УТВЕРЖДАЮ
Ректор ФГБОУ ВО «НГУЭУ»
_____ А.В. Новиков
2020 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФГБОУ ВО "НГУЭУ"

г. Новосибирск – 2020 г.

Содержание

1. Область применения

1.1 Политика информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Новосибирский государственный университет экономики и управления «НИНХ» (далее - Университет) описывает политику информационной безопасности с целью закрепления подходов к функционированию и совершенствованию системы обеспечения информационной безопасности в Университете.

1.2 Политика информационной безопасности Университета (далее – Политика) определяет:

- цели и задачи системы обеспечения информационной безопасности;
- основные принципы и общие требования по обеспечению информационной безопасности;
- организацию системы обеспечения информационной безопасности.

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

2 Нормативные ссылки

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 следующих нормативных правовых актах Российской безопасности:

- Конституция Российской Федерации.
- Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента РФ от 05.12.2016 г. № 646.
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».
- 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 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».
- Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

- Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

- ГОСТ Р ИСО 9001-2015 Системы менеджмента качества. Требования

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

- ПЛ СМК НГУЭУ 7.5.3-003.01-2018 Порядок разработки и внедрения нормативно-методической документации НГУЭУ

3 Термины, определения, обозначения и сокращения

3.1 Термины и определения

Аудит информационной безопасности — 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 9001-2015 и серии ГОСТ Р ИСО/МЭК 27000. Результаты проверки документально оформляются отчетным документом аудита.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах.

Владелец информационного ресурса – подразделение Университета, наделенное полномочиями владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами. Владелец информационного ресурса определяется на этапе создания соответствующего ресурса.

Данные – информация, представленная в электронной форме.

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

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Информационная безопасность — состояние защищенности интересов и информационных активов Университета в условиях угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств информационной безопасности - конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры Университета. Приоритетность свойств информационной

безопасности определяется значимостью информационных активов для интересов (целей) Университета.

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

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

Идентификация риска – процесс выявления и классификации рисков.

Информационный ресурс – различная информация Университета на всех этапах ее жизненного цикла, обеспечивающая основную деятельность Университета и представляющая ценность с точки зрения достижения поставленных целей.

Информационный риск (ИТ-риск, риск автоматизации процессов) – риск, связанный с использованием информационных технологий, неудовлетворительным состоянием автоматизированных информационных систем Университета.

Инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности. Нарушение может быть вызвано ошибками персонала, неправильным функционированием технических средств, природными факторами, преднамеренными злоумышленными действиями, приводящими к нарушению доступности, целостности, конфиденциальности информации.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Информационный технологический процесс — часть производственного технологического процесса, содержащая операции над информацией, необходимой для функционирования Университета.

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

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

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 операции – операции, связанные с повышенными рисками информационной безопасности.

Критичные процессы/системы – процессы/системы, связанные с использованием критичных информационных ресурсов.

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.

Мониторинг ИБ 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 информационная система или ее часть, информационные технологические процессы, информационные услуги и прочее.

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.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В данном документе оператором выступает Университет.

Операционный риск – риск, возникающий в результате недостатков в организации деятельности Университета, используемых технологиях, функционировании информационных систем, неадекватных действий или ошибок работников, 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.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

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

Риск информационной безопасности – риск, являющийся составной частью ИТ-риска, возникающий вследствие наличия угроз безопасности информационным ресурсам Университета.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

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 средств, обеспечивающих требуемый уровень безопасности информационных ресурсов участниками соответствующих процессов.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно - вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

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

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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.

Управление информационной безопасностью Университета — совокупность целенаправленных действий, осуществляемых в рамках Политики 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).

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

3.2 Обозначения и сокращения

АИС – автоматическая идентификационная система

ИБ – информационная безопасность

ПО – программное обеспечение

СМК – система менеджмента качества

ФГБОУ ВО «НГУЭУ», НГУЭУ, Университет – федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный университет экономики и управления «НИНХ»

4 Цели и задачи информационной безопасности Университета

4.1 Цель обеспечения информационной безопасности – создание и постоянное соблюдение в Университете условий, при которых риски, связанные с нарушением безопасности информационных ресурсов Университета, постоянно контролируются и исключаются, либо находятся на допустимом (приемлемом) уровне остаточного риска.

Процессы обеспечения информационной безопасности Университета являются составной и неотъемлемой частью процессов управления информационными технологиями и сопутствующими операционными рисками и осуществляются на основе циклической модели: “планирование - реализация - проверка - совершенствование - планирование - …”.

