Приложение №1
к приказу ФГБОУ ВО «ХТУ»
от 18.02.2026г. № 322

ИНСТРУКЦИЯ
РУКОВОДИТЕЛЯ СТРУКТУРНОГО ПОДРАЗДЕЛЕНИЯ, ОСУЩЕСТВЛЯЮЩЕГО ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ в ФГБОУ ВО «ХЕРСОНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция руководителя структурного подразделения, осуществляющего обработку персональных данных в ФГБОУ ВО «Херсонский технический университет», разработана на основании требований Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в соответствии с требованиями системы менеджмента качества образования университета.

1.2. Руководитель – лицо, непосредственно занимающееся управлением организации работ в структурном подразделении ФГБОУ ВО «ХТУ», осуществляющем обработку персональных данных (далее – ПДн).

1.3. Руководитель в процессе осуществления своих обязанностей руководствуется законодательством Российской Федерации в области обеспечения безопасности ПДн, локальными нормативными актами Университета.

1.4. Руководитель осуществляет следующие основные функции в области обеспечения безопасности ПДн:

- руководит организацией работ по защите информации и обработке персональных данных;
- вносит предложения по организации защиты информации и обработки персональных данных;
- предлагает кандидатов для допуска к обработке ПДн из числа работников структурного подразделения;
- контролирует исполнение нормативных документов, регламентирующих обработку ПДн и защиту информации;
- заслушивает ответственных за обеспечение безопасности ПДн и других работников структурного подразделения по вопросам защиты информации и обработки ПДн.

2. ОСНОВНЫЕ ОБЯЗАННОСТИ

2.1. Руководитель в целях исполнения функций в установленной сфере деятельности:

2.1.1. Организовывает и контролирует выполнение в подразделении мероприятий, связанных с защитой информации и обработкой ПДн.

2.1.2. Контролирует исполнение обязанностей ответственного за обеспечение безопасности ПДн в подразделении.

2.1.3. Контролирует периодичность, своевременность и ведение журналов инструктажа работников по соблюдению мер защиты информации и обработки ПДн.

2.1.4. Планирует и проводит контроль соблюдения работниками выполнения организационных мер по защите информации, правил обработки ПДн, правил работы со съемными машинными носителями информации.

2.1.5. Осуществляет контроль ведения журналов учета:

- документов, содержащих ПДн;
- технических средств, используемых в обработке ПДн.

2.1.6. Принимает участие в проведении проверок уполномоченными структурами.

2.1.7. Взаимодействует с работниками отдела обеспечения защиты информации по вопросам обеспечения выполнения требований по защите информации и обработке ПДн.

2.1.8. Доводит до подчиненных работников все принятые руководством Университета локальные нормативные акты в области защиты информации и обработки ПДн.

2.1.9. Организовывает контроль обеспечения работоспособности технических средств защиты ПДн, охранной сигнализации, средств защиты информации от несанкционированного доступа.

2.1.10. Знает перечень установленных в подразделении технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием.

2.1.11. Организовывает контроль учета, создания, хранения и использования документов и резервных копий, содержащих ПДн.

2.1.12. Организовывает контроль использования и обеспечения сохранности персональных устройств идентификации пользователей.

2.1.13. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационных систем, осуществления несанкционированного доступа к персональным данным и техническим средствам из состава информационных систем подразделения, сообщает о них работникам отдела обеспечения защиты информации.

3. ПРАВА И ПОЛНОМОЧИЯ

3.1. Руководитель имеет право:

3.1.1. Требовать от всех работников, осуществляющих обработку ПДн, выполнения установленной технологии обработки ПДн, положений, инструкций и других локальных нормативных актов Университета по обеспечению безопасности ПДн.

3.1.2. Участвовать в разработке мероприятий по совершенствованию защиты информации, обработки и хранения ПДн.

3.1.3. Приостанавливать процесс обработки ПДн или отстранять от работы работника в случаях нарушения установленной технологии обработки или требований по защите информации и ПДн.

