УТВЕРЖДЕНО
решением ученого совета
ФГБОУ ВО «МГТУ им. Г.И. Носова»
(протокол от 12. 03. 2025 № 5)

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

ПОЛОЖЕНИЕ ПО ВИДУ ДЕЯТЕЛЬНОСТИ

Политика информационной безопасности

СМК-ПВД-3/2-62-25

Версия 1

(взамен СМК-СМК-ПВД-83-17)

Магнитогорск – 2025

Содержание

1. Назначение и область применения

1.1. Настоящее Положение является документом системы менеджмента качества университета.

1.2. Настоящая Политика информационной безопасности (далее – Политика) устанавливает цели, организацию и порядок выполнения работ в области информационной безопасности в Федеральном государственном бюджетном образовательном учреждении высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова» (далее – МГТУ им. Г.И. Носова»).

1.3. Политика направлена на защиту информационных ресурсов, информационной инфраструктуры и процессов обработки информации университета от возможного нанесения им материального, физического или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи ее по каналам связи, а так же минимизацию подобных рисков.

2. Нормативные документы, регламентирующие деятельность

Настоящее Положение разработано на основании следующих документов:

– Трудовой кодекс Российской Федерации;

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями);

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями);

– Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (с изменениями и дополнениями);

– Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

– Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

– Постановление Правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственного за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»;

– Постановление Правительства Российской Федерации от 1.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 16.01.2023 № 24 (ред. от 19.08.2023) «Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан»;

– Постановление Правительства РФ от 10.01.2023 № 6 «Об утверждении Правил принятия решения о запрещении или об ограничении трансграничной передачи персональных данных уполномоченным органом по защите прав субъектов персональных данных и информирования операторов о принятом решении»;

– Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

– Приказ ФСТЭК от 11.02.2013 № 17 (ред. от 28.08.2024) «Об утверждении Требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Приказ Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка. Утв. ФСТЭК России 15 февраля 2008 г.);

– Руководящий документ ФСБ России от 10 июля 2014 г. № 378 «Состав и содержание 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»;

– Руководящий документ ФСБ России от 21 февраля 2008 г. № 149/5-144 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»;

– Руководящий документ ФСБ России от 21 февраля 2008 г. № 149/6/6-622 «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27003-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации», утв. приказом Федерального агентства по техническому регулированию и метрологии от 19.05.2021 № 387-ст;

– Государственный стандарт Российской Федерации ГОСТ Р 50992-96 «Защита информации. Основные термины и определения»;

– Государственный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27004-21 «Методы и средства обеспечения безопасности»»;

– Государственный стандарт Российской Федерации ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;

– Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021)

– Политика обработки и защите персональных данных в МГТУ им. Г.И. Носова;

– Устав МГТУ им. Г.И. Носова;

– Трудовые договоры с работниками;

– Договоры, заключаемые между МГТУ им. Г.И. Носова и субъектом персональных данных;

– Согласия субъектов на обработку персональных данных;

и иные нормативно-правовые акты, устанавливающие требования к обеспечению информационной безопасности.

3. Термины, определения и сокращения

В настоящем Положении применены следующие термины с соответствующими определениями:

актив (информационный актив) - это информация или ресурс информационной системы, имеющие ценность для организации, использующиеся для достижения целей организации, являющиеся объектами защиты и кибератаки с целью нарушения свойств безопасности.

безопасность информации (данных) – состояние защищенности информации (данных), при которой обеспечиваются ее (их) конфиденциальность, доступность и целостность.

доступность информации (ресурсов информационной системы) - это состояние информации (ресурсов информационной системы), при котором обладающие необходимыми правами доступа могут их беспрепятственно реализовать.

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

защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

инцидент ИБ - это событие (или группа событий) ИБ, которые могут привести или уже привели к успешной кибератаке, нарушению работы информационного актива, нанесению ущерба интересам компании.

конфиденциальность информации - это состояние информации, при котором доступ к ней имеют только те, кто обладает соответствующими правами доступа.

кибератака (компьютерная атака) - это целенаправленное вредоносное воздействие на актив для нарушения его нормального функционирования и/или для реализации угрозы ИБ обрабатываемой ресурсом информации.

объект доступа - это информация или ресурс информационной системы (например, файл или запись в базе данных), с которым взаимодействует субъект доступа в соответствии с назначенными ему правами доступа.