4.2 Основными целями защиты информации Университета являются:

- соответствие законодательным требованиям и договорным обязательствам;
- снижение рисков Университета, связанных с использованием информационных технологий;
- предотвращение или минимизация ущерба от инцидентов ИБ;
- достижение адекватности мер по защите от реальных угроз ИБ;
- повышение стабильности функционирования Университета в целом.

4.3 Основными задачами деятельности по обеспечению защиты информации Университета являются:

- создание условий для максимальной автоматизации выполнения различных операций Университета и исключения ручных операций при условии минимизации рисков;
- контроль состояния информационной безопасности на всех этапах жизненного цикла автоматизированных информационных систем;
- обеспечение целостности информации, предусматривающее предотвращение несанкционированной модификации или разрушение информации;
- обеспечение конфиденциальности информации, что связано с предотвращением несанкционированного ознакомления с информацией;
- обеспечение безопасности средств обработки информации Университета и информационных ресурсов при доступе третьих сторон;
- своевременное выявление, оценка и прогнозирование потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
- выработка рекомендаций по устранению уязвимостей;
- обеспечение жизнедеятельности Университета и безопасности его информационных ресурсов в условиях форс-мажорных обстоятельств (экономические и политические кризисы, природные и техногенные катастрофы, террористические угрозы и пр.);

- оптимизация затрат на обеспечение информационной безопасности.

4.4 Безопасность информационных активов Университета оценивается и обеспечивается по каждому из следующих аспектов:

- доступность;
- целостность;
- конфиденциальность.

При этом критерием оценки является вероятность, размер и последствия нанесения Университету любого вида ущерба (невыполнение имеющихся перед государством и контрагентами обязательств, финансовые потери, репутационные потери и прочее).

4.5 Состояние информационной безопасности оказывает непосредственное влияние на операционные риски деятельности Университета, в связи с чем, любой факт (инцидент) нарушения информационной безопасности рассматривается как существенное событие.

5. Основные принципы обеспечения информационной безопасности

Университет определяет следующие основные принципы обеспечения информационной безопасности:

Осведомленность о риске информационной безопасности. Процессы обеспечения информационной безопасности затрагивают каждого работника Университета, использующего его информационные ресурсы, и накладывают на него соответствующие обязанности и ограничения.

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

Минимальность полномочий. Любому работнику 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 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 информационных 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 информационной инфраструктуры, появления новых угроз, инцидентов и проблем, планируются и внедряются дополнительные меры защиты.

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

6. Объекты защиты

6.1 Основными объектами системы информационной безопасности в Университете являются:

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

– работники и контрагенты Университета, являющиеся пользователями автоматизированных систем;

– 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.

7. Источники угроз

7.1 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. При этом предполагается возможность сговора работника Университета с внешним злоумышленником, но не сговор двух и более работников Университета.

Целью злоумышленника является получение контроля над информационным ресурсом, приводящего к нарушению его доступности, целостности или конфиденциальности.

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

7.2 Источниками угроз информационным активам Университета являются:

– внешние и внутренние злоумышленники;

– ошибочные действия работников;

– вирусные атаки;

– отказы и сбои оборудования и программного обеспечения;

– техногенные и природные катастрофы;

– террористические угрозы.

8. Исходная концептуальная схема обеспечения информационной безопасности

8.1 Концептуальная схема ИБ Университета направлена на защиту информационных ресурсов 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.

8.2 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.

8.3 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.

8.4 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.

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

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 автоматизированных систем.

9.3 Общие требования по обеспечению формулируются для следующих областей:

– назначение и распределение ролей и доверия к работникам и пользователям АИС;

– защита от несанкционированного доступа, управление доступом и регистрацией в АИС;

– управление жизненным циклом автоматизированных информационных систем;

– антивирусная защита;

– использование ресурсов сети Интернет;

– использование средств криптографической защиты информации;

– защита информационных технологических процессов;

– защита материальных носителей информации.

9.3.1 *Назначение и распределение ролей, и обеспечение доверия к работникам и пользователям АИС.* «Ролевое» управление является основным механизмом управления полномочиями пользователей и администраторов в автоматизированных информационных системах.

Роли формируются с учетом принципа минимальности полномочий.

Ни одна роль не должна позволять пользователю проводить единолично критичные операции.

Критичные технологические процессы должны быть защищены от ошибочных и несанкционированных действий администраторов. Штатные процедуры администрирования, диагностики и восстановления должны выполняться через специальные роли в автоматизированных информационных системах без непосредственного доступа к данным.

В критичных системах по решению владельца информационного ресурса может вводиться роль администратора информационной безопасности автоматизированной информационной системы, в функции которого входит подтверждение прав и полномочий пользователей, заведенных в системе ее администратором.