3.1.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты информации и обработки ПДн, несанкционированного доступа, утраты, порчи защищаемых ПДн и технических средств из состава информационных систем.

3.1.5. В соответствии с инструкцией ходатайствовать перед ректором Университета о привлечении подчиненных работников, виновных в нарушениях норм и правил обработки ПДн, к дисциплинарной ответственности.

3.1.6. Давать свои предложения по совершенствованию организационных, технологических и технических мер защиты информации и обработки ПДн в подразделении.

4. ОТВЕТСТВЕННОСТЬ

4.1. Руководитель несет персональную ответственность за полноту и своевременное выполнение требований федеральных законов, нормативных документов в области защиты информации и обработки ПДн, а также настоящей Инструкции.

4.2. Руководитель, виновный в нарушении норм, регулирующих получение, обработку, защиту и передачу ПДн, привлекается к дисциплинарной ответственности в порядке, установленном Трудовым кодексом Российской Федерации, локальными нормативными актами ФГБОУ ВО «ХТУ», а также к административной или уголовной ответственности в порядке, установленном законодательством Российской Федерации.

Приложение №2
к приказу ФГБОУ ВО «ХТУ»
от 18.02. 2026г. № 322

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СТРУКТУРНОМ ПОДРАЗДЕЛЕНИИ ФГБОУ ВО «ХТУ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция ответственного за обеспечение защиты персональных данных в структурном подразделении федерального государственного бюджетного образовательного учреждения высшего образования «Херсонский технический университет) разработана на основании требований Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

1.2. Ответственный – лицо, отвечающее за организацию и состояние защиты обработки персональных данных (далее – ПДн) в структурном подразделении.

1.3. Ответственный назначается приказом Университета из числа работников Университета.

1.4. Ответственный непосредственно подчиняется руководителю структурного подразделения.

1.5. Ответственный осуществляет контроль за выполнением требований локальных нормативных актов Университета по обеспечению безопасности приема, обработки, хранения и передачи ПДн.

1.6. Ответственный в процессе осуществления своих обязанностей по обработке ПДн руководствуется законодательством Российской Федерации и нормативными правовыми актами в области обеспечения защиты ПДн, локальными нормативными актами ФГБОУ ВО «ХТУ».

2. ОСНОВНЫЕ ОБЯЗАННОСТИ

2.1. Ответственный за обеспечение безопасности персональных данных в структурном подразделении в целях исполнения функций в установленной сфере деятельности:

2.1.1. Осуществляет выполнение и контроль организационных мероприятий по защите информации и обработки ПДн в структурном подразделении.

2.1.2. Ведет журналы инструктажей работников структурного подразделения, допущенных к обработке ПДн.

2.1.3. Проводит первичный инструктаж для вновь принятых или переведенных из других отделов работников с инструкциями и положениями по обработке ПДн в Университете.

2.1.4. Инструктирует работников по соблюдению правил обработки ПДн и эксплуатации автоматизированных систем, а также по вопросам обеспечения информационной безопасности и правилам работы с применяемыми средствами защиты информации.

2.1.5. Осуществляет периодический контроль по соблюдению работниками организационных мер защиты информации, правил обработки ПДн, правил работы со съемными машинными носителями информации.

2.1.6. Взаимодействует с работниками отдела информационной безопасности университета по вопросам обеспечения требований по защите информации и обработке ПДн.

2.1.7. Организовывает работы по плановому контролю работоспособности технических средств защиты ПДн.

2.1.8. Контролирует исправность охранной сигнализации и средств защиты информации от несанкционированного доступа.

2.1.9. Знает перечень установленных в структурном подразделении технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием.

2.1.10. Контролирует целостность печатей и пломб на допущенных к обработке персональных данных защищенных устройствах, компьютерах и серверах структурного подразделения.

2.1.11. Обеспечивает соблюдение работниками структурного подразделения утвержденного порядка проведения работ по установке, модернизации и устранению неисправностей аппаратных и программных средств компьютеров и серверов из состава информационных систем.

