	НИУ МГСУ **Информационно-вычислительный центр**	СК И ПВД 06 - 44 - 2019

УТВЕРЖДАЮ
Ректор НИУ МГСУ

_____ **А.А. Волков**

“20” 05 2019 г.

Ввести в действие с

“20” 05 2019 г.

АЛЬБОМ
внутренней организационно-распорядительной документации в области обработки и защиты персональных данных

Выпуск 3

МОСКВА 2019г.

Оглавление

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящий Альбом внутренней организационно-распорядительной документации в области обработки и защиты персональных данных (далее – Альбом) в Федеральном государственном бюджетном образовательном учреждении высшего образования "Национальный исследовательский Московский государственный строительный университет" (далее – оператор, НИУ МГСУ) предназначен для ознакомления с основными принципами сбора, обработки, хранения, передачи и защиты персональных данных физических лиц (далее – субъекты персональных данных), которые реализуются в НИУ МГСУ.

1.2 Настоящий Альбом выпускается во исполнение действующих нормативно-правовых актов Российской Федерации в области защиты информации и персональных данных и предназначен для использования следующим кругом лиц:

- работники НИУ МГСУ, допущенные к обработке персональных данных;
- работники НИУ МГСУ, ответственные за защиту персональных данных;
- администраторы НИУ МГСУ, ответственные за работу информационных систем по обработке персональных данных.

1.3 Настоящий Альбом вступает в силу с момента его утверждения ректором университета и действует бессрочно, до замены его новым Альбомом. Все изменения вносятся приказом ректора.

1.4 Все работники, допущенные к обработке персональных данных, должны быть ознакомлены с настоящим Альбомом под подпись.

2. НОРМАТИВНЫЕ ССЫЛКИ

2.1 Настоящий Альбом разработан в соответствии с требованиями следующих нормативно-правовых документов в области защиты информации и персональных данных:

- Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018) «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) «О персональных данных»;
- Постановление Правительства РФ от 6 июля 2008 г. № 512 (ред. от 27.12.2012) й «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Роскомнадзора от 05.09.2013г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- Приказ Роскомнадзора от 15.03.2013 N 274 (ред. от 14.01.2019) «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

3. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

3.1 Под персональными данными (ПДн), обрабатываемыми в Университете, понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), позволяющая идентифицировать его личность, в том числе: его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, а также сведения о фактах, событиях и обстоятельствах жизни работника, обучающегося и/или иного субъекта персональных данных.

3.2 Оператором персональных данных является Университет, самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

3.3 Ответственный за защиту персональных данных Университета – уполномоченное лицо, назначенное приказом ректора Университета, отвечающий за работу оператора персональных данных.

3.4 Ответственный за организацию обработки персональных данных в структурном подразделении Университета – уполномоченное лицо, назначаемое руководителем подразделения и утверждаемое приказом ректора Университета или распоряжением курирующего вопросы обработки и защиты ПДн проректора, отвечающее за обработку персональных данных в структурном подразделении.

3.5 Администратор информационных систем персональных данных – уполномоченное лицо, назначаемое приказом ректора Университета, отвечающее за процесс функционирования работы информационной системы персональных данных, а также за разграничение прав доступа работников к обрабатываемым персональным данным.

3.6 Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с персональными данными, с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.7 Автоматизированная обработка персональных данных – обработка персональных данных с использованием средств автоматизации, включающих в себя автоматизированные рабочие места, а также средства информационных систем персональных данных.

3.8 Неавтоматизированная обработка персональных данных – обработка персональных данных, осуществляемая при непосредственном участии человека без использования средств автоматизации.

3.9 Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

3.10 Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

3.11 Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения персональных данных).

3.12 Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных.

3.13 Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных к конкретному субъекту персональных данных.

3.14 Информационная система персональных данных (ИСПДн) – совокупность персональных данных, содержащихся в базах данных и обеспечивающих их автоматизированную обработку информационных технологий и технических средств.

3.15 Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

3.16 Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

3.17 Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым представлен с согласия субъекта персональных данных или на которые в соответствии с Федеральными законами не распространяются требования конфиденциальности. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектами персональных данных в качестве общедоступных. Данные сведения могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных, по решению суда или уполномоченных государственных органов.

3.18 Конфиденциальность персональных данных – обязательное для соблюдения Университетом или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

3.19 Трансграничная передача персональных данных – передача персональных данных субъекта персональных данных Университета на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3.20 Обработка персональных данных в Университете ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.21 Субъекты персональных данных в Университете разделяются на несколько категорий:

- работники (кандидаты) – физические лица, претендующие на замещение вакантных должностей, работники, состоящие с Университетом в трудовых отношениях, в том числе работающие в Университете по совместительству (далее по тексту – работники), вступившие в трудовые отношения с работодателем;
- обучаемые – физические лица всех категорий, участники образовательной деятельности Университета: поступающие, студенты всех форм обучения (бакалавриат, специалитет, магистратура), выпускники, аспиранты, докторанты, соискатели, слушатели курсов повышения квалификации, дополнительных образовательных программ и др., пользующиеся или пользовавшиеся услугами Университета, или подавшие в Университет заявление о намерении пользования услугами лица;
- контрагенты – физические лица и лица, являющиеся представителями юридических лиц, с которыми заключаются договорные отношения;
- посетители – физические лица, не являющиеся работниками или обучаемыми, осуществляющие посещение территории Университета на разовой или временной основе.

3.22 Безопасность информации – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность при ее обработке техническими средствами.

3.23 Защита персональных данных – действия, направленные на предотвращение и пресечение несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать несанкционированное уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также предотвращение иных несанкционированных действий в отношении персональных данных.

3.24 Код АРМ – присвоенный идентификатор каждому автоматизированному рабочему месту индивидуально согласно реестру АРМ, допущенных к обработке персональных данных.

4. СОДЕРЖАТЕЛЬНАЯ ЧАСТЬ

Положение об обработке и защите персональных данных в Федеральном государственном бюджетном образовательном учреждении высшего образования «Национальный исследовательский Московский государственный строительный университет» (НИУ МГСУ)

1. Назначение и область применения

1.1. Настоящее Положение об обработке и защите персональных данных в НИУ МГСУ (далее по тексту – Положение) разработано в соответствии с действующими нормативно-правовыми актами Российской Федерации в области обработки и защиты персональных данных.

1.2. Настоящим Положением определяется порядок использования персональных данных, обрабатываемых в НИУ МГСУ (далее по тексту – Университет), цели обработки персональных данных, состав персональных данных, подлежащих обработке, а также процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

1.3. Действие настоящего Положения распространяется на все процессы по сбору, записи, систематизации, накоплению, хранению, уточнению, извлечению, использованию, передаче (распространению, предоставлению, доступу), обезличиванию, блокированию, удалению, уничтожению персональных данных, осуществляемых как с использованием средств автоматизации, так и без использования таких средств.

1.4. Целью настоящего Положения является защита персональных данных, обрабатываемых в Университете от несанкционированного доступа и разглашения. Персональные данные, обрабатываемые в Университете, являются конфиденциальной, строго охраняемой информацией.

1.5. Режим конфиденциальности персональных данных снимается в случаях их обезличивания или по истечении сроков их обработки, или продлевается на основании заключения экспертной комиссии Университета, если иное не определено законом.

2. Цели и задачи обработки персональных данных

2.1. Цели обработки персональных данных в Университете определяются исходя из правовых актов, регламентирующих деятельность Университета, целей фактически осуществляемой Университетом деятельности, а также деятельности, которая предусмотрена учредительными документами Университета.

2.2. Персональные данные субъектов персональных данных обрабатываются в Университете для выполнения ряда целей:

- соблюдение федеральных законов и иных нормативных правовых актов Российской Федерации по направлениям деятельности;
- содействие субъектам персональных данных в осуществлении трудовой деятельности;
- содействие субъектам персональных данных в осуществлении образовательной деятельности;
- учет результатов исполнения договорных обязательств;
- обеспечение социальными льготами в соответствии с законодательством Российской Федерации и нормативными документами Университета;
- обеспечение личной безопасности в период работы и/или обучения;
- обеспечение соблюдения правил приема в соответствии с законодательством и нормативными документами Университета;
- гласности и открытости деятельности приемной комиссии;
- содействие субъекту персональных данных в издательской деятельности научных трудов и других материалов;
- размещение персональных данных на сайтах Университета;
- осуществление деятельности структурных подразделений Университета;
- сбор персональных данных посредством интернет-сервисов, функционирующих на сайтах Университета и т.д.

2.3. Основные задачи обработки персональных данных в Университете определяются исходя из целей обработки персональных данных Университета:

– выполнение требований федеральных законов и иных нормативных правовых актов Российской Федерации по направлениям деятельности;

– исполнение договоров, одной из сторон которого является субъект персональных данных или контрагент;

– учет информации об обучающихся в Университете и информации о движении контингента обучающихся;

– формирование отчетов по Университету;

– назначение и начисление стипендий и иных выплат;

– обработка данных приемных кампаний Университета, учет личных данных поступающих, обработка результатов вступительных испытаний;

– обработка личных дел и индивидуальных планов аспирантов, соискателей и докторантов, анализ деятельности по подготовке и аттестации научных и научно-педагогических кадров;

– комплексный мониторинг деятельности Университета, мониторинг качества учебного процесса;

– бухгалтерский учет и контроль финансово-хозяйственной деятельности Университета и исполнения финансовых обязательств по заключенным договорам;

– обработка электронных библиотечных карт и читательских билетов, обеспечение учета книговыдачи;

– предоставление субъекту сведений о его обучении в Университете в период обучения и после него;

– предоставление и контроль доступа посетителей на территории Университета;

– рассмотрение кандидатур на вакантные должности или для предоставления возможности получения ученой степени;

– иные задачи, необходимые для повышения качества и эффективности образовательной деятельности.