Должностные обязанности работников и трудовые договоры предусматривают обязанности персонала по выполнению требований по обеспечению информационной безопасности.

Приказы и распоряжения, актуальная информация по вопросам обеспечения информационной безопасности, в том числе по выявленным нарушениям, доводятся до работников Университета под роспись.

9.3.2 *Управление доступом к информационным ресурсам и регистрация.* Все информационные ресурсы Университета идентифицируются, категорируются и имеют своих владельцев.

Доступ к информационным ресурсам всем работникам Университета предоставляется только на основании документально оформленных заявок, согласованных с их владельцами. По умолчанию определяется отсутствие доступа.

Доступ к информационным ресурсам не предоставляется (прекращается) в случае отсутствия производственной необходимости, изменения функциональных и должностных обязанностей, увольнения работника.

Проводится периодический формальный контроль соответствия согласованных и реальных прав доступа к информационным ресурсам текущему статусу пользователя.

Прямой доступ пользователей к базам данных не предоставляется.

Доступ ко всем информационным ресурсам Университета осуществляется только после авторизации пользователя.

Журналы аудита действий пользователей и администраторов автоматизированных 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.

9.3.3 *Управление жизненным циклом автоматизированных информационных систем.* Процедуры по обеспечению информационной безопасности предусматриваются на всех стадиях жизненного цикла автоматизированных информационных систем: при разработке (приобретении), эксплуатации, модернизации, снятии с эксплуатации.

Разработка, тестирование автоматизированных информационных систем отделяются от эксплуатации.

Разработка и тестирование программного обеспечения проводятся на выделенных физически или логически средствах вычислительной техники (виртуальные серверы), не использующихся для эксплуатации автоматизированных информационных систем.

В контрактах со сторонними разработчиками на поставку систем предусматривается их ответственность за наличие в поставляемых системах скрытых недокументированных возможностей, ведущих к ущербу Университету, а также соблюдение условий конфиденциальности.

Все изменения, вносимые в автоматизированные информационные системы, контролируются и документируются. Дистрибутивные комплекты и исходные тексты систем собственной разработки, а также дистрибутивные комплекты приобретаемых систем хранятся в отделе развития информационной инфраструктуры.

Дистрибутивные комплекты средств защиты информации и средств антивирусной защиты, документация на критичные автоматизированные системы в обязательном порядке хранятся в подразделении, ответственном за обеспечение информационной безопасности.

Ввод автоматизированных информационных систем в эксплуатацию производится только после их проверки на соответствие предъявленным требованиям по информационной безопасности. Не допускается эксплуатация автоматизированных систем, не прошедших проверку и имеющих не устраненные критичные замечания.

При выводе автоматизированной информационной системы из эксплуатации или замене входящего в ее состав оборудования осуществляется принудительное удаление информации с соответствующих машинных носителей и из памяти компьютеров за исключением ведущихся в установленном порядке контрольных архивов электронных документов.

9.3.4 *Антивирусная защита.* Антивирусная защита обеспечивается использованием в Университете специализированного программного обеспечения отечественного производителя.

Для снижения влияния человеческого фактора, исключения возможности отключения или отсутствия обновления антивирусных средств, контроль и управление антивирусным программным обеспечением, а также устранение выявленных уязвимостей в системном программном обеспечении производится централизованно в автоматизированном режиме. При этом обеспечивается минимально возможный период обновления.

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.

Каждый работник Университета обязан выполнять правила эксплуатации антивирусного ПО и требования антивирусной защиты в отношении внешних источников и носителей информации, а также сети Интернет, немедленно прекращать работу и информировать системного администратора и/или Администратора ИБ при подозрениях на вирусное заражение.

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

9.3.5 *Безопасное использование ресурсов сети Интернет.* Использование ресурсов сети Интернет в подразделениях Университета разрешается исключительно в производственных целях с применением необходимых меры для противодействия хакерским атакам и распространению спама.

Порядок публикации информации в сети Интернет определяется отдельными регламентами. Обсуждение работниками Университета на форумах и в конференциях сети Интернет вопросов, касающихся их служебной деятельности, допускается только при наличии соответствующих указаний руководства.

Использование рабочих станций с доступом к ресурсам сети Интернет для обработки критичной информации запрещается.

9.3.6 *Использование средств криптографической защиты информации.* Применение средств криптографической защиты информации для обеспечения безопасности информационных ресурсов Университета и взаимодействия со сторонними организациями производится в соответствии с порядком, установленным государственными уполномоченными органами.

Использование средств электронной подписи обеспечивает целостность электронного документа и подтверждение авторства подписавшей его стороны и является лучшей практикой организации электронного документооборота при взаимодействии с контрагентами. Криптографические ключи, предназначенные для защиты электронного документооборота Университета со сторонними организациями, изготавливаются сторонами самостоятельно.