2.1.12. Ведет и хранит журналы учета используемых компьютеров и серверов.

2.1.13. Контролирует соответствие реальной конфигурации компьютеров и серверов их спецификациям.

2.1.14. Ведет учет изменений аппаратно-программной конфигурации компьютеров и серверов, составляет и хранит служебные акты, на основании которых были произведены данные изменения. Вносит соответствующие изменения в их спецификацию.

2.1.15. Обеспечивает и контролирует порядок учета, создание, хранение и использование документов и резервных копий, содержащих ПДн.

2.1.16. Контролирует порядок использования и обеспечения сохранности персональных устройств идентификации пользователей.

2.1.17. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационных систем, осуществления несанкционированного доступа к ПДн и техническим средствам из состава информационных систем структурного подразделения

применяет меры к пресечению подобных действий и сообщает о них руководителю структурного подразделения и работникам управления комплексной безопасности университета.

3. ПРАВА И ПОЛНОМОЧИЯ

3.1. Ответственный имеет право:

3.1.1. Требовать от работников структурного подразделения, осуществляющих обработку ПДн, выполнения установленной технологии обработки ПДн, положений, инструкций и других нормативных правовых документов по обеспечению безопасности ПДн.

3.1.2. Участвовать в разработке мероприятий по совершенствованию безопасности обработки и хранения ПДн.

3.1.3. Обращаться к руководителю структурного подразделения с предложением о приостановке обработки ПДн или отстранению от работы работника структурного подразделения в случаях нарушения им установленной технологии обработки или требований по защите информации и ПДн.

3.1.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты информации и обработки ПДн, несанкционированного доступа, утраты, порчи защищаемых ПДн и технических средств из состава информационных систем.

3.1.5. Подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты информации и обработки ПДн в подразделении.

4. ОТВЕТСТВЕННОСТЬ

4.1. Ответственный несет персональную ответственность за полноту и своевременное выполнение требований федеральных законов, нормативных правовых актов, документов в области защиты информации и обработки ПДн, а также настоящей Инструкции.

4.2. Ответственный, виновный в нарушении норм, регулирующих получение, обработку, защиту и передачу посторонним лицам ПДн, привлекается к дисциплинарной ответственности в порядке, установленном Трудовым кодексом Российской Федерации, локальными нормативными актами ФГБОУ ВО «ХТУ», а также к административной или уголовной ответственности в порядке, установленном законодательством Российской Федерации.

Приложение №3
к приказу ФГБОУ ВО «ХТУ»
от 18.02 2026г. № 322

ИНСТРУКЦИЯ
РАБОТНИКА СТРУКТУРНОГО ПОДРАЗДЕЛЕНИЯ, ОСУЩЕСТВЛЯЮЩЕГО ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ В ФГБОУ ВО «ХТУ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция работника структурного подразделения, осуществляющего обработку персональных данных в подразделениях ФГБОУ ВО «ХТУ», разработана на основании требований Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в соответствии с требованиями системы менеджмента качества образования университета.

1.2. Работник – лицо, непосредственно занимающееся получением, обработкой, хранением, учетом персональных данных (далее – ПДн).

1.3. Работник допускается к работе после изучения положений и инструкций по правилам обработки ПДн и прохождения инструктажа.

1.4. Работник в процессе осуществления своих обязанностей по обработке ПДн руководствуется законодательством Российской Федерации и иными нормативными правовыми актами в области обеспечения безопасности ПДн, локальными нормативными актами ФГБОУ ВО «ХТУ».

1.5. Работа с ПДн строится на следующих принципах:

- принцип персональной ответственности за каждый документ независимо от типа носителя (бумажный, электронный) персональную ответственность несет конкретный работник;

- принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

2. ОСНОВНЫЕ ОБЯЗАННОСТИ

2.1. Знать и выполнять требования локальных нормативных актов Университета, затрагивающих вопросы защиты информации и обработки ПДн в подразделении.