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение,

уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

оценка риска – оценка вероятности реализации риска и величины возможных потерь при реализации конкретного вида риска и/ или совокупность рисков, принимаемых на себя МГТУ им. Г.И. Носова.

пароль - секретная строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системе для получения доступа к данным и программам. Пароль является средством защиты данных от несанкционированного доступа.

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

права доступа - это полномочия пользователя или сущности (например, программы или устройства) на обработку информации - чтение, запись, изменение, копирование, передачу, удаление.

риск – возможность в МГТУ им. Г.И. Носова потерь (убытков), незапланированных расходов и возможность снижения планируемых доходов.

риск информационной безопасности – риск, являющийся составной частью ИТ-риска, возникающий вследствие наличия угроз безопасности информационным ресурсам МГТУ им. Г.И. Носова.

событие ИБ - это зафиксированное изменение состояния информационного актива, которое может являться причиной инцидента ИБ.

средство защиты информации - техническое, программное или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа к информации или ресурсам информационной системы.

средство криптографической защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты защищаемой законом информации, в которых для обеспечения безопасности охраняемой информации осуществляется ее криптографическое преобразование.

субъект доступа - это пользователь или сущность, которые выполняют обработку информации в соответствии с назначенными им правами доступа.

техническая защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

учетная запись - информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (Адрес электронной почты, телефон и т.п.).

уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

целостность информации - это состояние информации, при котором она либо остается неизменной, либо изменения осуществляются только теми, кто имеет на это право.

электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронно-цифровой подписи (ЭЦП) и позволяющий идентифицировать владельца сертификата открытого ключа, а также установить отсутствие искажения информации в электронном документе.

В настоящей Политике применены следующие сокращения:

ЗИ – защита информации;

ИБ – информационная безопасность;

ИР – информационный ресурс;

ИС – информационная система;

ИСПДн – информационная система обработки персональных данных;

КИВС – корпоративная информационно-вычислительная сеть;

ЛВС – локальная вычислительная сеть;

МГТУ им. Г.И. Носова – Федеральное государственное бюджетное образовательное учреждение высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова»;

НСД – несанкционированный доступ;

ПДн – персональные данные;

ПО – программное обеспечение;

СЗИ – средства защиты информации;

СКЗИ – средства криптографической защиты информации;

УИТиАСУ – управление информационных технологий и автоматизированных систем управления МГТУ;

ФСТЭК – Федеральная служба по техническому и экспортному контролю.

ЭЦП – электронная цифровая подпись.

4. Общие положения

4.1. Целью деятельности, предусмотренной данной Политикой, является:

– определение принципов построения и обеспечения защиты информации при разработке информационных ресурсов, принадлежащих МГТУ им. Г.И. Носова;

– определение основных видов угроз информационной безопасности при разработке и эксплуатации информационных ресурсов, принадлежащих МГТУ им. Г.И. Носова;

– определение принципов защиты информационных ресурсов, принадлежащих МГТУ им. Г.И. Носова;

– определение принципов обеспечения качества при планировании и проведении работ в области информационной безопасности и защиты информации.

– выполнение требований законодательства Российской Федерации в области защиты информации и обработки и защиты информации;

– информирование о принципах и подходах, применяемых в МГТУ им. Г.И. Носова к организации и проведению работ по обеспечению информационной безопасности и защиты информации.

4.2. Действие данной Политики распространяется на:

– Всех пользователей информационных ресурсов, принадлежащих МГТУ им. Г.И. Носова;

– Работников МГТУ им. Г.И. Носова, задействованных в процессах разработки и эксплуатации информационных ресурсов, принадлежащих МГТУ им. Г.И. Носова;

– Третьих лиц, привлекаемых к разработке и эксплуатации информационных ресурсов, принадлежащих МГТУ им. Г.И. Носова.

5. Организация и порядок выполнения деятельности

5.1. Данная Политика регламентирует:

– состав и характер принципов и подходов, применяемых в МГТУ им. Г.И. Носова для организации и проведения работ в области защиты информации;

– состав актуальных угроз безопасности информации;

– перечень направлений и подходов, необходимых к реализации при проведении работ по защите информационных систем и сервисов информационных ресурсов МГТУ им. Г.И. Носова;

– права и обязанности пользователя информационных ресурсов МГТУ им. Г.И. Носова;

– принципы взаимодействия пользователя информационных ресурсов МГТУ им. Г.И. Носова» и МГТУ им. Г.И. Носова при реализации положений данной Политики.