3. Объем и категории обрабатываемых персональных данных

3.1. Содержание и объем обрабатываемых персональных данных в Университете соответствует целям обработки. Обрабатываемые в Университете персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3.2. Университет, как оператор персональных данных, обязан сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных, и получить от субъекта персональных данных согласие на их обработку

3.3. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его законным представителем в любой позволяющей подтвердить факт его получения форме.

3.4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного квалифицированной электронной подписью.

3.5. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

– фамилию, имя, отчество (при наличии), адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– фамилию, имя, отчество (при наличии), адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

– наименование и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

– срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

– подпись субъекта персональных данных.

3.6. В форме электронного документа согласия субъекта персональных данных на обработку его персональных данных оформляется по аналогичной форме согласия и заверяется квалифицированной электронной подписью.

3.7. В случае отказа субъекта персональных данных дать согласие на обработку персональных данных, ему доводится разъяснение юридических последствий отказа предоставить свои персональные данные на обработку.

3.8. В зависимости от субъектов персональных данных в Университете обрабатываются и дополнительные персональные данные, необходимые для исполнения целей обработки персональных данных. Состав таких персональных данных включат в себя:

– фамилия, имя, отчество;

– дата рождения;

– гражданство;

– номер страхового свидетельства;

– ИНН;

– данные об образовании (реквизиты дипломов/иных документов);

– данные о приобретенных специальностях;

– семейное положение;

– данные о членах семьи (степень родства, Ф. И. О., год рождения, паспортные данные, включая прописку и место рождения);

– фактическое место проживания;

– контактная информация;

– данные о военной обязанности;

– данные о текущей трудовой деятельности (дата начала трудовой деятельности, кадровые перемещения, оклады и их изменения, сведения о поощрениях, данные о повышении квалификации и т. п.);

– номера телефонов родственников для связи в экстренных случаях;

– сведения об отношении к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);

– сведения о факте судимости (отсутствии судимости (или) о погашенной (снятой) судимости);

– другие сведения в зависимости от категории субъектов персональных данных Университета в соответствии с настоящим Положением.

3.9. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных либо его законным представителем. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Университет должен немедленно остановить обработку персональных данных субъекта.

4. Сбор и обработка персональных данных

4.1. Всю информацию о персональных данных субъект персональных данных предоставляет самостоятельно. субъект персональных данных предоставляет Университету достоверные сведения о себе. Университет проверяет достоверность сведений, сверяя данные предоставленные субъектом персональных данных, с имеющимися у него документами.

4.2. Если персональные данные субъекта персональных данных возможно получить только у третьей стороны, то он должен быть уведомлен об этом заранее.

4.3. В случае недееспособности субъекта персональных данных Согласие на обработку его персональных данных в письменной форме дает его законный представитель.

4.4. Персональные данные субъекта подлежат сбору и обработке только на законных основаниях согласно статье 9 «Согласие субъекта персональных данных на обработку его персональных данных» Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) «О персональных данных», только после предоставления субъектом согласия на обработку в бумажном либо в электронном виде.

4.5. При обработке персональных данных должны соблюдаться следующие принципы:

– обработка персональных данных осуществляется на законной и справедливой основе;

– Университет не получает и не обрабатывает персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, Университет вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

– получение информации о здоровье работника производится только в объеме, необходимом для определения возможности выполнения работником трудовых обязанностей;

– обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

– не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только персональные данные, которые отвечают целям их обработки;

– содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки;

– при обработке персональных данных обеспечена точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор принимает необходимые меры по удалению или уточнению неполных или неточных данных;

– хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.6. Обработка персональных данных допускается в следующих случаях:

– обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

– обработка персональных данных необходима для достижения целей;

– обработка персональных данных необходима для исполнения договорных отношений;

– обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

– обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных;

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации.

4.7. Сбор и обработка персональных данных осуществляется при условии наличия согласия субъекта персональных данных. Персональные данные, необходимые для выполнения целей Университета по обработке персональных данных, предоставляются субъектом персональных данных лично либо законным представителем.

4.8. Исключение составляют случаи, когда в соответствии с действующим законодательством допускается обработка персональных данных без получения согласия субъекта, а именно:

– обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

– обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

– обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект, а также для заключения договора по инициативе субъекта или договора, по которому субъект будет являться выгодоприобретателем или поручителем;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта невозможно;

– обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

– обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

– обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

– обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных. Исключение составляет обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;

– осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных, либо по его просьбе;

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

5. Виды обработки персональных данных

5.1. Обработка персональных данных в Университете осуществляется как с использованием средств автоматизации, так и без использования таких средств.

5.2. При обработке персональных данных в Университете, осуществляемой без использования средств автоматизации, должны соблюдаться требования Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008г. № 687.

5.3. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях, в специальных разделах и т.п.

5.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

– указание сведений о цели обработки, сведений об операторе по обработке персональных данных, ФИО и адреса субъекта персональных данных, источника получения данных, сроках обработки;

– наличие поля, предназначенного для отметки субъекта персональных данных о своем согласии на предоставление сведений конфиденциального характера оператору и/или наличие согласие на обработку персональных данных в бумажном виде;

– реализация возможности ознакомления субъекта персональных данных со своими персональными данными, при этом, важно, чтобы у такого субъекта не было доступа к персональным данных других субъектов;

– отсутствие объединенных полей для данных, собранных с разными целями.

5.5. При ведении журнала с персональными данными для организации однократных пропусков субъектов на территорию Университета следует выполнять определенные условия:

– разработать акт, в котором указать цели, способы, сроки работы с персональными данными и перечень допущенных лиц, имеющих доступ;

– заносить данные так, чтобы обезопасить персональные данные субъектов;

– не копировать их без весомых на то причин и только при уведомлении ответственного за обработку в структурном подразделении.

5.6. Не допускается распространение материального носителя, если планируется использовать только часть сведений. В таком случае оператор копирует нужную часть и обеспечивает конфиденциальность неиспользуемых данных.

5.7. Информационные системы и автоматизированные рабочие места, входящие в состав ИСПДн по обработке персональных данных, содержат персональные данные, указанные в настоящем Положении, а также иные необходимые данные для выполнений целей и задач.

5.8. Работникам, имеющим право осуществлять обработку персональных данных, предоставляются автоматизированные рабочие места и доступ к информационным системам (при необходимости), к которым контролируется доступ по уникальным логинам и паролям.

5.9. Персональные данные вносятся в информационные системы как в автоматическом, так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

6. Доступ работников к персональным данным, обрабатываемым в Университете

6.1. Доступ к персональным данным, обрабатываемым в Университете, работникам, не допущенным к обработке таких данных, запрещается.

6.2. Нахождение лиц, не являющихся работниками, допущенных к обработке персональных данных, в помещениях, в которых ведется обработка персональных данных, возможно только в присутствии работника, допущенного к обработке персональных данных.

6.3. Работники Университета получают доступ к персональным данным субъектов персональных данным исключительно в объеме, необходимом для выполнения своих должностных обязанностей.

6.4. Для получения доступа к персональным данным работнику Университета необходимо обратится к ответственному за обработку персональных данных в данном структурном подразделения Университета.

6.5. Работник Университета получает доступ к персональным данным субъектов персональных данных после ознакомления и изучения требований настоящего Положения и иных внутренних нормативных документов Университета по защите персональных данных и выполнений действий ответственного по защите информации в структурном подразделении Университета.

6.6. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, контроль за действиями допущенных работников к обработке персональных данных, учет и контроль автоматизированных рабочих мест по обработке персональных данных возлагается на ответственного за обработку персональных данных, назначенным внутреннем приказом.

7. Передача персональных данных

7.1. При передаче персональных данных субъекта персональных данных Университет должен соблюдать следующие требования:

- не сообщать персональные данные субъекта персональных данных третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных законодательством Российской Федерации;
- не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные субъекта персональных данных, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это право соблюдено;
- лица, получающие персональные данные субъекта персональных данных, обязаны соблюдать конфиденциальность;

– не запрашивать информацию о состоянии здоровья субъекта персональных данных, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции, обучающимся – учебы, лицом, нуждающимся в медицинской помощи или получающим (получившим) медицинскую помощь и др.

7.2. Передача (обмен и т.д.) персональных данных между отделами (структурными подразделениями) Университета осуществляется только между работниками, имеющими доступ к персональным данным субъектов.

7.3. Передача информации, содержащей сведения о персональных данных субъектов персональных данных, по телекоммуникационным сетям без их письменного согласия запрещается.

7.4. При передаче персональных данных субъекта работники, осуществляющие передачу, предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они передаются.

