого обновления.

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 26 из 33
--	---	-------------

17 Политика использования СКЗИ и ЭП

17.1 Применение средств криптографической защиты информации для обеспечения безопасности информационных активов университета и взаимодействия со сторонними организациями производится в соответствии с порядком, установленным государственными уполномоченными органами.

17.2 Во внутренних системах университета СКЗИ используются в зависимости от результатов оценки рисков информационной безопасности.

17.3 Конфиденциальность информации при передаче по публичным сетям и внешним каналам связи обеспечивается обязательным применением шифрования.

17.4 Риски, связанные с возможной компрометацией криптографических ключей или доступом к защищаемой информации в обход средств криптографической защиты, должны минимизироваться специальными техническими и организационными мерами.

17.5 СКЗИ допускается не использовать для формирования и проверке ПЭП.

17.6 Сертифицированные СКЗИ применяются в обязательном порядке:

- при использовании криптографических мер защиты информации в ИСПДн и ГИС;
- для формирования и проверке КЭП.

17.7 Применяемые сертифицированные СКЗИ подлежат поэкземплярному учету.

17.8 Должны быть приняты меры по исключению посторонних лиц в помещениях, в которых используются сертифицированные СКЗИ.

17.9 Владелец НЭП\КЭП должен обеспечить конфиденциальность ключей электронной подписи.

17.10 Владельцам НЭП и КЭП запрещается:

- осуществлять несанкционированное копирование ключевых носителей;
- передавать ключевые носители лицам, к ним не допущенным;
- вносить изменения в сертифицированные СКЗИ;
- оставлять АРМ с установленным СКЗИ без контроля;
- оставлять аппаратный носитель ключей НЭП\КЭП без контроля.

17.11 Предпочтительным вариантом хранения ключей НЭП и КЭП является использование специализированных аппаратных съемных носителей информации Рутокен или eToken. Хранение ключей на ином съемном носителе информации, на жестком диске АРМ владельца электронной подписи, в т.ч. в реестре операционной системы или на сетевом диске,

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 27 из 33
--	--	-------------

должно быть согласовано руководством владельца электронной подписи с руководством ИТУ.

17.12 Аппаратный носитель ключей НЭП\КЭП должен быть подключен к АРМ только на время необходимости использования ключей.

18 Политика информационной безопасности на этапах жизненного цикла информационной системы

18.1 На этапе проектирования информационной системы, автоматизирующей бизнес-процессы, должны быть учтены требования информационной безопасности исходя из:

- категории обрабатываемой информации;
- классификации информационной системы по требованиям защиты информации;
- формирования модели угроз;
- определения требований к системе защиты.

18.2 При определении необходимости использования наложенных СЗИ необходимо предварительно провести мероприятия по проверке совместимости данных СЗИ с программным обеспечением информационной системы. При отсутствии совместимости – разработать и внедрить компенсирующие меры, нейтрализующие угрозы.

18.3 Должна проводиться оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации, обрабатываемой в информационном активе. Оценка эффективности может проводиться в форме государственной аттестации или оценки соответствия требованиям ИБ. Оценка соответствия ИС требованиям ИБ проводится в форме проверки реализации мер по обеспечению безопасности информации с учетом требований регуляторов.

19 Политика резервного копирования

19.1 Резервному копированию должны подвергаться информация, обрабатываемая в ИС и ИР, а также конфигурационная информация системного и прикладного программного обеспечения, серверного и сетевого оборудования, а также СЗИ.

19.2 Должен быть определен перечень информационных активов, подлежащих резервному копированию, а также параметры резервного копирования, в т.ч. тип, периодичность, максимальное время восстановления, период допустимой потери информации, место хранения резервной копии.

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 28 из 33
--	--	-------------

19.3 Тип и периодичность резервного копирования должны устанавливаться таким образом, чтобы обеспечить минимальные потери данных и время простоя информационных активов.

19.4 Резервное копирование должно производиться в автоматическом режиме при наличии технической возможности. События резервного копирования должны регистрироваться в журнале.