5.2. Планирование работ по обеспечению выполнения данной Политики осуществляется на основании ежегодного Плана работ по комплексной защите информации, утверждаемого ректором МГТУ им. Г.И. Носова или лицом, имеющим необходимые полномочия (проректор по цифровизации).

5.3. Организация работ по обеспечению выполнения требований данной Политики возлагается на:

– начальника управления информационных технологий и автоматизированных систем управления (УИТиАСУ);

– начальника отдела защиты информации УИТиАСУ;

– начальника отдела информационных ресурсов и систем УИТиАСУ

под общим руководством проректора по цифровизации.

5.4. Контроль выполнения работ по обеспечению выполнений положений данной Политики возлагается на проректора по цифровизации.

5.5. Мероприятия по обеспечению выполнений требований данной Политики носят постоянный характер и обязательны к выполнению всеми работниками МГТУ им. Г.И. Носова, задействованными в предусмотренными данной Политикой процессах.

5.6. По результатам выполнения мероприятий, предусмотренных ежегодным планом по комплексной защите информации, производится анализ выполнения и разрабатывается перечень мероприятий по улучшению качества работы в области защиты информации и обеспечения конфиденциальности информации.

6. Концепция обеспечения информационной безопасности в МГТУ им. Г.И. Носова

Организация и функционирование системы информационной безопасности МГТУ им. Г.И. Носова должны соответствовать требованиям нормативно-правовых актов Российской Федерации в области защиты информации и следующим принципам:

– **законность** – принцип предполагает разработку системы информационной безопасности на основе федерального законодательства в области информатизации и защиты информации, и других нормативных актов по безопасности;

– **комплексность** – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их обработки (преобразования) и

использования, во всех режимах функционирования; способность системы информационной безопасности МГТУ к развитию и совершенствованию в соответствии с изменениями условий функционирования университета:

комплексность достигается:

– разработкой комплекта организационно-распорядительной документации, соответствующей требованиям Законодательства РФ в области защиты информации, и устанавливающей требования к процессам обработки информации в университете;

– организацией физической охраны помещений университета и обеспечением соответствующего режима доступа на территорию университета, ограничением доступа лиц в помещения с обработкой конфиденциальной информации;

– специальной организацией делопроизводства с ориентацией на защиту конфиденциальной информации и информации для внутреннего использования;

– внедрением системы электронного документооборота, соответствующей требованиям информационной безопасности, являющейся одной из составных частей системы безопасной обработки информации в МГТУ, и позволяющей контролировать стадии обработки документа и процесс внесения изменений в документ;

– мероприятиями по подбору, расстановке и специальной подготовке кадров университета, занимающихся обработкой конфиденциальной и служебной информации;

– рациональным использованием технических средств защиты информации;

– развернутой информационно-аналитической деятельностью.

Комплексность реализуется совокупностью правовых, организационных и инженерно-технических мероприятий.

– **своевременность** – упреждающий характер мер обеспечения информационной безопасности;

– **экономическая целесообразность** и сопоставимость возможного ущерба и затрат на обеспечение безопасности. Во всех случаях стоимость системы безопасности должна быть ниже размера возможного ущерба от любых видов риска;

– **специализация** – мероприятия по защите информации осуществляются с привлечением к разработке и внедрению мер и средств защиты информации и информационной инфраструктуры профессионально подготовленных специалистов университета;

– **взаимодействие и координация:** означает осуществление мер обеспечения информационной безопасности на основе четкой взаимосвязи соответствующих подразделений и служб университета;

– **совершенствование:** предусматривает совершенствование мер и средств защиты информации на основе собственного опыта и новых технических средств защиты информации;

– **централизация управления: п**редполагает самостоятельное функционирование системы информационной безопасности по единым правовым, организационным, функциональным и методологическим принципам и централизованным управлением деятельностью системы информационной безопасности;

– **ответственность** – должна быть явно определена за обеспечение безопасности информационных и управляющих систем университетом;

– **информированность** – собственники информации, пользователи информационных систем, студенты, сотрудники и партнеры университета должны быть проинформированы о правилах утвержденной политики информационной безопасности, а также степени ответственности при работе с конфиденциальной информацией университета. Факт ознакомления и изучения подтверждается подписью сотрудника в листе ознакомления с документом.