7.5. Трансграничная передача персональных данных может осуществляться в соответствии с требованиями законодательства Российской Федерации на территорию иностранных государств согласно списку утвержденных таких государств в приказе Роскомнадзора от 15.03.2013 N 274 (ред. от 14.01.2019) «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных», для обеспечивающих адекватную защиту прав субъектов персональных данных:

– Австралия - Австралийский союз;
– Аргентинская Республика;
– Габонская Республика;
– Государство Израиль;
– Государство Катар;
– Канада;
– Королевство Марокко;
– Малайзия;
– Мексиканские Соединенные Штаты;
– Монголия;
– Новая Зеландия;
– Республика Ангола;
– Республика Бенин;
– Республика Кабо-Верде;
– Республика Казахстан;
– Республика Коста-Рика;
– Республика Корея;
– Республика Мали;
– Республика Перу;
– Республика Сингапур;
– Тунисская Республика;
– Республика Чили;
– Южно-Африканская Республика.

7.6. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

– наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу;

– предусмотренных международными договорами Российской Федерации;

– предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

– исполнения договора, стороной которого является субъект персональных данных;

– защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта.

7.7. К числу внешних потребителей персональных данных Университета в соответствии с нормами действующего законодательства относятся, в частности, следующие государственные органы:

– налоговые органы;

– правоохранительные органы;

– военкоматы;

– органы социального страхования;

– пенсионные фонды;

– подразделения муниципальных органов управления;

– судебные органы.

7.8. При передаче персональных данных субъекта уполномоченные лица должны придерживаться следующих требований:

– передача персональных данных субъекта третьим лицам осуществляется только с письменного согласия субъекта, за исключением случаев, установленных федеральными законами;

– не допускается передача персональных данных субъекта в коммерческих целях без его письменного согласия;

– передача персональных данных по телефону запрещается;

– работникам Университета, допущенные к обработке персональных данных, запрещена запись, хранение и вынос за пределы контролируемой зоны обработки персональных данных Университета на внешних носителях, передача по внешним адресам электронной почты или размещение в сети Интернет информации, содержащей персональные данные субъектов, за исключением случаев, установленных иными внутренними локальными актами и/или документами Университета;

– передача третьим лицам документов (иных материальных носителей), содержащих персональные данные субъектов, осуществляется по письменному запросу третьего лица на предоставление персональных данных субъекта. Ответы на письменные запросы даются на бланке Университета и в том объеме, который позволяет не разглашать излишних сведений о субъекте персональных данных в порядке, установленном действующим законодательством;

– работники Университета, передающие персональные данные субъектов третьим лицам, должны передавать их с обязательным уведомлением лица, получающего эти документы, об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она передается, и с предупреждением об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральными законами. Уведомление и предупреждение могут быть реализованы путем подписания Акта/договора передачи носителей персональных данных, в котором приведены указанные условия.

7.9. Представителю субъекта персональные данные передаются в порядке, установленном действующим законодательством и настоящим Положением. Информация передается при наличии одного из документов:

– нотариально удостоверенной доверенности представителя субъекта;

– письменного заявления субъекта, написанного в присутствии уполномоченного работника Университета (если заявление написано субъектом не в его присутствии, то оно должно быть нотариально заверено).

7.10. Предоставление персональных данных субъекта государственным органам производится в соответствии с требованиями действующего законодательства Российской Федерации.

7.11. Персональные данные субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта, за исключением случаев, когда передача персональных данных субъекта без его согласия допускается действующим законодательством Российской Федерации.

7.12. Документы, содержащие персональные данные субъекта, могут быть отправлены посредством федеральной почтовой связи заказным письмом. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие персональные данные, вкладываются в конверт, в документах делается надпись о том, что персональные данные, содержащиеся в письме, являются конфиденциальной информацией и не подлежат распространению и (или) опубликованию. Лица, виновные в нарушении требований конфиденциальности, несут ответственность, предусмотренную законодательством Российской Федерации.

7.13. Учет переданных персональных данных осуществляется в рамках принятых в Университете правил делопроизводства путем регистрации входящей и исходящей корреспонденции и запросов.

7.14. В случае, если лицо, обратившееся в Университет с запросом на предоставление персональных данных, не уполномочено на получение информации, относящейся к персональным данным, уполномоченные лица Университета обязаны отказать данному лицу в выдаче такой информации. Лицу, обратившемуся с соответствующим запросом, выдается уведомление в свободной форме об отказе в выдаче информации, а копия уведомления хранится в соответствии с принятыми правилами делопроизводства (как исходящая корреспонденция).

8. Обезличивание персональных данных

8.1. Данная процедура обеспечивает не только защиту от несанкционированного использования, но и сохраняет возможность обработки персональных данных.

8.2. При осуществлении процедуры обезличивания учитываются следующие требования к методам обезличивания:

– требования к свойствам обезличенных персональных данных, получаемых при применении метода обезличивания;

– требования к свойствам, которыми должен обладать метод обезличивания.

8.3. При обезличивании должны быть реализованы следующие требования к свойствам, получаемых обезличенных персональных данных:

– сохранение полноты;

– сохранение структурированности обезличиваемых персональных данных;

– сохранение семантической целостности обезличиваемых персональных данных;

– анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений, обезличенных персональных данных между собой для деобезличивания).

8.4. При обезличивании должны быть реализованы следующие требования к свойствам метода обезличивания:

– обратимость (возможность проведения деобезличивания);

– возможность обеспечения заданного уровня анонимности;

– увеличение стойкости при увеличении объема обезличиваемых персональных данных.

8.5. В зависимости от необходимости Университет применяет один из 4-х методов обезличивания, каждый их которых соответствует вышеперечисленным требованиям:

– метод введения идентификаторов (замена части значений персональных данных идентификаторами с созданием таблицы соответствия последних исходным данным);

– метод изменения состава или семантики (замена результатами статистической обработки, обобщения или удаления части сведений);

– метод декомпозиции (разбиение множества персональных данных на несколько подмножеств с последующим раздельным хранением подмножеств);

– метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

9. Сроки обработки и порядок хранения персональных данных

9.1. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют соответствующие цели обработки персональных данных в соответствии с законодательством Российской Федерации.

9.2. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки, или в случае утраты необходимости в достижении этих целей.

9.3. Персональные данные субъектов могут обрабатываться, хранится и передаваться как на бумажных носителях, так и в электронном виде.

9.4. Персональные данные на бумажных носителях хранятся в запираемых шкафах или сейфах структурных подразделений, осуществляющих обработку персональных данных, и специализированных помещениях архива Университета.

9.5. Персональные данные субъектов в электронном виде обрабатываются на автоматизированных рабочих станциях и в информационных системах по обработке таких данных.

9.6. Доступ работников к персональным данным, обрабатываемым в Университете, осуществляется только допущенными к обработке.

9.7. Должно обеспечиваться раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящим Положением.

9.8. Контроль за хранением и использованием материальных носителей, содержащих персональные данные, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют непосредственные ответственные за обработку персональных данных в структурных подразделениях.

10. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

10.1. В случае достижения цели обработки персональных данных Университет обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Университетом и субъектом персональных данных, либо если Университет не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

10.2. В случае отзыва субъектом персональных данных согласие на обработку своих персональных данных Университет не вправе осуществлять обработку персональных данных без

согласия субъекта, если только Университет осуществляет обработку персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

10.3. В случае выявления неправомерной обработки персональных данных Университет предпринимает меры по уничтожению этих данных в срок, не превышающий семи рабочих дней со дня выявления неправомерной обработки.

10.4. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока Университет осуществляет блокирование таких данных и обеспечивает уничтожение в срок, не превышающий 6 месяцев со дня выявления неправомерной обработки, если иной срок не установлен федеральным законодательством.

10.5. В случае, если уничтожение персональных данных было произведено по результатам обработки обращения субъекта персональных данных и (или) запроса уполномоченного органа по защите прав субъектов, о предпринятых действиях Университета уведомляет субъекта персональных данных и (или) уполномоченный орган по защите прав субъектов.

10.6. Уничтожение ПДн производится в соответствии с актуальными внутренними процессами Университета.

10.7. Лицами, ответственными за архивную обработку документов в Университете, осуществляется систематический контроль за выделением документов на бумажных носителях, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

10.8. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (например, вымарыванием).

10.9. Уничтожение бумажных носителей персональных данных осуществляется механическим способом (шредирование).

10.10. Уничтожение персональных данных, не подлежащих архивному хранению, осуществляется только комиссией в составе ответственного за защиту персональных данных и представителя структурного подразделения, в чьем ведении находятся указанные персональные данные. По результатам уничтожения оформляется Акт.

10.11. Уничтожение персональных данных на электронных носителях осуществляется с помощью удаления файлов, содержащих персональные данные, без физического уничтожения носителя, например, путем стирания информации с использованием сертифицированного программного обеспечения с гарантированным уничтожением. По результатам уничтожения оформляется Акт.

11. Защита персональных данных

11.1. В целях обеспечения сохранности и конфиденциальности персональных данных субъектов персональных данных Университета все операции по обработке данной информации должны выполняться только работниками, допущенными к обработке персональных данных Университета, осуществляющими данную работу в соответствии со своими должностными обязанностями, и подписавшими «Обязательство о неразглашении персональных данных».

11.2. Университет, как оператор персональных данных при обработке персональных данных, обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

11.3. Обеспечение безопасности персональных данных достигается путем решения некоторых задач в частности:

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием необходимых мер;

– установлением правил доступа к персональным данным, обрабатываемых в информационных системах, а также обеспечением регистрации доступа к данным;

– контролем за принимаемыми мерами по обеспечению безопасности и уровнем защищенности.

