Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный медицинский университет» Министерства здравоохранения Российской Федерации

ФГБОУ ВО ОрГМУ Минздрава России

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 009FC4DA3211AF7E63EF4688F649F8E6D5
Владелец: Мирошниченко Игорь Васильевич
Действителен: с 19.10.2022 до 12.01.2024

Приложение к приказу
ФГБОУ ВО ОрГМУ Минздрава России
№ ___от «___»_____20__ г.

ПОЛОЖЕНИЕ

«Об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

П 171.01–2018

Оренбург 2018

Содержание

1 Назначение

1.1 Положение «Об организации и проведении работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных» (далее – Положение) определяет требования в Университете:

- к работе персонала в информационной системе персональных данных (далее – ИСПДн),
- обеспечению безопасности персональных данных (далее ПДн) при их обработке,
- порядку разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных,
- использованию средств защиты информации,
- разработке и принятию мер по предотвращению возможных опасных последствий таких нарушений,
- порядку приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления,
- порядку обучения персонала практике работы в ИСПДн,
- порядку проверки электронного журнала обращений к ИСПДн,
- порядку контроля соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией,
- исполнения правил обновления общесистемного и прикладного программного обеспечения, правил организации антивирусной защиты и парольной защиты ИСПДн,
- порядку охраны и допуска посторонних лиц в помещения ограниченного доступа.

1.2 Данное Положение разработано в целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

1.3 Положение разработано отделом комплексной безопасности.

2 Область применения

Требования данного Положения обязательны для выполнения всеми структурными подразделениями Университета.

3 Нормативные ссылки

В настоящем Положении использованы ссылки на следующие нормативные документы:

- Конституция Российской Федерации;
- Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149–ФЗ;
- Федеральный закон Российской Федерации от 27.07.2006 № 152–ФЗ «О персональных данных»;
- Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 г. № 188;
- Постановление Правительства Российской Федерации от 21 марта 2012 г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- Положение П 059.01–2018 «Об обработке персональных данных»
- Стандарт Организации СТО 003.01–2018 «Управление документированной информацией»

4 Термины и определения

В настоящем Положении используются следующие термины и их определения:

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

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила

разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Обработка информации – действия (операции) с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

Оператор – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных. В случае обработки персональных данных под оператором понимается государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

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

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

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

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

Уничтожение информации – действия, в результате которых становится невозможным восстановить содержание информации в информационной системе и (или) в результате которых уничтожаются материальные носители информации.

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Нарушения – действия, связанные с неисполнением требований руководящих документов по информационной безопасности, применению средств защиты информации и разграничения доступа, использованию технического, информационного и программного обеспечения ИСПДн. По степени их опасности делятся на нарушения первой, второй и третьей категории:

- К нарушениям первой категории относятся нарушения, повлекшие за собой разглашение (утечку) защищаемых сведений, утрату содержащих их машинных носителей информации и машинных документов, уничтожение (искажение) информационного и программного обеспечения, выведение из строя технических средств.
- К нарушениям второй категории относятся нарушения, в результате которых возникают предпосылки к разглашению (утечке) защищаемых сведений или утрате содержащих их машинных носителей информации и машинных документов, уничтожению (искажению) информационного и программного обеспечения, выведению из строя технических средств.
- Остальные нарушения относятся к нарушениям третьей категории.

5 Обозначения и сокращения

В настоящем Положении использованы следующие обозначения и сокращения:

- ВТСС – Вспомогательные технические средства и системы;
- ЖМД – Жесткий магнитный диск;
- ИС – информационная система;
- ИСПД (ИСПДн)– информационная система персональных данных (информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств);
- НСД – несанкционированный доступ;
- ОБ – Обеспечение безопасности;
- ОТСС – Основные технические средства и системы;
- ПД (ПДн) – персональные данные;

- ПО – программное обеспечение;
- РФ – Российская Федерация;
- СВТ – средства вычислительной техники;
- СЗИ – Система защиты информации;
- СМК– Система менеджмента качества;
- СТО – Стандарт организации;
- Университет – Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский медицинский университет» Минздрава России;
- ФЗ – федеральный закон;
- ФСБ – Федеральная служба безопасности;
- ФСТЭК– Федеральная служба по техническому и экспортному контролю;
- ЦИТ – Центр информационных технологий.

6 Ответственность

6.1 Специалисты ЦИТ несут ответственность за:

- проведение резервного копирования в ИСПДн с периодичностью не менее 1 раза в месяц;
- проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных;
- проведение мероприятий антивирусной защиты в ИСПДн;
- несоблюдение требований настоящего Положения.