7. Объекты защиты

К объектам, подлежащим защите от потенциальных угроз и противоправных посягательств, относится любая документированная информация, информационные системы, системы хранения информации и телекоммуникационные сети, неправомерное обращение с которыми может нанести ущерб МГТУ им. Г.И. Носова.

Все объекты, в отношении которых могут быть осуществлены угрозы безопасности или противоправные посягательства, имеют различную уязвимость с точки зрения возможного материального или морального ущерба. Соответственно, объекты защиты подлежат классификации по уровням уязвимости (опасности), степени риска.

Наибольшую уязвимость представляют информационные ресурсы, содержащие конфиденциальную информацию, и сведения о движении финансовых средств.

Режим защиты информации устанавливается:

– в отношении сведений, отнесенных к государственной тайне, – уполномоченными органами на основании Закона Российской Федерации «О государственной тайне» и обеспечивается специальным подразделением МГТУ им. Г.И. Носова и, занимающимся охраной информации, представляющей собой государственную тайну;

– в отношении конфиденциальной информации – владельцем информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона и обеспечивается:

– в отношении персональных данных – Федеральным законом № 152-ФЗ «О персональных данных», Постановлениями Правительства РФ и подзаконными актами организаций-регуляторов в области обработки персональных данных;

– в отношении служебной информации – внутренними организационно-распорядительными документами университета в области информационной безопасности.

8. Основные виды угроз

Любое лицо, имеющее логический или физический доступ к информационным ресурсам и компонентам соответствующих информационных технологий (программному обеспечению и данным, средствам вычислительной техники, коммуникационному оборудованию и каналам связи) может являться потенциальным злоумышленником.

Целью злоумышленника является получение контроля над информационным ресурсом МГТУ им. Г.И. Носова, приводящего к нарушению его доступности, целостности или конфиденциальности.

Для достижения злоумышленник может использовать все экономически соизмеримые с потенциальным ущербом способы проведения атак на всех уровнях архитектуры автоматизированных информационных систем.

Источниками угроз информационными активами МГТУ им. Г.И. Носова являются:

- внешние и внутренние злоумышленники;
- ошибочное действие работников;
- вирусные атаки;
- отказы и сбои оборудования и программного обеспечения;
- техногенные и природные катастрофы;
- террористические угрозы.

Угрозы информационным ресурсам МГТУ им. Г.И. Носова проявляются в виде:

- разглашения конфиденциальной информации;
- утечки конфиденциальной информации через технические средства обеспечения производственной деятельности различного характера и исполнения;
- несанкционированного доступа к охраняемым сведениям, вследствие чего происходит их искажение, уничтожение или подделка;
- наличия уязвимостей в программном обеспечении;
- ошибочных действий пользователей информационных систем.

Перечень актуальных угроз, методы их нейтрализации должны быть отражены в модели угроз, разрабатываемой при выборе модели защиты информационных систем МГТУ им. Г.И. Носова. Выбор средств защиты информации и организационно-распорядительных мер по защите информации осуществляется исходя из необходимости нейтрализации угроз, описанных в модели угроз.

9. Защита информационных ресурсов

Защита информационных ресурсов предусматривает комплекс правовых, организационных, технических и программных мер и средств по защите информации в процессе документооборота, хранения, распространения и передачи принадлежащей МГТУ им. Г.И. Носова информации, а именно:

- реализация разрешительной системы допуска исполнителей (пользователей) к работам, документам и информации конфиденциального характера с обязательным ознакомлением допущенных исполнителей с требованиями нормативных документов в области защиты информации и ответственности за нарушение требований;
- ограничение доступа исполнителей и посторонних лиц в помещения, где проводятся работы по обработке информации конфиденциального характера;
- разграничение доступа пользователей к данным автоматизированных систем различного уровня и назначения;
- учет документов, информационных массивов, регистрация действий пользователей информационных систем, контроль несанкционированного доступа и других действий пользователей, способных создать угрозу информационной безопасности;

– шифрование информации, передаваемой по телекоммуникационным сетям общего пользования и применения криптографических средств защиты при использовании открытых каналов связи;

– минимизация влияния паразитных электромагнитных излучений и наводок (ПЭМИН) на средства вычислительной техники и телекоммуникационные каналы связи информационных систем МГТУ им. Г.И. Носова; мероприятия по исключению негласного съема информации через электрические цепи питания – электрическая развязка цепей питания, заземления и других цепей технических средств, выходящих за пределы контролируемой территории (при необходимости);

– использование средств постановки акустических помех для предотвращения негласного съема акустической информации;

– системы гарантированного электропитания (источники бесперебойного питания);

– проверка технических средств объектов информатизации и программного обеспечения на предмет выявления включенных в них недокументированных возможностей, закладных устройств, средств теневого входа и устройств негласного съема информации;

– предотвращение внедрения в автоматизированные информационные системы вредоносного программного кода и программ вирусного характера.