11.4. Для обеспечения защищенности персональных данных субъектов персональных данных в Университете соблюдается ряд мер:

– ограничение и регламентация состава работников, функциональные обязанности которых требуют обработку персональных данных;

– строгий контроль ответственного по обработке персональных данных в структурном подразделении и ознакомление работников, допущенных к обработке с регламентирующими документами по работе с персональными данными;

– знание работником требований регламентирующих документов по работе с персональными данными;

– рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации и считывание с мониторов;

– разграничение прав допуска к персональным данным субъектов персональных данных;

– организация порядка уничтожения информации;

– пропускной режим Университета;

– оснащение помещений техническими средствами охраны и сигнализации (в случае необходимости).

11.5. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Университета.

12. Обязанности Университета по обработке персональных данных

12.1. Обязанности Университета при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

– обязан в порядке, предусмотренном статьей 14 Федерального закона № 152 - ФЗ от 27 июля 2006г. «О персональных данных», сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, предоставить возможность ознакомления с ними, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые

относятся к субъекту персональных данных и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

12.2. Обязанности Университета по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных:

– в случае выявления недостоверных персональных данных субъекта персональных данных или неправомерных действий с ними, при обращении или по запросу субъекта (работника, и/или обучающегося и др.) или его законного представителя, либо уполномоченного органа по защите прав персональных данных субъекта, оператор обязан осуществить блокирование персональных данных, относящихся к субъектам персональных данных, с момента такого обращения или получения такого запроса на период проверки;

– в случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъект персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных - также в указанный орган.

12.3. Защита персональных данных субъекта персональных данных от неправомерного их использования или утраты должна быть обеспечена Университетом за счет своих средств.

12.4. Субъект персональных данных или его представитель должны быть ознакомлены с документами Университета, устанавливающими порядок обработки персональных данных субъектов персональных данных, а также об их правах и обязанностях в этой области.

13. Обязанности и права субъекта персональных данных

13.1. Субъект персональных данных обязан:

– передавать Университету комплект достоверных документированных персональных данных;

– своевременно в срок, не превышающий одного месяца, сообщать Университету об изменении своих персональных данных.

13.2. Субъект персональных данных имеет право:

– на полную информацию о своих персональных данных и обработке этих данных;

– на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации;

– требовать исключения, исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований закона, их блокирования, уничтожения;

– обжаловать неправомерные действия Университета при обработке и защите персональных данных.

13.3. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

13.4. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю Университетом при обращении либо получении запроса или его законного представителя.

13.5. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании законодательства Российской Федерации;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством Российской Федерации;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- фамилию, имя, отчество и место нахождения лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные законодательством Российской Федерации.

13.6. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

- обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекта персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

14. Рассмотрение запросов субъектов персональных данных или их представителей. Доступ субъектов персональных данных к персональным данным, обрабатываемым в Университете

14.1. Субъект персональных данных в соответствии с частью 1 статьи 14 Федерального закона «О персональных данных» вправе обращаться к руководству Университета с требованием

об уточнении его персональных данных, о блокировании или уничтожении персональных данных в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

14.2. Сведения, касающиеся обработки персональных данных, предоставляются субъекту персональных данных в доступной форме. В таких сведениях не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

14.3. Сведения, касающиеся обработки персональных данных, предоставляются по письменному запросу субъекта персональных данных или его законного представителя. Запрос должен содержать:

– номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

– сведения, подтверждающие участие субъекта персональных данных в правоотношениях с Университетом, либо сведения, иным образом подтверждающие факт обработки персональных данных в Университете, подпись заинтересованного субъекта персональных данных или его представителя.

14.4. К запросу, направленному представителем субъекта персональных данных, должен прилагаться документ (надлежащим образом заверенная копия), подтверждающий его полномочия.

14.5. Субъект персональных данных имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей его персональные данные. субъект персональных данных имеет право вносить предложения по внесению изменений в свои персональные данные в случае обнаружения в них неточностей.

14.6. Университет обязан сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя не позднее тридцати рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

14.7. Ответ в адрес субъекта персональных данных может быть направлен через отделение почтовой связи заказным письмом с уведомлением о вручении.

14.8. В случае отказа в предоставлении субъекту персональных данных или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя информации о наличии персональных данных о соответствующем субъекте персональных данных, Университет обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати рабочих дней со дня обращения субъекта персональных данных или его законного представителя, либо с даты получения запроса субъекта персональных данных или его законного представителя.

14.9. Мотивированный ответ в адрес субъекта персональных данных может быть направлен через отделение почтовой связи заказным письмом с уведомлением о вручении.

14.10. Субъект персональных данных вправе обратиться повторно к руководству Университета или направить повторный запрос в целях получения сведений, касающихся обработки персональных данных, а также в целях ознакомления с обрабатываемыми персональными данными до истечения указанного срока в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

14.11. Субъекту персональных данных может быть отказано в выполнении повторного запроса, не соответствующего установленным требованиям. Такой отказ должен быть мотивированным.

14.12. Право субъекта персональных данных на доступ к его персональным данным ограничено в соответствии с пунктами 3 и 4 части 8 статьи 14 Федерального закона «О персональных данных», если обработка его персональных данных в Университете осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, а также, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

15. Внутренний контроль соответствия обработки персональных данных в Университете установленным требованиям

15.1. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных проводится в целях выявления и предотвращения нарушений законодательства Российской Федерации в области персональных данных и выполнения регламентирующих действий согласно данному Положению и внутренним нормативным документам в области защиты информации.

15.2. Внутренний контроль осуществляется соответствующей комиссией, назначенной приказом Ректора Университета, совместно с ответственным за обработку персональных данных в проверяемом структурном подразделение Университета.

15.3. Внутренний контроль подразделяется на плановый и внеплановый.

15.4. Плановый внутренний контроль проводится на основании плана, утвержденного ректором Университета и ответственным за обработку персональных данных по Университету. Периодичность планового контроля - не реже одного раза в год. Срок проведения планового внутреннего контроля составляет от 20 рабочих дней.

15.5. Внеплановый контроль проводится по решению лица, ответственного за защиту персональных данных по Университету, на основании поступившего письменного или устного обращения от субъекта персональных данных о нарушении законодательства в области персональных данных либо от структурных подразделений. Внеплановый внутренний контроль должен быть завершен не позднее 10 дней со дня принятия решения о его проведении.

15.6. Результаты внутреннего контроля оформляются в виде актов и отчета по проведению проверки.

15.7. При выявлении в ходе внутреннего контроля нарушений в акте отражаются перечень нарушений. В отчете отображаются необходимые корректирующие действия по устранению нарушений в соответствующие сроки.

15.8. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, ответственному за защиту персональных данных Университета докладывает член комиссии и предоставляет оригинал (копию) акта и отчета о проведенной проверке.

16. Ответственность за разглашение информации, связанной с персональными данными

16.1. Ответственный за защиту по Университету в целом несет ответственность за:

– соблюдение работниками Университета, имеющими доступ к персональным данным, законодательства Российской Федерации, в том числе требований к защите персональных данных, нормативных правовых актов по вопросам обработки персональных данных и внутренних документов данной области;

– контроль за работой ответственных за защиту информации в структурных подразделениях Университета;

– поддержание достигнутого уровня защиты персональных данных и их ресурсов на этапах эксплуатации.

16.2. Ответственные за защиту персональных данных в структурных подразделениях Университета несут ответственность за:

– ознакомление работниками, производящих обработку персональных данных, с внутренней нормативной документацией под роспись, регламентирующей обработку;

– надлежащий контроль за соблюдением работниками требований в области персональных данных;

– контроль предоставления доступа работников к персональным данным, обрабатывающихся в Университете, в соответствии с установленным порядком;

– контроль предоставления доступа только работникам, подписавшим Обязательство о неразглашении персональных данных;

– ведение журналов учета электронных носителей и мест хранения материальных носителей персональных данных, составление Актов об уничтожении персональных данных;

– приостановление возможности доступа работникам Университета, в случае нарушения ими требований внутренних нормативных документов в области защиты персональных данных либо законодательства Российской Федерации.

16.3. Администраторы информационных систем по обработке персональных данных несут ответственность за:

– обеспечение устойчивой работоспособности и информационной безопасности информационных систем при обработке персональных данных;

– проведение периодического контроля принятых мер по защите и обеспечению работоспособности и информационной безопасности в информационной системе.

16.4. Администраторы средств защиты персональных данных несут ответственность за:

– организацию работ по обеспечению безопасности персональных данных, обрабатываемых, передаваемых и хранимых при помощи автоматизированных рабочих мест в информационных системах;

– правильность использования и нормального функционирования средств защиты информации;

– контроль за работниками, ответственными по вопросам работы автоматизированных рабочих мест и настройке средств защиты информации на данных местах.

16.5. Работники, допущенные к обработке персональных данных, несут ответственность за:

– знание и выполнение требования действующих Федеральных законов и внутренней нормативной документации Университета в области защиты персональных данных;

– осуществление только тех операций с персональными данными, которые необходимы для выполнения должностных обязанностей;

– своевременное оповещение Администратора информационных систем по обработке персональных данных и ответственного за защиту персональных данных в структурном подразделении обо всех нарушениях, связанных с обработкой персональных данных.