2.2. Строго соблюдать установленные правила обеспечения защиты информации и обработки ПДн при работе с программными и техническими средствами автоматизированных информационных систем.

2.3. Соблюдать требования по защите информации и ПДн, правила работы со съемными машинными носителями информации, обеспечивать организационные меры по защите информации и ПДн.

2.4. Взаимодействовать с работниками отдела обеспечения защиты информации по вопросам, связанным с выполнением требований по обработке ПДн.

2.5. Соблюдать требования по учету, хранению и использованию электронных и материальных носителей информации, предназначенных для хранения ПДн.

2.6. Знать перечень установленных в подразделении технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием.

2.7. Соблюдать утвержденный порядок проведения работ по установке, модернизации и устранению неисправностей аппаратных и программных средств компьютеров и серверов из состава информационных систем.

2.8. Ежедневно контролировать целостность печатей и пломб на допущенных к обработке персональных данных защищенных устройствах, компьютерах и серверах подразделения.

2.9. Соблюдать порядок использования и обеспечения сохранности персональных устройств идентификации пользователей.

2.10. Немедленно поставить в известность руководителя и ответственного за обеспечение безопасности ПДн своего подразделения в случаях:

- несанкционированного доступа или разрушения целостности ПДн;
- утери устройства личной идентификации;
- при подозрении в компрометации личных ключей и паролей;
- при обнаружении изменений в размещении средств вычислительной техники, нарушении целостности пломб (наклеек, нарушении или несоответствии номеров печати);
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПЭВМ, выхода из строя

или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.);

- некорректного функционирования установленных на ПЭВМ технических средств защиты;

- непредусмотренных на ПЭВМ отводов кабелей и подключенных устройств.

2.11. Работникам запрещается:

- использовать компоненты средств вычислительной техники автоматизированных систем в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно программных средств ПЭВМ или устанавливать дополнительно любые программные и аппаратные средства;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- оставлять в помещении посторонних лиц, одних без присмотра;

- записывать и хранить ПДн на неучтенных носителях информации;

- записывать и хранить пароли, ключи доступа на видном месте;

- оставлять включенной без присмотра на любое время автоматизированную систему, не активировав средства защиты от несанкционированного доступа;

- передавать кому-либо свой личный идентификатор, кроме ответственного лица за обеспечение безопасности ПДн;

- использовать личные идентификаторы для формирования цифровой подписи любых электронных документов, кроме как регламентированных технологическим процессом на рабочем месте;

- оставлять без личного присмотра на рабочем месте или где бы то ни было свои личный идентификатор, машинные носители и распечатки, содержащие ПДн.

3. ПРАВА И ПОЛНОМОЧИЯ

3.1. Обращаться за помощью и консультациями в отдел информационной безопасности университета.

3.2. Участвовать в разработке мероприятий по совершенствованию защиты информации и обработки ПДн.

3.3. Обращаться к руководителю подразделения или ответственному за обеспечение защиты ПДн в подразделении с предложением о приостановке процесса обработки ПДн в случаях нарушения установленной технологии обработки или требований по защите информации и ПДн.

3.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты информации и обработки ПДн, несанкционированного доступа, утраты, порчи защищаемых ПДн и технических средств из состава информационных систем.

3.5. Подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты информации и обработки ПДн в подразделении.

4. ОТВЕТСТВЕННОСТЬ

4.1. Работник несет персональную ответственность за полноту и своевременное выполнение требований федеральных законов, нормативных документов в области защиты информации и обработки ПДн, а также настоящей Инструкции.

4.2. Работник, виновный в нарушении норм, регулирующих получение, обработку, защиту и передачу посторонним лицам ПДн, привлекается к дисциплинарной ответственности в порядке, установленном Трудовым кодексом Российской Федерации, локальными нормативными актами ФГБОУ ВО «ХТУ», а также к административной или уголовной ответственности в порядке, установленном законодательством Российской Федерации.