19.5 Резервные копии должны подвергаться регулярному тестированию (тестирование целостности самой резервной копии и тестирование восстановления из резервной копии).

19.6 Сотрудники обязаны сохранять копию всей значимой рабочей информации, необходимой для обеспечения непрерывности бизнес-процессов, в которых они задействованы, на соответствующих сетевых ресурсах. Периодичность сохранения копий информации определяется руководителем подразделения сотрудника и должно быть зафиксировано во внутреннем регламенте подразделения. Сотрудник несет персональную ответственность за сохранность информации и возможность восстановления в случае ее утраты в случае только локального хранения информации (например, на рабочем столе, локальном диске и т.д.).

19.7 Резервные копии, средства резервного копирования и восстановления должны располагаться на территориальном удалении от объекта проведения аварийного восстановления.

20 Политика управления рисками информационной безопасности

20.1 Целью управления рисками информационной безопасности является поддержание их на приемлемом для университета уровне.

20.2 Деятельность по управлению рисками нарушения ИБ включает в себя планирование, идентификацию риска, оценку риска, выбор способа реагирования на риск и разработку, планирование и внедрение мероприятий по управлению рисками нарушения ИБ.

20.3 Для каждой информационной системы определяется свой уровень приемлемого риска, проводится идентификация и анализ рисков, вероятность наступления рисков и результаты реализации рисков. Установленный уровень определяет принятие риска или его обработку с целью разработки мероприятий для закрытия риска.

20.4 Идентификация и оценка рисков проводится на регулярной основе, а также в случае возникновения существенных изменений способных повлиять на ранее определенную оценку. К таким изменениям могут относиться изменения в бизнес-процессах, изменения в составе информационного актива, инфраструктуры или ее компонентов, а также внешние факто-

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 29 из 33
--	--	-------------

ры (политические, экономические, экологические, социальные и т.д.), способные привести к возникновению новых рисков.

20.5 К возможным способам реагирования на риск относятся: избегание риска, минимизация риска, передача риска, принятие риска.

20.6 При выборе способа реагирования должна учитываться стоимость планируемых мероприятий по реагированию на риск по отношению к величине возможных потерь без проведения указанных мероприятий.

21 Политика управления уязвимостями

21.1 На постоянной основе должен производиться мониторинг уязвимостей в программных, программно-аппаратных средствах информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. В качестве источников информации об уязвимостях следует использовать:

- общедоступные профильные ресурсы по направлению ИБ в глобальной сети Интернет, в том числе базы угроз при использовании сертифицированных средств анализа защищенности;
- информационные порталы ФСТЭК России, НКЦКИ, ФСБ России;
- рассылки по электронной почте от отраслевого регулятора, ФСТЭК России, НКЦКИ, ФСБ России.

21.2 Для выявленных уязвимостей необходимо проводить оценку их применимости к существующим информационным активам университета.

21.3 Для определения уязвимостей, применимых к информационным активам университета, необходимо определить:

- критичность уязвимости;
- наличие обновления, устраняющего уязвимость;
- возможность оперативной установки такого обновления;
- целесообразность установки обновления, исходя из соотношения уровня критичности, временных затрат на его установку, степени возможного влияния на информационный актив;
- наличие и применимость компенсирующих мер;
- целесообразность применения компенсирующих мер вместо установки обновления.

21.4 При устранении уязвимостей ПО необходимо руководствоваться порядками, определенными в Методических документах ФСТЭК России по вопросам тестирования обновлений безопасности программных и программно-аппаратных средств, а также по вопросам организации процесса управления уязвимостями.

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 30 из 33
--	--	-------------

21.5 Обновления безопасности ПО должны быть получены только из доверенных источников с обязательной проверкой подлинности и целостности.

21.6 При установке обновлений ПО, полученных из доверенных источников необходимо проводить предварительное тестирование дистрибутивов ПО и обновлений на предмет проверки функциональности и корректности работы в тестовой среде.