– своевременное оповещение Администратора средств защиты персональных данных и ответственного за защиту персональных данных в структурном подразделении обо всех проблемах, связанных со средствами защиты информации и автоматизированных рабочих мест по обработке персональных данных.

16.6. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, обрабатываемых в Университете, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

16.7. Работник, которому в силу трудовых отношений с Университетом стала известна информация, составляющая персональные данные, в случае нарушения режима защиты этих персональных данных несет материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами Российской Федерации.

16.8. Разглашение персональных данных субъектов персональных данных (передача их посторонним лицам, в том числе работникам Университета, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативными актами (приказами, распоряжениями) Университета, может повлечь наложение на работника, имеющего доступ к персональным данным, дисциплинарного взыскания, если иное не предусмотрено законодательством РФ.

17. Заключительные положения

17.1. Настоящее Положение вступает в силу с момента его утверждения ректором Университета и действует бессрочно, до замены его новым положением.

17.2. Все изменения в Положение утверждаются приказом ректора Университета в установленном порядке.

17.3. Все работники Университета должны быть ознакомлены с настоящим Положением.

Инструкция ответственного за обработку и защиту персональных данных в НИУ МГСУ

1. Назначение и область применения

1.1. Настоящая Инструкция ответственного за защиту персональных данных в НИУ МГСУ, разработана в соответствии с Федеральным законом РФ от 27.07.2006 N152 (ред. от 31.12.2017) «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящая Инструкция определяет основные обязанности, функции, права и ответственность лица, ответственного за защиту персональных данных в НИУ МГСУ.

1.3. Ответственный за защиту персональных данных назначается приказом ректора из работников каждого структурного подразделения, задействованного в обработке персональных данных, и отвечает за контроль обработки персональных данных в НИУ МГСУ, организацию работ по обеспечению безопасности персональных данных, обрабатываемых, передаваемых и хранимых персональных данных, а также подготовку сотрудников по вопросам связанной с защитой информации и персональных данных

2. Основные требования и обязанности ответственного за защиту персональных данных

2.1. Для обеспечения информационной безопасности в области обработки персональных данных ответственный за защиту должен знать:

- законодательные акты, нормативные и методические материалы, в том числе организационно-распорядительную документацию НИУ МГСУ по вопросам, связанным с обеспечением защиты информации и персональных данных;
- структуру информационных систем по обработке персональных данных, и категорию персональных данных обрабатываемой в них;
- методы планирования и организации проведения работ по защите персональных данных в зоне ответственности.

2.2. К функциональным обязанностям ответственного за защиту персональных данных относятся:

- обеспечение соответствия деятельности НИУ МГСУ требованиям законодательных актов, нормативным и методическим материалам, в том числе организационно-распорядительной документации по вопросам, связанным с обеспечением защиты информации и персональных данных;
- повышение степени защищенности информации и персональных данных;
- своевременное предупреждение и реагирование на риски, связанные с нарушением защиты информации и персональных данных при их обработке в установленном п.3 настоящей Инструкции порядке.

2.3. В обязанности ответственного за защиту персональных данных входят следующие мероприятия по контролю исполнения требований законодательных актов, нормативных и методических материалов, в том числе организационно-распорядительной документации НИУ МГСУ по вопросам, связанных с обеспечением защиты информации и персональных данных:

- ознакомление работников, производящих обработку персональных данных, с требованиями законодательных актов, нормативными и методическими материалами, в том числе организационно-распорядительной документацией по вопросам, связанным с обеспечением защиты информации и персональных данных;
- доводить и ознакомлять допущенных работников к обработке персональных данных актуальную информацию, связанную с изменением требований, связанных с обеспечением защиты информации и персональных данных;
- контроль и учет работников, допущенных к обработке персональных данных;

- учет материальных носителей персональных данных и их мест хранения;
- блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки либо блокировать доступ работника к персональным данным в связи с увольнением/перевода работника, допущенного к обработке персональных данных;
- обеспечение физической безопасности помещений, в которых производится обработка ПДн согласно внутренним документам (исключение доступа к персональным данным посторонних лиц, хранение персональных данных в запираемых помещениях, шкафах, сейфах с соблюдением условий конфиденциальности);
- контроль соблюдения работниками требований, связанных с обеспечением защиты информации и персональных данных;
- участие в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации и персональных данных;
- сбор согласий на обработку персональных данных и контроль за осуществлением сбора согласий на обработку персональных данных работниками при условии, что подразделение является точкой входа для персональных данных субъекта любой категории;
- контроль за процедурой уничтожения персональных данных по актам уничтожения персональных данных (после уничтожения акты должны находиться на хранении у Ответственного за защиту персональных данных);
- контроль за процедурой ответов на запрос субъекта персональных данных, его законного представителя, уполномоченного органа по защите прав субъекта персональных данных или иного уполномоченного органа в соответствии с принятым в НИУ МГСУ Регламентом обработки запросов субъектов персональных данных или их представителей (организация ответов на запросы и их фиксирование в Журнале учета обращений субъектов ПДн ведется централизованно работниками Канцелярии НИУ МГСУ);
- поддержание в актуальном состоянии нормативно-организационных документов, а также своевременное их заполнение и/или получение указанных в пункте 6 «Приложения к инструкции ответственного за защиту персональных данных в НИУ МГСУ»;
- при оформлении и прекращение допуска работнику к обработке персональных данных, сообщать работникам отдела защиты информации и персональных данных сведения о работнике (ФИО, должность), одним из следующих способов: посредствам корпоративной электронной почтой; в виде служебной запиской в свободной форме; посредствам электронного документооборота.

3. Действия при обнаружении попыток несанкционированного доступа

3.1. К попыткам несанкционированного доступа относятся:
- сеансы работы с персональными данными не допущенных работников к обработке персональных данных;
- действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи допущенного работника к обработке персональных данных, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом;
- действия третьего лица, находящегося в месте хранения либо обработки персональных данных, без контроля работника, допущенного к обработке персональных данных.

3.2. При выявлении факта несанкционированного доступа ответственный за защиту персональных данных обязан:
- прекратить несанкционированный доступ информационный/физический к персональным данным;
- доложить непосредственному руководителю и в информационно-вычислительный центр служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

- известить руководителя структурного подразделения, в котором работает работник, допущенный к обработке персональных данных, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;
- известить администратора ИСПДн о факте несанкционированного доступа;
- участвовать в расследовании и выявленнии угрозы.

4. Права ответственного за обработку персональных данных

4.1. Требовать от работников выполнения локальных нормативно-правовых актов в части работы с персональными данными и защиты информации.

4.2. Блокировать доступ совместно с администратором ИСПДн к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

4.3. Проводить служебные расследования и опрашивать работников по фактам несоблюдения условий обработки персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

5. Ответственность за выполнение действий настоящей Инструкции

5.1. Ответственный за организацию обработки персональных данных несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных.

5.2. Ответственный за организацию обработки персональных данных при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную и/или иную ответственности в соответствии с законодательством Российской Федерации.

6. Приложения к инструкции ответственного за защиту персональных данных в НИУ МГСУ

Приложение 1
к Инструкции ответственного за обработку и
защиту персональных данных
в НИУ МГСУ

Перечень работников, допущенных к обработке персональных данных

_____
(наименование структурного подразделения НИУ МГСУ)

№ п.п.	Ф.И.О. (полностью)	Должность	Наименование структурного подразделения\отдел	Номер комнаты, корпус	Контактные данные (телефон, e-mail)	Примечание*
1.						
2.						
3.						
4.						

Ответственный за защиту персональных данных / _____ / _____
(подпись) *(И.О. Фамилия)*

«__» _____201_ г.
(дата)

Руководитель подразделения / _____ / _____
(подпись) *(И.О. Фамилия)*

«__» _____201_ г.
(дата)

* Вносятся данные о кадровых перемещениях (перевод, перемещение, увольнение

Приложение 2
к Инструкции ответственного за обработку и
защиту персональных данных
в НИУ МГСУ

Журнал учета электронных носителей персональных данных*:

_____

(наименование структурного подразделения НИУ МГСУ)

№ п.п.	Дата	Наименование носителя	Инвентарный номер носителя	Дата и № акта о вводе в эксплуатацию электронного носителя персональных данных**	Дата и № акта об уничтожении	Примечание***
1.						
2.						
3.						
4.						

Ответственный за защиту персональных данных / _____ / _____
(подпись) *(И.О. Фамилия)*

«__» _____201_ г.
(дата)

Руководитель подразделения / _____ / _____
(подпись) *(И.О. Фамилия)*

«__» _____201_ г.
(дата)

* Электронным носителем персональных данных считается: материальный носитель, используемый для записи, хранения и воспроизведения персональных данных, обрабатываемых с помощью средств вычислительной техники.

** Указываются данные о заявке замены и добавления электронных носителей персональных данных

*** Указывается дополнительная информация об электронном носителе информации (подключен к ФИС либо к ГИС, использование средств криптозащиты информации, использование электронной подписи и тд.).

