УТВЕРЖДАЮ
Ректор ФГБОУ ВО «МГТУ им. Г.И. Носова»
_____ В.М. Колокольцев
Введено в действие с «7» 02 2017 г.

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

ПОЛОЖЕНИЕ ПО ВИДУ ДЕЯТЕЛЬНОСТИ

Политика информационной безопасности

СМК-ПВД-83-17

Версия 2

Положение соответствует требованиям
ИСО 9001
Проректор по международной деятельности,
Лидер, ответственный за СМК,
_____ А.Г. Корчунов

Магнитогорск – 2017

СОДЕРЖАНИЕ

1 Назначение и область применения

1.1 Настоящая Политика является документом системы менеджмента качества университета.

1.2 Настоящая Политика устанавливает цели, организацию и порядок выполнения работ в области информационной безопасности в МГТУ им. Г.И. Носова:

- цели и задачи системы информационной безопасности, принципы ее организации и функционирования;
- виды угроз безопасности и ресурсы, подлежащие защите;
- основные направления разработки системы безопасности, включая правовую, организационную и инженерно-техническую защиту;
- информирование сотрудников и руководства университета о существующих требованиях по защите информации.

1.3 Настоящая Политика соответствует требованиям стандарта ИСО 9001.

2 Нормативные документы, регламентирующие деятельность

Настоящая Политика разработана на основании следующих документов:

Законодательные документы:

- Государственный стандарт Российской Федерации ГОСТ Р 50992-96 «Защита информации. Основные термины и определения».
- Государственный стандарт Российской Федерации ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
- Федеральный Закон № 152-ФЗ «О персональных данных» (редакция от 03.07.2016)
- Постановление Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1.11.2012 г.
- Приказ ФСТЭК №17 «Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11.02.2013 г.
- Приказ ФСТЭК №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 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».
- ИСО 9000 Системы менеджмента качества. Основные положения и словарь.

- ИСО 9001 Системы менеджмента качества. Требования.
- СМК-СМГТУ-29-11 Система менеджмента качества. Стандарт организации. Структура, содержание и изложение, правила оформления и обозначения документации системы менеджмента качества.
- СМК-ДП-4.2.3-01-14 Система менеджмента качества. Документированная процедура управления. Управление документами.
- СМК-МИ-29.02-11 Система менеджмента качества. Методическая инструкция. Общие требования к построению, содержанию, оформлению и управлению Положением о структурном подразделении.
- СМК-МИ-29.05-14 Система менеджмента качества. Методическая инструкция. Общие требования к построению, содержанию, оформлению и управлению Положением по виду деятельности.

Примечания

1 Если ссылочный документ заменен (отменен), то при пользовании настоящим документом, следует руководствоваться замененным (измененным) документом.

2 Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

В настоящем Положении применены следующие термины с соответствующими определениями:

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

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;

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;

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

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;

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

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 настоящем Положении применены следующие сокращения:

ЗИ – защита информации;

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;

ЭЦП – электронная цифровая подпись.

4 Общие положения

Основной целью настоящей политики информационной безопасности является представление гарантий защиты информации на всех основных этапах жизненного цикла информационной системы университета.

- защита информации, принадлежащей университету, от несанкционированных (преднамеренных и непреднамеренных) и противоправных действий по уничтожению, хищению, искажению, копированию, блокированию и подделки информации;
- предотвращение незаконного вмешательства в информационные ресурсы и информационные системы МГТУ им. Г.И. Носова, нарушения работы технических средств обработки и передачи информации, а также корпоративного программного обеспечения, включая средства информатизации;
- формирование целостного представления о системе информационной безопасности университета и взаимодействие различных элементов этой системы;
- определение путей реализации мероприятий по защите информации и создание в МГТУ им. Г.И. Носова системы защиты информации.

Исполнителями работ в области информационной безопасности, предусмотренных данной политикой, являются сотрудники отдела защиты информации УИТ и АСУ, а также ответственные в подразделениях университета, занимающихся обработкой информации в процессе осуществления деятельности университета.

5 Организация и порядок выполнения деятельности

5.1 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:

5.1.1 Законность – принцип предполагает разработку системы информационной безопасности на основе федерального законодательства в области информатизации и защиты информации, и других нормативных актов по безопасности.

5.1.2 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 им. Г.И. Носова 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 им. Г.И. Носова, 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. Предполагает 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.

5.2 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, 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.

5.3 Основные виды угроз

Угрозы информационным ресурсам 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.

5.4 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.

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

Информационные системы 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.

5.6 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.

5.7 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.

5.8 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 вуза 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.

6 Ответственность

Ответственность за выполнение требований данной Политики возлагается на сотрудников отдела защиты информации УИТ и АСУ МГТУ им. Г.И. Носова в лице его руководителя, и ответственных в подразделениях.

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.

СМК-ПВД-83-17 Система менеджмента качества. Положение по виду деятельности. *Политика информационной безопасности* разработал:

Начальник отдела защиты информации Д.Н. Мазнин

Лист согласования

СМК-ПВД-83-17

Политика информационной безопасности

Должность, Ведущий СМК с указанием направления деятельности	Подпись	И.О. Фамилия	Дата
Первый проректор–проректор по научно-инновационной работе, Ведущий СМК по научно-инновационной деятельности		М.В. Чукин	06.02.17
Начальник УИТ и АСУ, Ведущий СМК по информационной среде		К.А. Рубан	02.02.17г.
Начальник отдела менеджмента качества, Ведущий СМК по внутренним аудитам		А.Ю. Глухова	06.02.17

Экспертиза проведена:

Ведущий инженер отдела менеджмента качества А.Е.Кожемякина