6.2 Администратор безопасности, равно как и ответственный за защиту информации несут ответственность за:

- организацию мероприятий по восстановлению средств защиты информации возлагается администратора безопасности;
- организацию аттестации ИСПДн;
- проведение комплекса мероприятий по защите ПДн, при их обработке в ИСПДн;
- расследование инцидентов, связанных с ИСПДн;
- несоблюдение требований настоящего Положения.

6.3 Внутренний контроль за соблюдением Университетом законодательства Российской Федерации и локальных нормативных актов в области персональных данных, в том числе требований к защите персональных данных, настоящей Политике, осуществляется лицом, ответственным за организацию защиты персональных данных в Университете. Лицо, ответственное за организацию защиты персональных данных устанавливается приказом Ректора.

6.4 Персональная ответственность за соблюдение требований законодательства Российской Федерации и локальных нормативных актов Университета в области персональных данных, а также за обеспечение

конфиденциальности и безопасности персональных данных, на основании Реестра операторов, осуществляющих обработку персональных данных (регистрационный номер 08–0028026), возлагается на Ректора Университета.

6.5 Сотрудники Университета, допустившие нарушение норм, регулирующих обработку и защиту персональных данных субъектов персональных данных, привлекаются к дисциплинарной, материальной, гражданско–правовой, административной и уголовной ответственности в порядке, установленном Трудовым кодексом Российской Федерации, Кодексом Российской Федерации об административных правонарушениях, Уголовным кодексом Российской Федерации и иными федеральными законами.

7 Порядок работы персонала в части обеспечения безопасности ПДн при их обработке в ИСПДн

7.1 Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа Университета.

7.2 С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн приказом Ректора Университета назначаются администратор безопасности; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности ответственный за защиту информации.

7.3 Пользователь ИС имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. Полномочия пользователей к информационным ресурсам определяются политикой разграничения доступа (с градацией администраторы, пользователи, сторонние лица), устанавливаемой для каждого сотрудника, руководителем ЦИТ, персонально. При этом для хранения информации, содержащей ПДн, разрешается использовать только носители информации, расположенные в пределах локальной сети Университета.

7.4 Пользователь несет ответственность за правильность включения и выключения СВТ, входа в систему и все действия при работе в ИСПДн.

7.5 Вход пользователя в систему может осуществляться по выдаваемому ему идентификатору (логин) и по персональному паролю, выдаваемому руководителем ЦИТ. Персональные идентификаторы могут быть изменены в соответствии с параграфом 11 настоящего положения, в случаях компрометации, либо расторжения трудового договора.

7.6 Копирование персональных данных на внешние устройства, а также устройства вне локальной сети, без согласия субъекта, запрещено.

7.7 При работе со съемными машинными носителями информации, в случае согласия субъекта, пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных, лицензионных антивирусных программ, установленных на компьютерах ИСПДн, контролировать отсутствие на магнитных носителях остаточной

информации по окончании работы. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

7.8 Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и **обязан**:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

– знать и строго выполнять требования законодательных актов Российской Федерации в области защиты персональных данных;

– хранить в тайне свой пароль (пароли). В соответствии с п.п. 11.5 и 11.6 данного Положения и с установленной периодичностью менять свой пароль (пароли);

– хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

– выполнять требования настоящего Положения в полном объеме.

7.9 Немедленно известить ответственного за защиту информации и (или) администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

– нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее – НСД) к данным защищаемым СВТ;

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

– отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

– некорректного функционирования установленных на компьютеры технических средств защиты;

– непредусмотренных отводов кабелей и подключенных устройств.

7.10 Пользователю ИС категорически **запрещается**:

– использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;

– самовольно вносить какие–либо изменения в конфигурацию аппаратно–программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

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

– записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

– оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

– оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

– размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.

7.11 Администратор безопасности (а при его отсутствии – ответственный за защиту информации) обязан:

– знать состав основных и вспомогательных технических систем, и средств (далее – ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения в ИСПДн;

– контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах. В случае выявления нарушений составляется акт (Приложение 1), который визируется

– производить необходимые настройки подсистемы управления доступом установленных в ИСПДн средств защиты информации (далее – СЗИ) от НСД и сопровождать их в процессе эксплуатации, при этом:

- реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);
- контролировать доступ лиц к ИСПДн в соответствии со списком сотрудников, допущенных к работе (просмотр системных журналов);
- проводить инструктаж сотрудников–пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации. План инструктажа и сроки его проведения устанавливается приказом Ректора.
- контролировать своевременное (не реже чем один раз в течение 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;
- обеспечивать контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн, путем анализа системных журналов безопасности, аудита;

- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в 30 дней;
- осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации содержащих персональные данные.
- периодически тестировать функции СЗИ от НСД, в частности при изменении программной среды и полномочий исполнителей;
- восстанавливать программные средства и настройки СЗИ при сбоях, при поступлении соответствующего запроса от пользователя ИСПДн;
- контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования:
- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;
- контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, при необходимости внесения изменений, известить ответственного подрядчика, осуществляющего техническую поддержку данной системы;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта об уничтожении информации). Форма акта представлена в приложении 2, к настоящему положению.
- присутствовать (участвовать) в работах по внесению изменений в аппаратно–программную конфигурацию ИСПДн;
- поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положений в случае отказа средств и систем защиты информации принимать меры по их восстановлению;
- докладывать ответственному за защиту информации, о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;
- контролировать актуальность документации (в том числе лицензионной) на ИСПДн в соответствии с требованиями нормативных документов, в случае необходимости обновления, либо внесения изменений известить организацию-подрядчика, ответственную за техническую поддержку;
- по факту выявленных нарушений, изложенных п.п. 7.11. составляется акт. Форма акта представлена в приложении 1 к настоящему положению.

7.12. Администратор безопасности и ответственный за защиту информации имеют право:

– контролировать сотрудников–пользователей ИСПДн на предмет соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

– инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;

– требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

– участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

8 Порядок контроля, разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации

8.1 Контроль защиты информации в ИСПДн – комплекс организационных и технических мероприятий, которые проводятся в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно–технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

8.2 Основными задачами контроля являются:

– проверка организации выполнения мероприятий по защите информации в подразделениях, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

– выявление демаскирующих признаков объектов ИСПДн;

– уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно–технических воздействий на информацию;

– проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

– проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

– проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

– проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места.

– проверка выполнения комплекса мероприятий по пресечению нарушений требований (норм) защиты информации в ИСПДн;

проверка выполнения комплекса мероприятий по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

8.3 Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз, разрабатываемой организацией-подрядчиком, имеющей соответствующую лицензию (утверждается Ректором).

8.4 В ходе контроля проверяются:

– соответствие принятых мер по обеспечению безопасности персональных данных (далее – ОБ ПДн);

– своевременность и полнота выполнения требований настоящего Положения, а также иных нормативных актов Университета, в области защиты персональных данных;

– полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно–технических воздействий на информацию;

– эффективность применения организационных и технических мероприятий по защите информации;

– устранение ранее выявленных недостатков.

Кроме того, могут проводиться необходимые измерения и расчеты, приглашенными для этих целей специалистами организации, имеющей соответствующие лицензии ФСТЭК России.

8.5. Основными видами технического контроля являются визуально–оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно–технических воздействий на информацию.

8.6 Полученные в ходе ведения контроля результаты обрабатываются и анализируются администратором безопасности в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации администратор безопасности докладывает ответственному за безопасность для принятия решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения.

8.7 Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее – предпосылка).

- По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию администратора безопасности или ответственного за защиту информации проводится расследование.
- Для проведения расследования назначается комиссия с привлечением администратора безопасности. Состав комиссии утверждается приказом Ректора, в зависимости от характера выявленных нарушений. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования ответственный за безопасность принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению нарушений.

8.8 Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся, как правило, силами администратора безопасности и(или) ответственного за защиту информации, по согласованию с Ректором, план проверок утверждается приказом по Университету.

8.9 Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора безопасности, ответственного за защиту информации, ответственного за эксплуатацию объекта. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

8.10 Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в "Аттестате соответствия" (если проводилась аттестация) и (или) требованиям по обеспечению безопасности персональных данных.

8.11 В ходе обследования проверяется:

– соответствие текущих условий функционирования обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;

– соблюдение организационно–технических требований помещений, в которых располагается ИСПДн;

– сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;

– соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в настоящем положении;

– выполнение требований по защите информационных систем от несанкционированного доступа;

– выполнение требований по антивирусной защите.

8.12 Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, проложенных в выделенных и защищаемых помещениях, а также других нарушений и способов возникновения каналов утечки информации необходимо:

– тщательно осмотреть мебель, сувениры (особенно иностранного производства), оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проемы и т.д.;

– вскрыть и осмотреть розетки, выключатели осветительной сети, люки вентиляции и каналы скрытой проводки;

– проверить качество установки стеклопакетов оконных приемов;

– провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры), при необходимости для проведения данных видов работ могут привлекаться организации, имеющие соответствующие лицензии ФСБ России.