Защита информационных ресурсов от несанкционированного доступа должна предусматривать:

– обоснованность доступа (определение соответствующей формы допуска к информации для разных групп пользователей);

– персональную ответственность, заключающуюся в том, что исполнитель (пользователь) должен нести ответственность за сохранность доверенных ему документов (носителей информации, информационных массивов) и за свои действия в информационных системах;

– надежность хранения, когда документы (носители информации, информационные массивы) хранятся в условиях, исключающих несанкционированное ознакомление с ними, их уничтожение, подделку или искажение;

– разграничение информации по уровню конфиденциальности, заключающееся в предупреждении показания сведений более высокого уровня конфиденциальности в документах (носителях информации, информационных массивах) с более низким уровнем конфиденциальности, а также предупреждение передачи конфиденциальной информации по незащищенным линиям связи;

– контроль над действиями исполнителей (пользователей), работающих в автоматизированных системах, и использующих телекоммуникационные сети, в том числе телекоммуникационные сети общего пользования, включая сеть Интернет и другие глобальные вычислительные сети;

– целостность технической и программной среды, обрабатываемой информации и средств защиты, которая заключается в физической сохранности средств информатизации, неизменности программной среды, определяемой предусмотренной технологией обработки

информации, выполнении средствами защиты предусмотренных функций, изолированности средств защиты от пользователей.

Требование обоснованности доступа к информационным ресурсам реализуется в рамках системы допуска к работам, документам и сведениям, в которой устанавливается: кто, кому, в соответствии с какими полномочиями, какие документы и сведения (носители информации, информационные массивы), для каких действий или для какого вида доступа может предоставить и при каких условиях. Система допуска предполагает определение для всех групп пользователей автоматизированных систем или информационных и программных ресурсов, прав доступа и разрешение действий над информацией (просмотр/чтение, запись, модификация, удаление, выполнение).

Требование о персональной ответственности реализуется с помощью:

– ознакомления исполнителей с требованиями нормативной документации в области защиты информации и подтверждающей ознакомление личной подписи исполнителей в журналах, карточках учета, других разрешительных документах, а также на самих документах;

– индивидуальной идентификации пользователей и инициированных ими процессов в автоматизированных системах;

– проверки подлинности (аутентификации) исполнителей (пользователей) на основе использования паролей, электронных и механических ключей, магнитных карт, электронной цифровой подписи, а также биометрических характеристик личности как при доступе в автоматизированные системы, так и в выделенные помещения (зоны).

Условие надежности хранения реализуется с помощью:

– хранилищ конфиденциальных документов, оборудованных средствами охраны в соответствии с установленными требованиями, доступ в которые ограничен и осуществляется в установленном порядке;

– выделения помещений, в которых разрешается работа с конфиденциальной документацией, оборудованных сейфами и металлическими шкафами, а также ограничения доступа в эти помещения;

– размещения систем обработки и хранения конфиденциальной информации в специализированном помещении ограниченного доступа;

– использования криптографического преобразования информации в автоматизированных системах в случаях, предусмотренных требованиями нормативных документов.

Система контроля над действиями исполнителей реализуется с помощью:

– организационных мер контроля при работе исполнителей с конфиденциальными документами и сведениями;

– регистрации (протоколирования) действий пользователей с информационными и программными ресурсами автоматизированных систем с указанием даты и времени, идентификаторов запрашивающего и запрашиваемых ресурсов, вида взаимодействия и его результата, включая запрещенные попытки доступа;

– сигнализации и оповещения о несанкционированных действиях пользователей.

9.1 Защита Web-ресурсов МГТУ им. Г.И. Носова

Информационные системы МГТУ им. Г.И. Носова размещенные на постоянной основе в сети Интернет и применяемые для распространения и публикации принадлежащей МГТУ им. Г.И. Носова общедоступной информации являются Web-ресурсами МГТУ им. Г.И. Носова.