Приложение №4
к приказу ФГБОУ ВО «ХТУ»
от 18.02.2026г. № 322

ИНСТРУКЦИЯ ПО НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ФГБОУ ВО «ХЕРСОНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция по неавтоматизированной обработке персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Херсонский технический университет» разработана на основании требований Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», устанавливает порядок обработки, распространения и использования персональных данных в университете.

1.2. Основные термины:

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если действия с персональными данными в отношении каждого из субъектов персональных данных осуществляются при непосредственном участии человека. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе данных либо были извлечены из нее.

1.3. Обработка персональных данных осуществляется Университетом в соответствии с законодательством Российской Федерации и локальными актами Университета.

2. ПОРЯДОК ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации персональных данных на отдельных

материальных носителях (далее – материальные носители), в специальных разделах или на полях форм (бланков).

2.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, должны использоваться отдельные материальные носители.

2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными нормативными актами Университета.

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

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации (при необходимости получения письменного согласия на обработку персональных данных);

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

2.5. При ведении журналов (реестров, книг), содержащих персональные

данные, необходимые для однократного пропуска субъекта персональных данных на территорию Университета, должны соблюдаться следующие условия:

2.5.1. Необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена нормативным актом Университета, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию Университета;

2.5.2. Копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается.

2.5.3. Персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию Университета.

2.6. В случае, когда материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

- при необходимости уничтожения части персональных данных уничтожается материальный носитель с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

2.7. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

2.8. Правила, предусмотренные пунктами 2.6 и 2.7 настоящей Инструкции, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе

персональных данных и информации, не являющейся персональными данными.

2.9. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

3.2. Работникам обрабатывающим персональные данные, запрещается разглашать информацию, содержащую персональные данные.

3.3. Должно быть обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.4. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

3.5. Документы, содержащие персональные данные, должны обрабатываться отдельно от других документов. На документах должна указываться пометка «Персональные данные». Документы должны храниться в запираемых шкафах и сейфах. Ключи от них должны находиться у ответственных за данную работу лиц.

3.6. На персональных ЭВМ, дисках, папках и файлах, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы).

3.7. Учет съемных носителей информации с персональными данными допускается производить по установленным для этого учетным формам.

3.8. На носителях информации проставляются любым доступным способом следующие учетные реквизиты: учетный номер и дата, пометка «Персональные данные», подпись ответственного работника.

3.9. Запрещается хранение съемных носителей с персональными данными вместе с носителями открытой информации, на рабочих столах, либо

оставление их без контроля ответственных лиц или передача на хранение другим лицам.

3.10. Носители информации должны храниться в местах, недоступных для посторонних лиц.

3.11. Запрещается вынос съемных носителей с персональными данными из служебных помещений.

3.12. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся на них сведений немедленно ставятся в известность ответственный за обработку персональных данных и руководитель соответствующего структурного подразделения Университета.

3.13. По факту утраты носителя составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей персональных данных.

3.14. Съемные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется соответствующей комиссией, состав которой утверждается приказом Университета. По результатам уничтожения носителей составляется акт соответствующей формы.

3.15. На период обработки информации в помещении могут находиться лица, допущенные в установленном порядке к обрабатываемой информации.

3.16. В случае размещения в одном помещении нескольких технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации.

3.17. Передача персональных данных допускается только в случаях, установленных законодательством Российской Федерации в соответствии с действующими локальными нормативными актами Университета, по письменному поручению соответствующего руководителя.

3.18. По окончании обработки информации оператор обязан произвести стирание остаточной информации на жестком диске и в оперативной памяти компьютера.

3.19. При увольнении или переводе оператора автоматизированной системы ответственное лицо должно принять организационные меры по оперативному изменению паролей (идентификаторов).

3.20. Запрещаются обработка и хранение сведений о персональных данных на ПЭВМ, подключенной к сети, имеющей доступ к Интернету без межсетевого экрана, а также их передача по незащищенным каналам связи.