8.13 Государственный контроль состояния защиты информации осуществляется Федеральной службой по техническому и экспортному контролю России и Федеральной службой безопасности России в рамках их полномочий в соответствии с действующим законодательством Российской Федерации. Доступ представителей указанных федеральных органов исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, а также документа установленной формы на право проведения проверки.

9 Порядок обучения персонала практике работы в ИСПДн

9.1 Перед началом работы в ИСПДн пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации, утвержденных приказом Ректора.

9.2 Пользователи должны продемонстрировать администратору безопасности и (или) ответственному за защиту информации наличие необходимых знаний и умений для выполнения требований настоящего Положения.

9.3 Пользователи, демонстрирующие недостаточные умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего положения, к работе в ИСПДн не допускаются.

9.4 Для оказания методической помощи могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИСПДн, организаций–лицензиатов ФСТЭК России и ФСБ России.

9.5 К работе в ИСПДн допускаются только сотрудники, ознакомленные с требованиями настоящего положения, а также требованиями иных нормативных актов университета, в области защиты персональных данных и показавшие твердые теоретические знания и практические навыки.

10 Антивирусная защита

10.1 К использованию на компьютерах допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

10.2 Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется системным администратором ЦИТ.

10.3 Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

10.4 Ежедневно, в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

- Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
- Настройки средств антивирусной защиты должны быть выполнены в соответствии с требованиями безопасности персональных данных определенного для данной ИСПДн уровня защищенности.

10.5 Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

10.6 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, системным администратором должна быть выполнена антивирусная проверка ИСПДн.

10.7 На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

10.8 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором безопасности, либо системным администратором) должен провести внеочередной антивирусный контроль компьютера.

10.9 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

– приостановить обработку данных в ИСПДн;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные подразделения, использующие эти файлы в работе;

– совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;

– провести лечение или уничтожение зараженных файлов.

10.10 Контроль за организацией антивирусного защиты в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора по безопасности.

11 Политика парольной защиты

11.1 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора безопасности.

11.2 Личные пароли, по желанию пользователя, могут быть сгенерированы и распределены централизованно, либо выбираться самостоятельно с учетом следующих требований:

– пароль должен быть не менее 8 символов;

– в числе символов пароля ***обязательно*** должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

– символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования ПЭВМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– при смене пароля новое значение должно отличаться от предыдущих;

– пользователь не имеет права сообщать личный пароль другим лицам.

Владельцы паролей должны быть ознакомлены в устной форме с перечисленными выше требованиями и предупреждены об ответственности за

использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

11.3 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 360 дней.

11.4 Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться системным администратором (либо новым постоянным пользователем) немедленно после окончания последнего сеанса работы данного пользователя с системой на основании указания руководителя структурного подразделения (служебная записка) специалистам ЦИТ.

11.5 Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности,

11.7 В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по восстановлению парольной защиты.

11.7 Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности.

12 Аттестация информационной системы

12.1 Аттестация ИСПДн организуется Университетом, с привлечением подрядных организаций, обладающих соответствующей лицензией ФСБ и ФСТЭК России, и включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие СЗИ требованиям по безопасности информации.

12.2 Проведение аттестационных испытаний ИСПДн должностными лицами, осуществляющими проектирование и (или) внедрение СЗИ ИСПДн, не допускается.

12.3 В качестве исходных данных, необходимых для аттестации ИСПДн, используются модель угроз безопасности информации, акт классификации ИСПДн, акт определения уровня защищенности ПДн при их обработке в ИСПДн, техническое задание на создание СЗИ, проектная и эксплуатационная документация на СЗИ, организационно–распорядительные документы по защите информации, результаты анализа уязвимостей ИСПДн, материалы предварительных и приемочных испытаний СЗИ (при наличии).

12.4 Аттестация ИСПДн проводится в соответствии с программой и методиками аттестационных испытаний. Для проведения аттестации ИСПДн применяются национальные стандарты, а также методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4

пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085. По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии (не соответствии) ИСПДн требованиям по защите информации и аттестат соответствия в случае положительных результатов аттестационных испытаний.

12.5 При проведении аттестационных испытаний должны применяться следующие методы проверок (испытаний):

– экспертно–документальный метод, предусматривающий проверку соответствия СЗИ ИСПДн установленным требованиям по защите информации, на основе оценки эксплуатационной документации, организационно–распорядительных документов по защите информации, а также условий функционирования ИСПДн;

– анализ уязвимостей ИСПДн, в том числе вызванных неправильной настройкой (конфигурированием) программного обеспечения и средств защиты информации;

– испытания СЗИ путем осуществления попыток несанкционированного доступа (воздействия) к ИСПДн в обход ее СЗИ.