Приложение 3
к Инструкции ответственного за обработку и
защиту персональных данных
в НИУ МГСУ

Начат «___» _____ ____ г.
Окончен «___» _____ г.
На _____ листах

Журнал учета обращений граждан (субъектов персональных данных) или их представителей по вопросам обработки персональных данных

№ п.п.	ФИО субъекта	Дата обращения	Тема обращения	Отметка об исполнении	ФИО исполнителя	Подпись

Приложение 4
к Инструкции ответственного за обработку и
защиту персональных данных
в НИУ МГСУ

Журнал учета мест хранения материальных носителей персональных данных:

_____

(наименование структурного подразделения НИУ МГСУ)

№ п.п.	Полное наименование помещения	Виды носителей*	Примечание
1.			
2.			
3.			

Ответственный за защиту персональных данных / _____ / _____
(подпись) *(И.О. Фамилия)*

«__» _____201_ г.
(дата)

Руководитель подразделения / _____ / _____
(подпись) *(И.О. Фамилия)*

«__» _____201_ г.
(дата)

*Возможные виды носителей:

- Жесткие диски, входящие в состав автоматизированных рабочих мест (производится учет системных блоков или ноутбуков, т.к. жесткие диски не имеют инвентарного номера) (Жесткий диск в составе АРМ);
- Бумажные носители

Приложение 5
к Инструкции ответственного за обработку и
защиту персональных данных
в НИУ МГСУ

ЛИСТ ОЗНАКОМЛЕНИЯ
с внутренней нормативной документацией в области защиты персональных данных для работников, производящих обработку персональных данных

№	Наименование документа	Дата и № документа	Подпись работника	Дата ознакомления
1.	Положение об обработке и защите персональных данных в Федеральном государственном бюджетном образовательном учреждении высшего образования «Национальный исследовательский Московский государственный строительный университет»			
2.	Инструкция работника, производящего обработку персональных данных			
3.	Инструкция по организации антивирусной защиты			
4.	Инструкция по организации парольной защиты			
5.	Инструкция по использованию корпоративной почты и доступа в Интернет			

Обязательство:
Я предупрежден(а) о персональной ответственности за выполнение вышеперечисленных внутренних нормативных документов в области защиты информации НИУ МГСУ. В случае нарушения безопасности конфиденциальной информации либо персональных данных, буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____
Структурное подразделение (полное/сокращенное наименование)

_____ / _____ /
(должность) *(подпись)* *(И.О. Фамилия)*

«__» _____201_ г.
(дата)

Приложение 6
к Инструкции ответственного за обработку и
защиту персональных данных
в НИУ МГСУ

ЛИСТ ОЗНАКОМЛЕНИЯ
с внутренней нормативной документацией в области защиты персональных данных для работников, ответственных за обработку и защиту персональных данных

№	Наименование документа	Дата и № документа	Подпись работника	Дата ознакомления
1.	Положение об обработке и защите персональных данных в Федеральном государственном бюджетном образовательном учреждении высшего образования «Национальный исследовательский Московский государственный строительный университет»			
2.	Инструкция ответственного за защиту персональных данных			
3.	Инструкция по организации антивирусной защиты			
4.	Инструкция по организации парольной защиты			
5.	Инструкция по использованию корпоративной почты и доступа в Интернет			

Обязательство:
Я предупрежден(а) о персональной ответственности за выполнение вышеперечисленных внутренних нормативных документов в области защиты информации НИУ МГСУ. В случае нарушения безопасности конфиденциальной информации либо персональных данных, буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____
Структурное подразделение (полное/сокращенное наименование)

_____ / _____ / _____
(должность) *(подпись)* *(И.О. Фамилия)*

«__» _____201_ г.
(дата)

Приложение 7
к Инструкции ответственного за обработку и
защиту персональных данных
в НИУ МГСУ

НИУ МГСУ

"____" _____ 201__ г. Москва

А К Т

Об уничтожении персональных данных

Комиссия, в составе:

_____ _____
Ф.И.О (должность)

_____ _____
Ф.И.О (должность)

_____ _____
Ф.И.О. (должность)

Провела отбор носителей персональных данных и установила, что информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Инвентарный номер носителя ПДн	Примечание

Всего съемных носителей _____
(цифрами и прописью)

На указанных носителях персональные данные уничтожены путем _____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПДн уничтожены путем _____.
(разрезания, сжигания, механического уничтожения, и т.п.)

_____ _____
(подпись) *(И.О. Фамилия)*

_____ _____
(подпись) *(И.О. Фамилия)*

_____ _____
(подпись) *(И.О. Фамилия)*

Приложение 8
к Инструкции ответственного за обработку и
защиту персональных данных
в НИУ МГСУ

Форма согласования
замены/перемещения АРМ в составе ИСПДн

Структурное подразделение (полное/сокращенное наименование)	
Руководитель структурного подразделения	
Телефон, e-mail	
ФИО, должность ответственного за защиту персональных данных	
Телефон, e-mail	

Обоснование необходимости замены/перемещения АРМ: _____

_____

_____

Сведения о действующем АРМ:

№	Код АРМ	Структурное подразделение (сокращенное наименование)	Корпус	Помещение	Инвентарный номер	ФИО, должность МОЛ

Сведения о согласуемом к замене/перемещению АРМ:

№	Код АРМ	Структурное подразделение (сокращенное наименование)	Корпус	Помещение	Инвентарный номер	ФИО, должность МОЛ

Ответственный за защиту персональных данных _____ _____ «__» _____201_ г.
(подпись) *(И.О. Фамилия)* *(дата)*

Руководитель подразделения _____ _____ «__» _____201_ г.
(подпись) *(И.О. Фамилия)* *(дата)*

Материально ответственное лицо _____ /_____ «__» _____201_ г.
(подпись) *(И.О. Фамилия)* *(дата)*

Ответственный за защиту персональных данных НИУ МГСУ _____ _____ «__» _____201_ г.
(подпись) *(И.О. Фамилия)* *(дата)*

Инструкция работника, производящего обработку персональных данных

1. Назначение и область применения

1.1. Настоящая Инструкция определяет основные обязанности и ответственность работника, допущенного к обработке персональных данных.

1.2. Работник при выполнении работ с персональными данными обеспечивает информационную безопасность данных и несет персональную ответственность за соблюдение данной Инструкции и иных документов по защите информации.

2. Основные обязанности работника, производящего обработку персональных данных

2.1. Выполнять требования по обеспечению информационной безопасности персональных данных, установленные законодательством Российской Федерации, внутренней организационно-распорядительной документацией по защите персональных данных в Университете и настоящей Инструкцией.

2.2. При работе с персональными данными не допускать присутствие в помещении, где расположены автоматизированные рабочие места по обработке данных и/или бумажные носители информации, не допущенных к обрабатываемой информации лиц или располагать в недоступном месте для исключения возможности просмотра/считывания информации посторонними лицами.

2.3. После окончания либо временной приостановки обработки персональных данных, необходимо блокировать автоматизированное рабочее место и/или убрать бумажные носители информации в недоступное посторонним лицам место (запираемый шкаф, сейф и т. д.).

2.4. Не допускать потери парольной информации для доступа к автоматизированным рабочим местам и/или информационным системам по обработке персональных данных. Хранить парольную информацию в недоступном третьим лицам месте и не оставлять без присмотра. Также не допустимо в устной либо в письменной форме передавать парольную информацию третьим лицам.

2.5. Запрещается производить обработку персональных данных под чужими учетными записями на автоматизированных рабочих местах так и в информационных системах по обработке персональных данных.

2.6. В случае выявления инцидентов информационной безопасности (фактов или попыток несанкционированного доступа к персональным данным, обрабатываемой на автоматизированном рабочем месте или к бумажным носителям информации) немедленно сообщить об этом ответственному за защиту персональных данных по структурному подразделению либо в информационно-вычислительный центр Университета.

2.7. Ставить в известность ответственного за защиту персональных данных по структурному подразделению о:

- несанкционированном перемещении автоматизированного рабочего места в другое помещение (кабинет, корпус, здание);
- некорректной работе автоматизированного рабочего места или программного обеспечения;
- нарушениях требований информационной безопасности;
- фактах или попытках несанкционированного доступа к персональным данным.

2.8. Работник, допущенный к обработке персональных данных и имеющий доступ к автоматизированным рабочим местам и/или к информационной системе по обработке персональных данных, несет персональную ответственность за свои действия.

2.9. Работнику ***ЗАПРЕЩАЕТСЯ***:

- записывать и хранить персональные данные на неучтенных установленным порядком электронных носителях информации;
- осуществлять несанкционированную распечатку персональных данных;

– самостоятельно подключать к автоматизированному рабочему месту какие-либо неучтенные устройства;

– самостоятельно вносить какие-либо изменения в конфигурацию аппаратных средств автоматизированного рабочего места;

– самостоятельно устанавливать и/или запускать (выполнять) на автоматизированном рабочем месте любые системные или прикладные программы, загружаемые по сети или с внешних носителей;

– осуществлять обработку персональных данных на неучтенных установленным порядком автоматизированных рабочих местах;

– отключать (блокировать) средства защиты информации;

– оставлять бесконтрольно или в незаблокированном состоянии автоматизированного рабочего места с загруженными персональными данными и/или с доступом к информационной системе по обработке персональных данных;

– использовать персональные данные субъектов для личных целей.

2.10. Особенности обработки персональных данных без использования средств автоматизации:

– персональные данные при их неавтоматизированной обработке и хранении должны обособляться от иной информации путем фиксации их на отдельных материальных носителях и хранится в отдельных шкафах;

– при фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы;

– хранение материальных носителей персональных данных осуществляется в специальных местах (ящиках, шкафах, сейфах и т.д.), обеспечивающих сохранность материальных носителей и исключающих несанкционированный к ним доступ.