21.7 При отсутствии возможности установки обновлений должны быть приняты компенсирующие меры для закрытия выявленных уязвимостей критичного уровня.

22 Политика управления инцидентами

22.1 Процесс управления инцидентами ИБ должен включать 4 этапа:

- планирование и подготовка: определение ответственного и группы реагирования, определения порядка взаимодействия между участниками, классификация событий и инцидентов ИБ, разработка сценариев реагирования на инциденты ИБ;

- использование: обнаружение и оповещение о возникновении события ИБ и определения данного события определенному классу инцидента ИБ, регистрация инцидента, реагирование на инцидент, закрытие инцидента;

- анализ: детальный анализ инцидента, формирование отчетности, проведения внутреннего расследования инцидента.

- улучшение: проведения мероприятий по улучшению процесса управления инцидентами ИБ.

22.2 Инциденты ИБ должны выявляться:

- сотрудниками университета во время выполнения своих должностных обязанностей;

- сотрудниками подрядных организаций, осуществляющих сопровождение информационных систем и ресурсов университета, посредством анализа их работоспособности;

- в результате мониторинга событий ИБ.

23 Политика повышения осведомленности сотрудников в области информационной безопасности

23.1 В рамках обучения и повышения осведомленности сотрудников в области ИБ ответственными сотрудниками должны проводиться следующие мероприятия:

- вводный инструктаж по ИБ при первичном обращении за доступом к информационным активам университета;

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 31 из 33
--	--	-------------

- на постоянной основе размещение информационных материалов по основным угрозам и проблемам безопасности (публикация новостей, рассылки в корпоративной почте) и оперативное доведение информации о появлении новых угроз, методиках реагирования на возможные инциденты, изменениях в нормативно-правовых и локальных нормативных актах;
- обязательное обучение сотрудников по требованиям информационной безопасности;
- проведение тестирования сотрудников на знания требований информационной безопасности.

23.2 Информация вводного инструктажа по вопросам ИБ предоставляется сотруднику при его первом входе в личный кабинет корпоративной информационной системы университета, с которой он обязан ознакомиться и подтвердить свое ознакомление. Журнал фиксации ознакомления с требованиями ИБ ведется в электронном виде в корпоративной информационной системе университета

23.3 Обучение может быть организовано в очном, заочном формате или с использованием дистанционных технологий и должно быть направлено на получение знаний безопасной работы с информацией и информационными активами, в том числе:

- с персональными данными;
- со сведениями конфиденциального характера;
- с электронной почтой и сетью Интернет;
- со средствами вычислительной техники и съемными носителями информации;
- с используемыми СЗИ и СКЗИ.

23.4 По результатам обучения должно проводиться тестирование для определения уровня освоения учебного материала. Сотрудники, не набравшие необходимые баллы для успешного прохождения тестирования, должны пройти обучение и тестирование повторно. Сотрудник не допускается к работе с информацией и информационными активами до момента успешного прохождения тестирования.

23.5 Обучение проводится не реже 1 раза в 2 года.

23.6 Повышение квалификации в области ИБ проводится для специалистов, в должностные обязанности которых входит обеспечение информационной безопасности. Повышение квалификации проводится не реже 1 раза в 2 года.

23.7 Повышение осведомленности работников в области ИБ проводится на постоянной основе и включает в себя постоянное размещение информационных материалов по основным угрозам и проблемам безопасности (публикация новостей, рассылки в корпоративной почте) и оперативное доведение информации о появлении новых угроз, методиках реагиро-

	Система менеджмента качества СТО С.001-2025 Политика по защите информации	с. 32 из 33
--	---	-------------

вания на возможные инциденты, изменениях в нормативно-правовых и локальных нормативных актах.

24 Разработчик

Руководитель группы ИБ
ОССА ИТ управления

Магола Д.С.

Лист регистрации изменений

	Номер приказа, дата утверждения изменений	Количество страниц изменения	Дата получения изменения	Подпись уполномоченного по качеству
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				