МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Северный (Арктический) федеральный университет имени М.В. Ломоносова»

УТВЕРЖДЕНО
приказом ректора университета
от 03.12.2013 № 1133

ПОЛИТИКА
информационной безопасности Северного (Арктического) федерального университета имени М.В. Ломоносова
П 109 – 12.3

г. Архангельск
2013

1. ВВЕДЕНИЕ

1.1. Политика информационной безопасности федерального государственного автономного образовательного учреждения высшего профессионального образования «Северный (Арктический) федеральный университет имени М.В. Ломоносова» (далее – университет) разработана в соответствии с действующим законодательством Российской Федерации, нормами права в части обеспечения информационной безопасности (далее - ИБ), требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, противодействия техническим разведкам и технической защиты информации.

1.2. Руководители структурных подразделений университета ответственны за обеспечение выполнения требований информационной безопасности в структурных подразделениях.

1.3. Работники университета обязаны соблюдать требования настоящей Политики и иных документов, регламентирующих деятельность в области информационной безопасности.

1.4. Настоящая Политика разработана в соответствии с законодательством Российской Федерации, нормами права в части обеспечения информационной безопасности, нормативными актами Правительства Российской Федерации, нормативными актами федерального органа исполнительной власти, уполномоченного в области безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия иностранным техническим разведкам, и основывается в том числе на:

– доктрине информационной безопасности Российской Федерации (от 09 сентября 2000 года Пр-1895);

– ГОСТ Р ИСО 9001-2008 «Системы менеджмента качества»;

– ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»;

– ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью».

1.5. Контроль за выполнением требований настоящей Политики осуществляет отдел по комплексной защите информации управления информационно-коммуникационных технологий университета.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Настоящая Политика распространяется на все структурные подразделения университета и обязательна для исполнения всеми работниками. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах университета, а также в договорах.

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

3.1. В настоящей Политике используются следующие термины:

3.1.1 **автоматизированная система (далее – АС)** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

3.1.2 **аудит информационной безопасности университета** – процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самим университетом (внутренний аудит), так и независимыми внешними организациями (внешний аудит) на основе рекомендаций ГОСТ Р ИСО 9001-2008 и ГОСТ Р ИСО/МЭК 17799-2005. Результаты проверки документально оформляются свидетельством аудита;

3.1.3 **информационный технологический процесс** – часть производственного технологического процесса, содержащая операции над информацией, необходимой для функционирования университета;

3.1.4 **информационная безопасность (далее – ИБ)** – состояние защищенности информационных активов университета в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т. п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов университета. Защищенность достигается обеспечением совокупности свойств ИБ – конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры университета;

3.1.5 **информационные активы университета** – активы университета, имеющие отношение к его информационной сфере и представляющие ценность для нее с точки зрения достижения уставных целей;

3.1.6 **инцидент информационной безопасности** – действительное, предпринимаемое или вероятное нарушение ИБ, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов университета;

3.1.7 **код аутентификации электронного сообщения** – данные, используемые для установления подлинности и контроля целостности электронного сообщения;

3.1.8 **мониторинг информационной безопасности университета** – постоянное наблюдение за объектами, влияющими на обеспечение ИБ университета, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы, информационные услуги и пр.;

3.1.9 **риск** – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы;

3.1.10 **роль в университете** – заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом в университете. К субъектам относятся персонал университета, его клиенты, а также инициируемые от их имени действия над объектами. Объектами являются аппаратные и программные средства, информационные ресурсы, услуги и процессы, составляющие АС;

3.1.11 **угроза** – опасность, предполагающая возможность потерь (ущерба);

3.1.12 **управление информационной безопасностью университета** – совокупность целенаправленных действий, осуществляемых в рамках Политики ИБ в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер);

3.1.13 **уязвимость** – недостатки или слабые места информационных активов, которые могут привести к нарушению ИБ университета при реализации угроз в информационной сфере.

4. ЦЕЛИ И ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УНИВЕРСИТЕТА

4.1. Основными целями защиты информации университета являются:

4.1.1 предотвращение или снижение ущерба от инцидентов ИБ;

4.1.2 достижение адекватности мер по защите от реальных угроз ИБ;

4.1.3 повышение стабильности функционирования университета в целом.

4.2. Основными задачами деятельности по обеспечению ИБ университета являются:

4.2.1. повышение эффективности мероприятий по обеспечению и поддержанию ИБ с учетом требований системы менеджмента качества;

4.2.2. выявление, оценка и прогнозирование потенциальных угроз информационной безопасности и уязвимостей объектов защиты;

4.2.3. выработка рекомендаций по устранению уязвимостей.