12.6 Допускается аттестация ИСПДн на основе результатов аттестационных испытаний выделенного набора сегментов ИСПДн, реализующих полную технологию обработки информации. В этом случае распространение аттестата соответствия на другие сегменты ИСПДн осуществляется при условии их соответствия сегментам ИСПДн, прошедшим аттестационные испытания. Сегмент считается соответствующим сегменту ИСПДн, в отношении которого были проведены аттестационные испытания, если для указанных сегментов установлены одинаковые классы защищенности, уровни защищенности, уровни важности, угрозы безопасности информации, реализованы одинаковые проектные решения по ИСПДн и ее СЗИ. В сегментах ИСПДн, на которые распространяется аттестат соответствия, Оператором обеспечивается соблюдение эксплуатационной документации на СЗИ и организационно–распорядительных документов по защите информации.

12.7 Особенности аттестации ИСПДн на основе результатов аттестационных испытаний выделенного набора ее сегментов, а также условия и порядок распространения аттестата соответствия на другие сегменты ИСПДн определяются в программе и методиках аттестационных испытаний, заключении и аттестате соответствия.

12.8 Повторная аттестация информационной системы осуществляется по окончании срока действия аттестата соответствия, который не может превышать 5 лет, или повышения класса защищенности информационной системы. При увеличении состава угроз безопасности информации или изменения проектных решений, реализованных при создании СЗИ, проводятся

дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

13 Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

13.1 Обеспечение защиты информации в ходе эксплуатации аттестованной ИСПДн осуществляется в соответствии с эксплуатационной документацией на СЗИ и законодательными нормами Российской Федерации, в области защиты персональных данных и в том числе включает:

– управление (администрирование) СЗИ;

– выявление инцидентов и реагирование на них;

– управление конфигурацией аттестованной ИСПДн и СЗИ;

– контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИСПДн.

13.2 В ходе управления (администрирования) СЗИ специалистами ЦИТ, либо администратором безопасности осуществляются:

– заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИСПДн и поддержание правил разграничения доступа в ИСПДн;

– управление средствами защиты информации в ИСПДн, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

– установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;

– централизованное управление СЗИ (при необходимости);

– регистрация и анализ событий в ИСПДн, связанных с защитой информации (далее – события безопасности);

– информирование пользователей об угрозах безопасности информации, о правилах эксплуатации СЗИ и отдельных средств защиты информации, а также их обучение;

– сопровождение функционирования СЗИ в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно–распорядительных документов по защите информации;

13.3 В ходе выявления инцидентов и реагирования на них администратором безопасности, либо лицом ответственным за защиту информации осуществляются:

– определение лиц, ответственных за выявление инцидентов и реагирование на них;

– обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИСПДн пользователями и администраторами;

– анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

13.4 В ходе управления конфигурацией, аттестованной ИСПДн и ее СЗИ администратором безопасности, осуществляются:

– поддержание конфигурации ИСПДн и ее СЗИ (структуры СЗИ, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на СЗИ (поддержание базовой конфигурации ИСПДн и ее СЗИ);

– управление изменениями базовой конфигурации ИСПДн и СЗИ, в том числе определение типов возможных изменений базовой конфигурации ИСПДн и СЗИ, санкционирование внесения изменений в базовую конфигурацию ИСПДн и СЗИ, документирование действий по внесению изменений в базовую конфигурацию ИСПДн и СЗИ, сохранение данных об изменениях базовой конфигурации ИСПДн и СЗИ, контроль действий по внесению изменений в базовую конфигурацию ИСПДн и ее СЗИ;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации ИСПДн и СЗИ на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн;

– определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПДн и СЗИ;

– внесение информации (данных) об изменениях в базовой конфигурации ИСПДн и СЗИ в эксплуатационную документацию на СЗИ;

– принятие решения по результатам управления конфигурацией о повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний.

13.5 В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн, администратором безопасности осуществляются:

– контроль за событиями безопасности и действиями пользователей в ИСПДн;

– контроль (анализ) защищенности информации, содержащейся в ИСПДн;

– анализ и оценка функционирования СЗИ, включая выявление, анализ и устранение недостатков в функционировании СЗИ;

– периодический анализ изменения угроз безопасности информации в ИСПДн, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

– документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн;

– принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) СЗИ, повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний.

14 Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации

14.1 Обеспечение защиты информации при выводе из эксплуатации, аттестованной ИС или после принятия решения об окончании обработки информации осуществляется Оператором в соответствии с эксплуатационной документацией на СЗИ и организационно–распорядительными документами по защите информации и, в том числе, включает:

– архивирование информации, содержащейся в ИС;

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

14.2 Архивирование информации, содержащейся в ИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности Оператора, сроки хранения определены сроком действия согласия Субъекта на обработку персональных данных.