3. Ответственность за нарушение безопасности при обработке персональных данных

3.1. На работника возлагается персональная ответственность за невыполнение и/или нарушение требований, установленных законодательством Российской Федерации, внутренней организационно-распорядительной документацией по защите персональных данных в Университете и настоящей Инструкцией.

3.2. Лицо, виновное в нарушении безопасности персональных данных, может быть привлечено к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

Инструкция по организации средств защиты информации

1. Назначение и область применения

1.1. Настоящая Инструкция определяет требования к организации защиты информационных систем по обработке персональных данных и автоматизированных рабочих мест от вредоносного воздействия компьютерных вирусов.

1.2. Настоящая Инструкция устанавливает ответственность и основные обязанности работников по эксплуатации средств защиты персональных данных.

2. Обеспечение информационной безопасности

2.1. К использованию в Университете допускаются только лицензионные средства защиты информации, сертифицированные Федеральной службой по техническому и экспортному контролю России, с возможностью централизованного управления.

2.2. Установка средств защиты информации на автоматизированных рабочих местах и информационных систем по обработке персональных данных осуществляется работниками информационно-вычислительного центра Университета, контроль за работоспособностью выполняется администратором средств защиты информации.

2.3. Запуск средств защиты информации осуществляется автоматически при поддержке централизованного управления.

2.4. Контроль автоматизированных рабочих мест и информационных систем по обработке персональных данных проводится постоянно в автоматическом режиме.

2.5. Обязательному контролю при помощи средств защиты информации подлежит любая информация, получаемая по сети или загружаемая со съемных носителей. Контроль информации проводится средствами в процессе или сразу после ее загрузки.

2.6. На серверах информационных систем по обработке персональных данных, применяется специализированные средства защиты информации и/или программные/аппаратные компоненты с повышенным уровнем защиты.

2.7. Организовано регулярное обновление сигнатур угроз на всех автоматизированных рабочих местах и информационных системах по обработке персональных данных.

3. Обязанности работника при работе с антивирусной системой

3.1. При возникновении подозрения на наличие угрозы (сообщение от средств защиты информации, нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник должен провести внеочередной контроль путем проверки целостности и выборочной проверки средствами защиты информации или сообщить о данной проблеме в информационно-вычислительный центр Университета.

3.2. В случае обнаружения при проведении средствами защиты информации проверки зараженных компьютерными вирусами файлов работник ***ОБЯЗАН***:

- приостановить работу без перезагрузки компьютера;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь работников информационно-вычислительного центра Университета);
- в случае обнаружения нового вируса, не поддающегося лечению, привлечь работников информационно-вычислительного центра Университета;
- поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за защиту персональных данных в структурном подразделении, владельца зараженных файлов, а также смежные структурные подразделения, которые пользуются данным файлом.

3.3. Работнику ***ЗАПРЕЩАЕТСЯ***:

– изменять конфигурацию средств защиты информации;

– скачивать из сети, в том числе средствами электронной почты, информацию, содержащую исполняемые модули, программы, драйверы и т. п.

4. Ответственность за выполнение действий настоящей Инструкции

4.1. Ответственность за организацию работы средств защиты информации на автоматизированных рабочих местах, серверах информационных систем по обработке персональных данных и локальной вычислительной сети возлагается на администратора средств защиты информации.

4.2. Ответственность за непрерывную работу мониторинга средств защиты информации, установленного информационным-вычислительным центром на автоматизированные рабочие места, возлагается на работника, использующего данное автоматизированное рабочее место.

4.3. На работника возлагается персональная ответственность за невыполнение и/или нарушение требований, настоящей Инструкцией.

4.4. Лицо, виновное в нарушении защиты информации, может быть привлечено к дисциплинарной ответственности.

Инструкция по организации парольной защиты

1. Назначение и область применения

1.1. Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей, блокирования и удаления учетных записей работников, в информационных системах Университета.

1.2. Требования данной Инструкции являются неотъемлемой частью комплекса мер по обеспечению информационной безопасности и защиты персональных данных.

1.3. Требования данной Инструкции распространяется на всех работников Университета, использующих в работе автоматизированные рабочие места и доступ к информационным системам.

2. Общие требования к учетной записи и генерации паролей

2.1. Каждому работнику Университета сопоставляется персональное уникальное имя (учетная запись), под которым он будет регистрироваться, работать на автоматизированных рабочих местах и с информационными системами. Использование несколькими работниками при работе одной и той же учетной записью запрещено, если данная учетная запись не является групповой (учетная запись подразделения).

2.2. Для формирования учетных данных работника Университета необходима форма заявки на регистрацию и/или служебное распоряжение, утверждённое руководителем структурного подразделения.

2.3. Пароли доступа к автоматизированным рабочим местам и/или информационным системам первоначально формируются уполномоченным администратором или администратором информационной системы, а в дальнейшем генерируются пользователями самостоятельно, но с учетом требований, изложенных ниже (исключения составляют некоторые информационные системы).

2.4. Основные требования к генерации паролей к учетным записям:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.), если это поддерживается информационной системой;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, логины учетных записей и т.д.), а также общепринятые сокращения (qwerty, pa$$w0rd, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем двумя символами.

2.5. Для генерации более «стойких» значений паролей могут применяться специальные программные средства генерации паролей. При этом рекомендовано исключать возможность повторной выработки тех же значений для других пользователей. Генерация паролей производится уполномоченным администратором или администратором информационной системы.

2.6. В случае если формирование личных паролей к учетным записям осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных администраторов систем или администраторов информационной системы.

2.7. Выдача парольной информации производится лично работнику Университета в руки уполномоченным администратором или администратором информационной системы при предъявлении документа, подтверждающего личность работника.

2.8. Смена забытого пароля производится уполномоченным администратором или администратором информационной системы при личном присутствие работника Университета при предъявлении документа, подтверждающего личность.

3. Дополнительные требования по организации парольной защиты

3.1. Если подсистемы информационной системы обладают соответствующими возможностями, то они настраиваются согласно требованиям настоящей инструкции и перечисленным ниже рекомендациям:

- принудительная смена пароля с периодом не больше 3 месяцев;
- предварительное оповещение работника о необходимости смены пароля за 14 дней;
- принудительная проверка сложности пароля;
- ведение истории не менее 3 последних паролей к учетной записи;
- централизованная или при помощи работников информационно-вычислительного центра настройка автоматизированных рабочих мест на использование блокировки рабочего места средствами операционной системы по истечению 15 минут неактивного состояния;
- для предотвращения «угадывания» паролей уполномоченный администратор или администратор информационной системы обязан настроить механизм временной блокировки учетной записи при пятикратном неправильном вводе пароля.

3.2. При необходимости доступа к персональной информации работника в его отсутствие осуществляется внеплановая смена пароля учетной записи уполномоченным администратором или администратором информационной системы. Основанием для внеплановой смены пароля в этом случае является заявка руководителя структурного подразделения Университета в информационно-вычислительный центр. В заявке указывается причина внеплановой смены и ФИО работника Университета.

4. Безопасность локальных учетных записей

4.1. Локальные учетные записи компьютеров (Administrator, Guest, User) предназначены для служебного использования уполномоченными администраторами или техническими работниками информационно-вычислительного центра при настройке операционных систем и установки программного обеспечения и не предназначены для повседневной работы.

4.2. В случае необходимости в использовании специализированных технических либо программных средств работнику Университета предоставляется локальная учетная запись уполномоченным администратором либо техническими работниками информационно-вычислительного центра.

5. Обязательства работников к использованию парольной информации

5.1. В случае компрометации либо угрозы компрометации личной парольной информации работника Университета к автоматизированном рабочему месту либо к информационной системе работник должен немедленно предпринять меры по внеплановой смене пароля, либо сообщить о данной угрозе уполномоченному администратору системы. Под компрометацией парольной информации понимается утрата, хищение носителя с паролем или его разглашение третьим лицам.

5.2. Запрещается хранить парольную информацию в общедоступных местах (на мониторе, системном блоке и т.п.), в электронном виде на автоматизированном рабочем месте и передавать третьим лицам. Хранение работниками своей парольной информации на бумажном носителе допускается только в недоступном для третьих лиц местах.

5.3. При смене пароля к учетной записи работник Университета должен сгенерировать пароль в соответствие с пунктом 2.4 настоящей Инструкции, либо обратится к уполномоченному администратору.

6. Ответственность за нарушение безопасности

6.1. Владельцы паролей (работники) должны быть ознакомлены под подпись с данной Инструкцией, предупреждены о персональной ответственности в случае нарушения и несоблюдении перечисленными выше требований и обязательств.

6.2. Форма и степень ответственности определяются исходя из вида угрозы, действиями либо бездействием соответствующего работника.

6.3. Лица, виновные в нарушении требований и обязательств по организации парольной защиты, могут быть привлечены к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации, исходя из вида угроз.

Инструкция по использованию корпоративной почты и доступа в Интернет

1. Назначение и область применения

1.1. Настоящий документ разработан с целью упорядочения действий работников с корпоративной почтой Университета, повышения персональной ответственности за действия, производимые в процессе получения, хранения и отправки сообщений электронной почты и использования доступом в сеть Интернет.