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

Во внутренних системах Университета механизмы криптографического контроля целостности используются в зависимости от результатов оценки рисков информационной безопасности.

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

9.3.7 *Защита информационных технологических процессов.* Непрерывность критичных процессов при наступлении отказов и сбоев обеспечивается резервированием оборудования, каналов связи, резервным копированием информации, регулярной проверкой их работоспособности и адекватности. Процедуры восстановления после сбоев документируются в соответствующих регламентах и планах.

9.3.8 *Защита материальных носителей информации.* Помещения Университета категорируются в зависимости от критичности размещаемых в них хранилищ информационных ресурсов. В соответствии с категорией обеспечивается техническая укрепленность помещений, оснащение средствами видеоконтроля, контроля доступа, пожаротушения и сигнализации.

Ведется учет материальных носителей информации, содержащих информацию, подлежащей защите.

10. Защита персональных данных

10.1 Система защиты персональных данных (далее - СЗПДн) строится на основании:

- модели угроз и нарушителя;
- положения об обработке и защите персональных данных;
- нормативных документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн для каждой ИСПДн Университета. На основании анализа актуальных угроз безопасности ПДн, описанного в Модели актуальных угроз и нарушителя, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по внутреннему контролю за соблюдением безопасности персональных данных.

Организационные мероприятия должны включать:

- правовое основание для сбора персональных данных;

- определение ответственных лиц за соблюдением мер безопасности;
- защиту персональных данных, обрабатываемых без средств автоматизации;
- защиту персональных данных, обрабатываемых с применением средств автоматизации;
- защиту объектов от хищения;
- защиту съемных накопителей, содержащих персональные данные;
- вопросы уничтожения персональных данных.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- защиты от несанкционированного доступа к персональным данным;
- антивирусной защиты для рабочих станций пользователей и серверов;
- межсетевого экранирования;
- обнаружения вторжений;
- контроля защищенности персональных данных;
- криптографической защиты информации, при передаче защищаемой информации по каналам связи;
- защиты среды виртуализации;
- защиты от утечки по техническим каналам утечки информации.

10.2 СЗПДн может включать в себя следующие подсистемы:

Идентификация и аутентификация субъектов доступа и объектов доступа. Подсистема обеспечивает присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Управление доступом субъектов доступа к объектам доступа. Подсистема обеспечивает управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивает контроль за соблюдением этих правил.

Ограничение программной среды. Подсистема обеспечивает установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

Регистрация событий безопасности. Подсистема обеспечивает сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Антивирусная защиты. Подсистема обеспечивает обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной

для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Обнаружения (предотвращения) вторжений. Подсистема обеспечивает обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

Контроль (анализа) защищенности персональных данных. Подсистема обеспечивает контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

Обеспечение целостности информационной системы и персональных данных. Подсистема обеспечивает обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

Обеспечение доступности персональных данных. Подсистема обеспечивает авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

Защита среды виртуализации. Подсистема исключает несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Защита технических средств. Подсистема исключает несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, обеспечивает защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Защита информационной системы, ее средств, систем связи и передачи данных. Подсистема обеспечивает защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными

системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

Выявления инцидентов и реагированию на них. Подсистема обеспечивает обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

Управление конфигурацией информационной системы и системой защиты персональных данных. Подсистема обеспечивает управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

10.3 В ИСПДн Университета выделяют следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администраторы ИСПДн;
- администраторы ИБ;
- пользователи ИСПДн.

Администратором ИСПДн является штатный работник Университета или лица сторонних организаций, осуществляющих свои функции на основании двухстороннего договора. Администратор ИСПДн не имеет полномочий для управления подсистемами обеспечения безопасности.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

Администратором ИБ является штатный работник Университета, ответственный за функционирование СЗПДн, назначается приказом ректора.

Администратор ИБ обладает следующим уровнем доступа и знаний:

- обладает правами администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор ИБ уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИСПДн;

– осуществлять аудит средств защиты.

Пользователем ИСПДн является штатный работник Университета, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПДн. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

– располагает конфиденциальными данными, к которым имеет доступ.

11. Управление информационной безопасностью

11.1 Управление системой обеспечения информационной безопасности осуществляет руководство Университета:

– утверждение и пересмотр политики информационной безопасности Университета;

– организация процесса управления информационной безопасностью в Университете, включая определение подразделений, ответственных за управление отдельными процессами обеспечения информационной безопасности, утверждение положений о них;

– обеспечение условий и утверждение бюджета для эффективной реализации политики информационной безопасности;

– анализ отчетов о состоянии информационной безопасности Университета.