14.3 Хранение архивной информации на бумажных носителях, производится в соответствии нормативными документами Университета.

14.4 При хранении архивной информации в электронном виде исключить доступ к ней третьих лиц.

14.5 Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю ИС или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

15 Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации

15.1 Системный администратор, обязан осуществлять периодическое резервное копирование информации.

15.2 Носители информации (ЖМД), предназначенные для создания резервной копии и хранения конфиденциальной информации выдаются установленным порядком руководителем, ответственным за защиту информации и (или) администратором. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору безопасности, или руководителю, или ответственному за защиту информации.

15.3 Перед резервным копированием пользователь или администратор безопасности обязан проверить электронный носитель (ЖМД) на отсутствие вирусов.

15.4 Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль в соответствии с разделом 7 настоящего Положения.

15.5 Запрещается запись посторонней информации на электронные носители резервной копии.

15.6 Порядок создания резервной копии:

– вставить в компьютер зарегистрированный электронный носитель для резервного копирования;

– выбрать необходимый каталог (файл) для создания резервного архива;

– при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;

– выполнить процедуру создания резервной копии;

– произвести копирование на отчуждаемый носитель;

– произвести отключение отчуждаемого носителя и убрать носитель в хранилище.

15.7 Хранение отчуждаемого носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище совместно с ключевой и аутентифицирующей информацией.

15.8 При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

15.9 Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

15.10 При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы и по согласованию с администратором безопасности, ответственным за защиту информации и, при условии проведенной аттестации информационной системы, представителем организации, проводившей аттестацию, оборудование передается в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

15.11 При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

15.12 При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных. Настройку данных средств должен выполнять сотрудник организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

15.13 Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

16 Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

16.1 Все изменения конфигураций технических и программных средств ИСПДн должны производиться только на основании служебной записки ответственного за эксплуатацию конкретного ИСПДн, на имя Ректора, либо в

связи с изменением в законодательстве Российской Федерации, в области персональных данных.

16.2 Право внесения изменений в конфигурацию аппаратно–программных средств, защищенных ИСПДн предоставляется:

– в отношении системных и прикладных программных средств – администратору безопасности и специалистам Центра Информационных технологий (в случае, если проводилась аттестация, по согласованию с органом по аттестации, проводившим аттестацию данной ИСПДн);

– в отношении аппаратных средств, а также в отношении программно–аппаратных средств защиты – администратору безопасности и специалистам Центра Информационных технологий (в случае, если проводилась аттестация, по согласованию с органом по аттестации, проводившим аттестацию данной ИСПДн);

– организации-подрядчику, уполномоченного на данный вид деятельности соответствующей лицензией, по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн.

16.3 Изменение конфигурации аппаратно–программных средств ИСПДн кем–либо, кроме администратора безопасности, специалистов Центра Информационных технологий и органа, уполномоченного на данный вид деятельности соответствующей лицензией, **запрещено**.

16.4 Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИСПДн инициируется служебной запиской ответственного за эксплуатацию ИСПДн, на имя Ректора, либо ответственного за защиту информации, с обоснованием необходимости внесения имений.

16.5 В служебной записке (далее заявка) могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

– установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн;

– обновление (замена) на компьютере(ах) программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ);

– удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

– наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного компьютера.

16.7 Заявка ответственного за эксплуатацию ИСПДн, в которой требуется произвести изменения конфигурации передается для ознакомления

администратору безопасности, который, утверждает производственную необходимость проведения указанных в заявке изменений.

16.8 Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производится системным администратором, либо администратором безопасности по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн. Работы производятся в присутствии ответственного за эксплуатацию данной ИСПДн.

16.9 Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

16.10 Установка и обновление ПО (системного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, прикладного ПО – с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

16.11 Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

16.12 После установки (обновления) ПО, администратор безопасности, либо специалист ЦИТ, должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их.

16.13 При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за защиту информации, который в свою очередь связывается с сотрудниками органа по аттестации (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкциям. В данном случае администратор безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

16.14 Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с отметками о внесении изменений в состав программных средств, должны храниться у ответственного за защиту информации.

16.15 Копии заявок могут храниться у администратора безопасности:

– для восстановления конфигурации ИСПДн после аварий;

– для контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;

– для проверки правильности установки и настройки средств защиты ИСПДн

16.16 Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора безопасности и сотрудника ответственного за эксплуатацию данной ИСПДн.

16.17 С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном компьютере.