5. ОБЪЕКТЫ ЗАЩИТЫ

5.1. Основными объектами системы информационной безопасности в университете являются:

5.1.1 информационные активы, содержащие информацию ограниченного распространения, включая персональные данные физических лиц, коммерческую тайну, а также открыто распространяемую информацию, необходимую для функционирования университета, независимо от формы и вида её представления;

5.1.2. работники и контрагенты университета, являющиеся пользователями информационных систем;

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

6. ИСХОДНАЯ КОНЦЕПТУАЛЬНАЯ СХЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УНИВЕРСИТЕТА

6.1. Концептуальная схема ИБ университета направлена на защиту ее информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий работников, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

6.2. Стратегия университета в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности (от организационных мер на уровне руководства университета до специализированных мер информационной безопасности по каждому выявленному в университете риску), основанных на оценке рисков информационной безопасности.

6.3. Наибольшими возможностями для нанесения ущерба университета обладают его собственные работники. Действия работников могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне университета), либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией работников и их способностью к адекватным действиям в нештатной ситуации.

6.4. Для противодействия угрозам информационной безопасности в университете на основе имеющегося опыта составляется модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модели угроз и нарушителя), тем ниже риски нарушения ИБ университета при минимальных ресурсных затратах.

6.5. При изменении характера угроз, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

7. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИБ

7.1. Основными принципами обеспечения ИБ являются:

7.1.1 контроль состояния защитных мер, влияющих на ИБ, с возможностью блокирования нежелательных действий и быстрого восстановления рабочих параметров информационной системы;

7.1.2 организация доступа пользователей к информационным активам университета по принципу «разрешено всё, что не запрещено»;

7.1.3 разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом совместимости этих мер с действующим технологическим процессом и затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей университета, а также повышать трудоемкость технологических процессов обработки информации и создавать дополнительные сложности для пользователей университета;

7.1.4 персонификация и адекватное разделение ролей и ответственности между работниками университета, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

8. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ

8.1. Модели угроз и нарушителей (прогноз ИБ) являются определяющими при развертывании, поддержании и совершенствовании системы обеспечения ИБ университета.

8.2. Источники угроз, уязвимости и объекты нападений, пригодные для реализации угрозы, типы возможных потерь, масштабы потенциального ущерба определяются документом «Модель угроз и нарушителей», разрабатываемым ответственным за обеспечение ИБ в университете.

9. ОБЩИЕ ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.1. Требования по обеспечению информационной безопасности университета разрабатываются исходя из проводимого моделирования угроз безопасности информации с соблюдением требований действующего федерального законодательства, нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и в области технической защиты информации.

9.2. Требования по обеспечению информационной безопасности университета обязательны к соблюдению всеми работниками университета и пользователями информационных систем.

9.3. Общие требования по обеспечению ИБ формулируются для следующих областей:

9.3.1. назначение и распределение ролей и доверия к работникам и пользователям АС;

9.3.2. защита от несанкционированного доступа, управление доступом и регистрацией в АС;

9.3.3. антивирусная защита;
9.3.4. использование ресурсов Интернет;
9.3.5. использование средств криптографической защиты информации;
9.3.6. защита информационных технологических процессов;
9.3.7. защита материальных носителей информации.

10. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

10.1. В целях выполнения задач по обеспечению информационной безопасности, в соответствии с рекомендациями международных и российских стандартов по безопасности, в университете функционирует подразделение, ответственное за обеспечение информационной безопасности – отдел по комплексной защите информации управления ИКТ.

10.2. Основной целью подразделения является обеспечение деятельности университета по реализации текущей политики ИБ в соответствии с уставными целями университета.

11. АУДИТ И САМООЦЕНКА ИБ

11.1. Порядок и периодичность проведения аудита ИБ университета, а также отдельных его структурных подразделений, определяется подразделением, ответственным за обеспечение ИБ, на основании потребности в такой деятельности.

11.2. Внешний аудит ИБ проводится независимыми организациями (индивидуальными предпринимателями), имеющими право на осуществление такой деятельности, с целью проверки и оценки ее соответствия требованиям действующего законодательства Российской Федерации в области информационной безопасности. Внешний аудит ИБ проводится на основании приказа ректора университета.

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

11.4. При подготовке к внешнему аудиту ИБ рекомендуется проведение самооценки ИБ.

12. ПОРЯДОК ПЕРЕСМОТРА ПОЛИТИКИ

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

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

12.3. С момента утверждения Политики ИБ ректором университета утрачивает силу предыдущая Политика информационной безопасности университета.