11.2 Все подразделения Университета и их руководители отвечают за реализацию политики информационной безопасности и управление процессами ее обеспечения в рамках своей компетенции.

11.3 В целях выполнения задач по обеспечению информационной безопасности, в соответствии с рекомендациями международных и российских стандартов по безопасности, обеспечения деятельности по реализации текущей политики ИБ в Университете, в соответствии с его уставными целями, (назначается ответственное лицо или функционирует подразделение), ответственное за обеспечение информационной безопасности – подразделение или ответственное лицо.

11.4 Подразделение или ответственное лицо:

– разрабатывает нормативные, инструктивные и методические документы Университета по обеспечению информационной безопасности;

– разрабатывает требования по защите информационных ресурсов в аспектах целостности и конфиденциальности на основе анализа рисков информационной безопасности;

– осуществляет контроль соответствия требованиям на всех стадиях жизненного цикла автоматизированных систем, от проектирования до снятия с эксплуатации;

– обеспечивает управление ключевыми системами средств криптографической защиты;

– организует проведение единой антивирусной политики в Университете;

– организует работу и осуществляет взаимодействие с администраторами автоматизированных информационных систем;

– проводит расследования инцидентов и фактов нарушений информационной безопасности и информирует руководство о результатах проведенного расследования;

– организует обучение персонала по вопросам информационной безопасности;

– осуществляет инструментальный контроль и мониторинг текущего состояния информационной безопасности;

– регулярно информирует руководство о состоянии информационной безопасности в Университете, в том числе, в составе сводных отчетов;

– обеспечивает взаимодействие с уполномоченными государственными органами по вопросам информационной безопасности;

– осуществляет анализ, оценку и прогноз риска, связанного с нарушением информационной безопасности Университета.

11.5 Подразделения, ответственные за обслуживание АИС, или администраторы АИС:

– обеспечивают выполнение требований информационной безопасности при подключении и администрировании коммуникационного оборудования, операционных систем, СУБД и систем доставки;

– проводят обновление системного ПО, связанное с устранением критичных уязвимостей;

– обеспечивают доступность информационных ресурсов в условиях отказов и других неблагоприятных событий в части коммуникационного оборудования, операционных систем, СУБД и систем доставки;

– обеспечивают выполнение требований информационной безопасности при администрировании автоматизированных информационных систем;

– обеспечивают хранение программной документации;

– осуществляют регистрацию информации об инцидентах, имеющих отношение к информационной безопасности.

– совместно с (подразделение, должностное лицо, ответственное за информационную безопасность) проводят категорирование информационных ресурсов, владельцами которых они являются, и определяют те из них, которые являются критичными;

– совместно с (подразделение, должностное лицо, ответственное за информационную безопасность) участвуют в оценке рисков реализации угроз их информационным ресурсам;

– устанавливают в пределах своей компетенции режим и порядок доступа, правила работы с информационными ресурсами, владельцами которых они являются;

– обеспечивают выполнение требований и процедур информационной безопасности при работе работников с информационными ресурсами Университета;

– обеспечивают учет в подразделении информационных ресурсов и работников, имеющих к ним доступ;

– обеспечивают инструктаж работников по вопросам информационной безопасности;

– обеспечивают контроль проведения антивирусных мероприятий в подразделении и соблюдения требований информационной безопасности;

– обеспечивают взаимодействие с (подразделение, должностное лицо ответственное за информационную безопасность) при инцидентах информационной безопасности.

12. Аудит и самооценка информационной безопасности

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

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

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

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

13. Ответственность

13.1 Все работники Университета несут ответственность за невыполнение требований настоящей политики.

13.2 Работники Университета, нарушающие требования информационной безопасности и руководители подразделений, не обеспечивающие их выполнение, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

13.3 Контроль за выполнением требований настоящей политики возлагается на руководство Университета, руководителей всех структурных подразделений Университета.

14. Изменения

14.1 Разработка и утверждение настоящей Политики производится в соответствии с ПЛ СМК НГУЭУ 7.5.3-003.01-2018 «Порядок разработки и внедрения нормативно-методической документации НГУЭУ».

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

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

14.4 Пересмотр Политики должен включать:

– проверку эффективности Политики, исходя из характера, числа и последствий зарегистрированных инцидентов нарушений ИБ;

– определение стоимости мероприятий по управлению информационной безопасностью и их влияние на эффективность по достижению уставных целей Университета;

– оценку влияния изменений в технологиях.

14.5 С момента утверждения Политики ректором Университета утрачивает силу предыдущая Политика информационной безопасности Университета.