Организация и эксплуатация Web-ресурсов МГТУ им. Г.И. Носова должна выполняться с соблюдением комплекса организационных и технических мероприятий, исключающих:

– несанкционированный доступ к информации, размещенной на Web-ресурсах МГТУ им. Г.И. Носова, с целью ее незаконной модификации, искажения или уничтожения;

– использование Web-ресурсов МГТУ им. Г.И. Носова для несанкционированной рассылки информации и распространения вредоносного программного обеспечения;

– несанкционированную публикацию информации на Web-ресурсах МГТУ им. Г.И. Носова и несанкционированное распространение информации от имени МГТУ им. Г.И. Носова в сети Интернет.

9.2 Защита информации в линиях связи (вычислительных сетях)

Передача конфиденциальной информации, принадлежащей МГТУ им. Г.И. Носова, по телекоммуникационным сетям общего пользования (включая сеть Интернет) должна выполняться с учетом следующих требований:

– информация, предаваемая по сетям общего пользования, должна быть защищена от несанкционированной модификации или подмены;

– должны применяться средства и методы проверки подлинности, позволяющие однозначно установить собственника и отправителя информации, а также факт внесения изменений в информацию в процессе передачи;

– собственник и отправитель информации не должен иметь возможность отказа от авторства информации, отправленной им по сетям общего пользования от имени МГТУ им. Г.И. Носова.

Для подтверждения авторства информации и контроля за внесением изменений информации, передаваемой по сетям общего пользования, транспортным сетям передачи данных и другим каналам передачи информации, должен применяться механизм **квалифицированной электронной подписи.**

При необходимости передачи конфиденциальной информации по всем видам телекоммуникационной связи (вычислительным и информационным сетям), основным направлением защиты информации, от перехвата, искажения и навязывания ложной информации является использование методов криптографического преобразования информации (шифрования).

Для защиты информации должны использоваться средства криптографической защиты данных для определенного уровня конфиденциальности передаваемой информации и соответствующая ключевая система, обеспечивающая надежный обмен информацией и аутентификацию (подтверждение подлинности) сообщений.

Средства криптографической защиты информации, применяемые для защиты конфиденциальной информации, передаваемой по телекоммуникационным сетям общего

пользования, должны соответствовать требованиям нормативно-правовых актов РФ, установленных для средств криптографической защиты информации.

Эксплуатация средств криптографической защиты информации должна выполняться с учетом требований к использованию средств криптографической защиты информации, установленных законодательством РФ и соответствующими подзаконными актами.

9.3 Защита учётных записей

Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования.

Категорически запрещается сообщать и передавать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

Сотрудники должны создавать для учётных записей сложные пароли, отвечающие рекомендуемым требованиям к сложности паролей – выбирать достаточную длину, разный тип символов, не использовать простые последовательности символов и простые слова, не использовать свои имена, фамилии, номера телефонов.

Сотрудники не должны использовать для рабочих учётных записей пароли, которые они используют для любых других учётных записей, личных или учётных записей других организаций.

9.4 Защита оборудования

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация Университета.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят только системные администраторы и специалисты технической поддержки из числа работников УИТиАСУ.

10. Обеспечение качества в системе безопасности

Необходимой составляющей системы безопасности должно быть обеспечение качества работ и используемых средств и мер защиты, нормативной базой которого является система стандартов и других руководящих нормативно-технических и методических документов по безопасности, утвержденных федеральными органами государственного управления в соответствии с их компетенцией и определяющие нормы защищенности информации и требования в различных направлениях защиты информации.

К основным стандартам и нормативно-техническим документам в области защиты информации от несанкционированного доступа (НСД) относятся: комплект руководящих документов Гостехкомиссии России (1992 г.), в том числе «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации», «Положение по организации разработки, изготовления и эксплуатации программы и технических средств защиты информации от НСД в АС и СВТ».

При разработке системы защиты информации объекта автоматизации, необходимо максимально эффективно использовать имеющиеся средства вычислительной техники и связи.

Дополнительные средства защиты и контроля защищенности, разрабатываются или заказываются только в случаях, когда имеющимися средствами нельзя достигнуть необходимых результатов.

При разработке автоматизированных систем различного назначения и систем информатизации (включая информационные системы персональных данных) серьезное внимание уделяется выбору общесистемного программного обеспечения и технических средств защиты.