16.18 Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя («группового имени») ***запрещено.***

16.19 Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется служебной запиской на имя руководителя Центра информационных технологий от ответственного за эксплуатацию данной ИСПДн. В заявке указывается:

– содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);

– должность (с полным наименованием организации), фамилия, имя и отчество сотрудника;

– имя пользователя (учетной записи) данного сотрудника;

– полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

16.20 На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, специалист ЦИТ производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании.

16.21 После внесения изменений в списки пользователей специалист ЦИТ должен обеспечить настройки средств защиты, соответствующие требованиям безопасности, указанной ИСПДн.

16.22 Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное (–ые) значение (–ия) пароля (–ей), которое (–ые) он обязан сменить при первом же входе в систему.

16.23 Исполненные заявка и задание передаются на хранение пользователю. Они могут впоследствии использоваться:

– для восстановления полномочий пользователей после аварий ИСПДн;

– для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;

– для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

17 Порядок контроля соблюдения условий использования средств защиты информации, в том числе криптографических

17.1 Технические средства защиты информации являются важным компонентом ОБ ПДн.

17.2 Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как сотрудниками, обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

17.3 Право проверки соблюдения условий использования средств защиты информации имеют:

– руководитель;

– ответственный за защиту информации;

– администратор безопасности.

17.4 Пользователю ИСПДн категорически запрещается:

– обрабатывать конфиденциальную информацию с отключенными СЗИ;

– менять настройки СЗИ.

17.5 Запрещается менять настройки программно–аппаратных СЗИ предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, без согласования с этой организацией.

17.6 Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлено нарушение требования п. 17.4, то составляется акт о выявленных нарушениях, который передается ответственному по защите информации для дальнейших разбирательств.

17.7 Криптографические средства защиты информации должны использоваться в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими

18 Порядок охраны и допуска посторонних лиц в защищаемые помещения

18.1 Вскрытие и закрытие защищаемых помещений осуществляется сотрудниками, работающими в данных помещениях. Список сотрудников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения

утверждается руководителем и передаётся на пост охраны, руководителем подразделения.

18.2 При отсутствии сотрудников, ответственных за вскрытие (сдачу под охрану) помещений, данные помещения могут быть вскрыты комиссией, состоящей из начальника отдела комплексной безопасности, специалиста по информационной безопасности, руководителя структурного подразделения и специалиста материального стола, о чем составляется акт вскрытия (Приложение 3).

18.3 При закрытии помещений и сдачей их под охрану сотрудники, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы и оргтехнику, а документы и носители информации на которых содержится конфиденциальная информация убираются для хранения в опечатываемый сейф (металлический шкаф).

18.4 При обнаружении нарушений целостности оттисков печатей, повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт о выявленных нарушениях в присутствии материально-ответственного лица. О происшествии немедленно сообщается руководителю и (или) ответственному за защиту информации. Руководителем принимаются меры по охране места происшествия и до прибытия должностных лиц в помещение никто не допускается, путем ограничения доступа в помещение.

18.5 Руководитель, ответственный за защиту информации и администратор безопасности организуют проверку ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации.

18.6 При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или ответственному за защиту информации, или руководителю, или администратору безопасности. Помещения вскрывать запрещается.

18.7 Помещения вскрываются ответственным за помещение, или руководителем, или ответственным за защиту информации в присутствии сотрудника охраны с составлением акта.

18.8 В соответствии с требованиями данного Положения при обработке защищаемой информации в ИСПДн исключить не контролируемое пребывание посторонних лиц в пределах границ контролируемой зоны ИСПДн, определенных соответствующим приказом Университета.

19 Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации

19.1 В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию,

использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн. Не допускается стирание неисправных носителей и передача их в сервисный центр для ремонта.

19.2 Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в сертифицированные средства защиты информации).

19.3 Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

19.4 Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

19.5 По факту уничтожения или стирания носителей составляется акт об уничтожении (приложение 2).

19.6 Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: ответственный за эксплуатацию ИСПДн, ответственный за защиту информации, администратор безопасности, при наличии информации на компакт-дисках – специалист ЦИТ.