2. Подключение к корпоративной почте

2.1. Корпоративная электронная почта предоставляется работникам Университета только для исполнения своих служебных обязанностей.

2.2. Решение о необходимости получения корпоративной почты работнику принимает непосредственный руководитель структурного подразделения.

2.3. Подключение к корпоративной почте производится уполномоченным администратором на основание формы заявки на регистрацию почты.

2.4. Выдача парольно-ключевой информации для доступа к корпоративной почте производится лично работнику Университета в руки под подпись уполномоченным администратором при предъявлении документа, подтверждающего личность работника.

3. Требования по эксплуатации корпоративной почты

3.1. При использовании корпоративной электронной почты необходимо:

- соблюдать требования настоящей Инструкции;
- использовать корпоративную электронную почту исключительно для выполнения служебных обязанностей;
- перед отправкой сообщения проверять правильность введенного электронного адреса получателя;
- ставить в известность уполномоченного администратора о любых фактах нарушения требований настоящей Инструкции;
- обращаться за изменением парольной информации для доступа к корпоративной электронной почте в случае компрометации парольной информации (утери, хищения, считывания и т.д.)

3.2. При использовании корпоративной электронной почты работнику Университета **ЗАПРЕЩАЕТСЯ**:

- рассылка электронных писем, содержащих конфиденциальную информацию;
- рассылка сообщений (в т.ч. рекламы, информации развлекательного характера или коммерческих предложений), информация в которых по содержанию заведомо не предназначена для адресатов, или адресатам, которые не давали разрешения на рассылку таких сообщений (спам);
- рассылка сообщений, содержащих материалы, запрещенные к распространению законодательством Российской Федерации;
- пересылать исполняемые файлы (с расширениями – .exe, .bat, .dll, .pif и т.п.);
- производить рассылку вредоносных программ или файлов, зараженных вирусами;
- рассылка сообщений, содержащих негативную информацию о деятельности Университета или ее работников;
- рассылка сторонним адресатам сообщений, содержащих адреса электронной почты работников без согласия последних;
- рассылка сообщений, содержащих компоненты программного обеспечения, используемые в Университете, лицами, в чьи обязанности не входит отправка таких сообщений, а также лицам (адресатам), не имеющим отношения к этому программному обеспечению;

- использование средств корпоративной электронной почты для отправки сообщений, не связанных с выполнением служебных обязанностей;
- использовать корпоративную электронную почту в личных целях некорпоративного характера;
- использование сторонних бесплатных почтовых сервисов в корпоративных целях и задачах (mail.ru, yandex.ru, и т.д.);
- предоставлять третьим лицам пароль доступа к своему личному корпоративному почтовому ящику;
- пересылать по электронной почте парольно-ключевую информацию к каким бы то ни было ресурсам Университета;
- открывать сообщения, для которых имеется предупреждение о возможном наличии вируса;
- открывать сообщения от неизвестного отправителя, содержащие вложенные файлы любых форматов;
- открывать сообщения, у которых поле «От:» («From:») не заполнено (анонимные сообщения);
- открывать сообщения, из содержания поля «Тема:» («Subj:») которых понятно, что у получателя нет прав на ознакомление с содержащейся в них информацией. О получении такого сообщения немедленно сообщить уполномоченному администратору и по его указанию переслать ему пришедшее письмо либо незамедлительно стереть из папок «Входящие» и «Отправленные» (в случае пересылки), а затем – и из папки «Удаленные».

4. Корректирующие действия при выявлении угрозы информационной безопасности

4.1. В целях контроля данной Инструкции содержимое почтового ящика работника Университета может быть проверено уполномоченным администратором без предварительного уведомления работника при условии угрозы информационной безопасности либо по требованию непосредственного руководителя данного работника.

4.2. В целях обеспечения информационной безопасности уполномоченный администратор вправе блокировать учетные данные к корпоративной электронной почте работника Университета в случаях:

- осуществления рассылки писем, содержащих вредоносные программы, спам, информацию, распространение которой запрещено нормативно-правовыми актами;
- возможности доступа к соответствующей корпоративной электронной почте третьих лиц;
- использования работником корпоративной электронной почты не по назначению;
- увольнения работника;
- в иных случаях нарушения настоящей Инструкции, по решению уполномоченного администратора.

4.3. В случаях, связанных с нарушениями требований настоящей Инструкции, уполномоченный администратор блокирует данный адрес (сменить пароль) и уведомляет о данных действиях непосредственного руководителя и ответственного за защиту информации Университета.

4.4. Блокирование почтового ящика может быть прекращено уполномоченным администратором при устранении угрозы информационной безопасности по указанию ответственного за защиту информации Университета.

5. Обеспечение информационной безопасности при использовании ресурсов сети Интернет

5.1. Подключение автоматизированного рабочего места к ресурсам сети Интернет осуществляется работниками информационно-вычислительного центра Университета на основании заявки, подписанной руководителем структурного подразделения. Заявка должна содержать следующую информацию:

- фамилию, имя, отчество лица и/или наименование структурного подразделения, которому предоставляется доступ к сети Интернет, его местонахождение;
- цели использования ресурсов сети Интернет;
- перечень необходимых информационных ресурсов.

5.2. Для предотвращения или снижения вероятности угроз безопасности информации при пользовании системами доступа в сеть Интернет запрещается:

- запрос и получение пользователями из сети Интернет материалов развлекательного характера (игр, клипов и т.д.);
- запрос и получение пользователями из сети Интернет программных продуктов без согласования с информационно-вычислительным центром;
- загрузка файлов мультимедиа (музыка, фильмы, игры);
- посещение сайтов развлекательного характера;
- осуществление попыток несанкционированного доступа к ресурсам сети Интернет, проведение или участие в сетевых атаках и сетевом взломе;
- обработка конфиденциальной информации на компьютере, имеющем соединение с сетью Интернет, при отсутствии соответствующих средств защиты информации;
- пересылка информации, содержащей сведения конфиденциального характера, через Интернет без использования программно-аппаратных средств, обеспечивающих соответствующую степень защиты;
- использовать на рабочем месте иные каналы доступа к сети Интернет, кроме установленных;
- проводить самостоятельное изменение конфигурации технического и программного обеспечения автоматизированного рабочего места, подключенного к сети Интернет;
- осуществлять перенос полученной по сети Интернет документированной информации в электронном виде на другие компьютеры без проверки ее средствами защиты информации.

5.3. В случае нарушения вышеперечисленных требований при использовании доступа к сети Интернет, работники или уполномоченный администратор информационно-вычислительного центра вправе отключить от ресурсов сети Интернет автоматизированное рабочее место до выяснения причин и уведомление ответственного за защиту информации Университета.

6. Ответственность за нарушение безопасности

6.1. Работники должны быть ознакомлены под подпись с данной Инструкцией, предупреждены о персональной ответственности в случае нарушения и несоблюдении перечисленными выше требований и обязательств.

6.2. Форма и степень ответственности определяются исходя из вида угрозы, действиями либо бездействием соответствующего работника.

6.3. Лица, виновные в нарушении требований и обязательств по использованию корпоративной почтой и интернетом, могут быть привлечены к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации, исходя из вида угроз.

5. Резерв

6. Лист регистрации изменений

Изменение	Наименование и номер документа-основания	Номера листов (страниц)		Дата введения изменения в действие	Подпись ответст-венного за внесение изменений
		Анну-лиро-ванных	Новых		

7. Лист рассылки

СК И ПВД 06 - 44 - 2019

Альбом внутренней организационно-распорядительной документации
в области обработки и защиты персональных данных

Должность	Инициалы, Фамилия
Проректор	Е.Н. Куликова
Проректор	Е.В. Королёв
Проректор	Е.С. Гогина
Проректор	А.П. Пустовгар
Проректор	М.Е. Лейбман
Проректор	З.М. Штымов
Директор ИГЭС	Н.А. Анискин
Директор ИИЭСМ	К.И. Лушин
Директор ИФО	О.А. Ковальчук
Директор ИЭУИС	О.Н. Кузина
Директор ИСА	Н.Д. Чередниченко
И.о. директора ИДО	Н.А. Губина
Директор филиала НИУ МГСУ в г.Мытищи	Г.Н. Баров
Начальник УМУ	О.М. Баранова
Начальник УРП	В.И. Макателемский
Главный бухгалтер УБУ и ФК	А.М. Мелешко
Начальник ПФУ	А.Л. Демин
Начальник АУ	Ю.В. Казакова
Начальник Второго отдела	В.Н. Святченко
Начальник ЦПДПК	Ю.В. Ушакова
Руководитель ОДО	А.А. Василькин
Начальник ЦОСП	А.Е. Беспалов
Начальник УБ	В.П. Задерей
Заведующий бюро пропусков	С.В. Черепанов
Директор ЦМО	Е.С. Толстых
Начальник УКМС	Н.В. Самотесова
Начальник ЦДПО	А.В. Федосьина
Начальник УНП	А.О. Адамцевич
Директор НТБ	Е.Н. Бойко
Директор СОК	В.А. Никишкин
Начальник ЦДП «Абитуриент»	А.В. Ермолаев
Заведующий архивом	С.П. Шутченко
Начальник ВК	А.В. Иосипенко
Начальник УМИП	Е.М. Чеботаева

Документ изъят:

Основание:

_____	_____	_____	_____
(Должность)	(Подпись)	(Дата)	(И. О. Ф.)