11. Мероприятия политики информационной безопасности

Исходя из представленных в политике задач, принципов организации и функционирования системы информационной безопасности, целесообразно выделить следующие обязательные мероприятия:

– информационно-аналитические исследования и прогнозные оценки информационной безопасности;

– обеспечение безопасности информационных ресурсов университета.

Мероприятиями информационно-аналитических исследований и прогнозных оценок безопасности являются:

– организация работ по выявлению конфиденциальной информации, обоснованию уровня ее конфиденциальности и документальному оформлению в виде перечней сведений, подлежащих защите;

– выявление и прогнозирование уязвимых мест в защите при работе с информационными ресурсами, разработка и осуществление комплекса оперативных и долговременных мер по их предупреждению и нейтрализации;

– координация деятельности подразделения службы информационной безопасности и обеспечения взаимодействия со всеми структурными подразделениями вуза в решении проблемы информационной безопасности.

Мероприятиями обеспечения безопасности информационных ресурсов МГТУ им. Г.И. Носова являются:

– организация и осуществление разрешительной системы допуска исполнителей к работе с документами и сведениями ограниченного доступа;

– организация хранения и обращения с конфиденциальными документами и документами для внутреннего использования (носителями информации);

– использования средств криптографической защиты информации при передаче конфиденциальной информации по общедоступным каналам связи;

– организация и координация работ по защите информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи;

– обеспечение безопасности в процессе проведения конфиденциальных совещаний, переговоров;

– осуществление контроля за сохранностью конфиденциальных документов (носителей информации), за обеспечением защиты информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи.

12. Ответственность

Соблюдение требований и правил в области информационной безопасности является обязательным для всех работников и обучающихся МГТУ им. Г.И. Носов», а также заинтересованных лиц.

Исполнителями работ в области информационной безопасности, предусмотренных данной политикой, являются сотрудники отдела защиты информации УИТиАСУ.

Ответственность за выполнение требований данной Политики возлагается на сотрудников отдела защиты информации УИТиАСУ МГТУ им. Г.И. Носова в лице его руководителя, а также ответственные в подразделениях университета, занимающихся обработкой информации в процессе осуществления деятельности университета.

Руководитель отдела защиты информации несет полную ответственность за качество и своевременность выполнения задач и функций по защите информации, возложенных на подразделение, в том числе:

– правильность документов, подготавливаемых подразделением;

– правильность применения и соблюдения требований документации СМК (пять уровней), входящих в компетенцию подразделения;

– организацию и проведение мероприятий по технической защите информации;

– выполнение приказов и указаний руководства университета в области защиты информации.

Ответственные в подразделениях отвечают за строгое и неукоснительное соблюдение требований, установленных нормативными документами по защите информации.

Лица, виновные в нарушении требований информационной безопасности, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

СМК-ПВД-3/2-62-25 Система менеджмента качества. Положение по виду деятельности. Политика информационной безопасности разработал:

Начальник отдела защиты информации Д.Н. Мазнин

Документ СМК (№ 42 от 27.02.2025)

Регистрация	
Номер документа	42
Дата регистрации	27.02.2025 14:34:36
Содержание	ПВД 32-62-25Политика Инф. безопасности
Подготовил	Тахтина Татьяна Васильевна (ПРОРЕКТОР ПО ЦИФРОВИЗАЦИИ, Секретарь проректора)
Подразделение инициатора	ПРОРЕКТОР ПО ЦИФРОВИЗАЦИИ
Прочие	
Состояние	Зарегистрирован, Согласование документов СМК: Согласован, Ознакомление с результатом согласования: Ознакомление завершено
Дополнительные реквизиты	

Согласование

ФИО, Должность	Результат	Дата	Замечание, комментарий
Согласование документов СМК			
Рубан Константин Алексеевич (Руководящий персонал, Проректор по цифровизации)	Согласовано	27.02.2025 14:41	
Мазнин Дмитрий Николаевич (Отдел защиты информации, Начальник отдела)	Согласовано	28.02.2025 14:51	
Уваровский Андрей Германович (Управление информационных технологий и автоматизированных систем управления, Начальник)	Согласовано	28.02.2025 10:50	
Звада Ольга Владимировна (Правовое управление, Начальник)	Согласовано	07.03.2025 13:58	
Иванова Анна Николаевна (Центр качества образования, Заведующий) (Заведующий ЦКО)	Согласовано	10.03.2025 08:33	