20 Хранение документированной информации

При выполнении требований данного положения в подразделениях создается следующая документированная информация:

№ п/п	Наименование документированной информации	Формат документации (бумажный/ электронный)	Место хранения	Срок хранения
1	Акт «О выявленных в ходе проверки нарушениях»	бумажный	Ответственный за ИСПДн	в течение срока действия аттестата соответствия, при его отсутствии не более 75 лет
2	Акт на уничтожение машинных (бумажных) носителей защищаемой информации, не содержащей сведения,	бумажный	Отдел комплексной безопасности	в течение срока действия аттестата соответствия, при его отсутствии не более 75 лет

№ п/п	Наименование документированной информации	Формат документации (бумажный/ электронный)	Место хранения	Срок хранения
	составляющие государственную тайну			
3	Акт о вскрытии защищаемого помещения.	бумажный	Отдел комплексной безопасности	в течение срока действия аттестата соответствия, при его отсутствии не более 75 лет
4	приказ «о назначении ответственных за организацию защиты персональных данных»	бумажный/ электронный	ОДО	постоянно
5	приказ Ректора «об утверждении состава комиссии по расследованию выявленных в ходе проверки нарушений»	бумажный/ электронный	ОДО	постоянно
6	приказ Ректора «об организации комплекса мероприятий по проверке ИСПДн»	бумажный/ электронный	ОДО	постоянно
7	приказ Ректора «об организации инструктажа по информационной безопасности»	бумажный/ электронный	ОДО	постоянно
8	приказ Ректора «об утверждении перечня инструкций по использованию программных и технических средств»	бумажный/ электронный	ОДО	постоянно

Приложение 1
(обязательное)

Форма акта о выявленных нарушениях

АКТ
О выявленных в ходе проверки нарушениях
от «___» _____ _____ г.

Дата и время начала проверки: «____» _____ __ г. ____ ч. ____ мин.
Дата и время завершения проверки: «____» _____ _____ г. ____ ч. ____ мин.

Настоящий акт составлен по результатам проверки
_____,
(Наименование объекта проверки)

проведенной в соответствии с
_____ .
(наименование и реквизиты приказа о проведении проверки)

Проверка проводилась по адресу_____
_____.
(Указывается место установки ИСПДн, либо место проведения проверки)

В ходе проверки установлено следующее.
_____
_____
_____
_____
_____.

В ходе проверки выявлены нарушения:
1._____ ;

2._____;

3._____.

Настоящий акт составлен в двух экземплярах.

Приложения:

1. на ___ л.
2. на ___ л.
3. на ___ л.

Председатель комиссии

_____

(подпись) (Ф.И.О.)

Члены комиссии:

_____

(подпись) (Ф.И.О.)

_____

(подпись) (Ф.И.О.)

Акт проверки получен:

_____ _____ _____

(наименование должности) *МП* *(подпись)* *(Ф.И.О.)*

«____» _____ _____ г.

С актом проверки ознакомлен:

_____ _____ _____

(наименование должности руководителя структурного подразделения) *МП* *(подпись)* *(Ф.И.О.)*

«____» _____ _____ г.

Приложение 2

(обязательное)

Форма акта об уничтожении

АКТ

На уничтожение машинных (бумажных) носителей защищаемой информации, не содержащей сведения, составляющие государственную тайну

Комиссия в составе:

Председатель комиссии:	
Члены комиссии:	

составила настоящий акт в том, что перечисленные в нем машинные (бумажные) носители защищаемой информации, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация), подлежат уничтожению как утратившие практическое значение и непригодные для перезаписи.

№ п/п	Вид носителя	Учетный номер носителя	Дата поступления	Краткое содержание информации

Всего подлежит списанию и уничтожению _____ наименований машинных (бумажных) носителей защищаемой информации
(прописью)

Правильность произведенных записей в акте проверил:

_____
(подпись)

Машинные (бумажные) носители защищаемой информации перед уничтожением сверили с записями в акте и полностью уничтожили путем

_____

_____

«_____»_____20__г.

Председатель комиссии:

Подписи членов комиссии:

Ф.И.О.	Подпись

Приложение 3
(обязательное)

Форма акта вскрытия помещения.

АКТ
О вскрытии защищаемого помещения.

"__" _____ 20___ г.

_____
(должность, фамилия, инициалы должностного лица, наименование органа)

на основании _____
в присутствии комиссии, в составе:

Должность	ФИО
Председатель комиссии	
Члены комиссии	

с привлечением _____
(должность, фамилия, инициалы приглашенного специалиста, наименование документа, удостоверяющего его личность)

произвел вскрытие _____
(наименование помещения)
расположенного по адресу: _____

В ходе осмотра должностным лицом предприняты следующие действия:
_____

В результате проведенных действий: _____
_____.

Помещение опечатано _____
(должность, фамилия, инициалы проверяющего)

Второй экземпляр акта получил: _____
(должность, фамилия, инициалы, дата, подпись представителя проверяемого субъекта)

Председатель комиссии:

Подписи членов комиссии:

Ф.И.О.	Подпись

Лист регистрации изменений

№ п/п	№ изменения	Дата и номер приказа о внесении изменений	Должность, Ф.И.О.	Подпись
1	2	3	4	5