ОРЛОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени И.С. Тургенева

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ОРЛОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени И.С. ТУРГЕНЕВА»
(ОГУ им. И.С.Тургенева)

12.10.2015 П Р И К А З № 927

Об утверждении положения по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПДН ОГУ имени И.С. Тургенева

В целях выполнения требований Федерального закона Российской Федерации от 27.07.2006 года № 152-ФЗ «О персональных данных», «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утвержденных приказом Гостехкомиссии России от 20.08.2002 года № 282, приказов ФСТЭК России от 11.02.2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», других законодательно - нормативных документов Российской Федерации, Орловской области и документов федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее - ОГУ имени И.С. Тургенева) в области безопасности информации,

п р и к а з ы в а ю:

1. Утвердить положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПДН ОГУ имени И.С. Тургенева

Ректор О.В. Пилипенко

СОГЛАСОВАНО

Директор департамента информатизации и перспективного развития А.В. Коськин

Начальник ПУ Т.И. Ератова

УТВЕРЖДАЮ

Ректор
ФГБОУ ВО «Орловский государственный университет И.С. Тургенева»

_____ О.В. Пилипенко

«11» октября 2017 г.

ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДН

Орел, 2017 г.

СОДЕРЖАНИЕ

Приложения, оформленные отдельными документами:

Приложение 1. Инструкция администратора безопасности ИСПДн.
Приложение 2. Инструкция по работе пользователей ИСПДн
Приложение 3. Инструкция администратора системного ИСПДн
Приложение 4. Инструкция ответственного за защиту информации
Приложение 5. Инструкция по организации парольной защиты в ИСПДн
Приложение 6. Инструкция по организации антивирусной защиты в ИСПДн
Приложение 7. Инструкция о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в ИСПДн

1. Общие положения

Данное «Положение по организации и проведению работ в федеральном государственном бюджетном образовательном учреждении высшего образования "Орловском государственном университете им. И.С. Тургенева" по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных», Федеральным законом Об информации, информатизации и защите информации" от 20.02. 95 г. № 24-ФЗ, Указом Президента Российской Федерации от 5 декабря 2016 г. №646 "Доктрина информационной безопасности Российской Федерации", Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», «Положением о методах и способах защиты информации в информационных системах персональных данных» утвержденным приказом ФСТЭК России от 5 февраля 2010 г. № 58, в целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн).

Положение устанавливает порядок организации и проведения работ по обеспечению безопасности персональных данных в ИСПДн. В документе определены:

перечень мероприятий по защите персональных данных;

система управления безопасностью персональных данных;

порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации;

порядок контроля защиты персональных данных;

порядок обучения персонала практике работы в ИСПДн;

порядок проверки электронного журнала обращений к ИСПДн;

правила антивирусной и парольной защиты, обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн;

порядок контроля соблюдения условий использования средств защиты информации;

порядок охраны и допуска посторонних лиц в помещения ИСПДн.

2. Порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в ИСПДн

Обеспечение безопасности персональных данных (далее – ОБ ПДн) осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных (далее – СЗ ПДн), направленных на минимизацию ущерба от возможной реализации угроз безопасности персональным данным.

2.1. Организационные меры

Организационные меры по защите персональных данных включают в себя следующие мероприятия:

2.1.1. Определение перечня персональных данных, обрабатываемых в ИСПДн.

2.1.2. Определение цели обработки персональных данных.

2.1.3. Определение сроков обработки и хранения персональных данных.

2.1.4. Назначение ответственных за обеспечение безопасности персональных данных.

Для разработки и осуществления мероприятий по организации и обеспечению безопасности персональных данных при их обработке в ИСПДн руководителем организации назначаются должностные лица, ответственные за обеспечение безопасности персональных данных (далее – «Ответственные лица»). Основные обязанности ответственных лиц за обеспечение безопасности персональных данных, их права и обязанности определены в разделе 2.3.2 настоящего Положения.

2.1.5. Определение круга лиц, допущенных к обработке персональных данных.

К обработке персональных данных допускаются сотрудники ФГБОУ ВО «Орловский государственный университет им. И.С. Тургенева», которые должны быть подготовлены к работе с информацией, требующей защиты.

Составляется список сотрудников, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей.

Разрабатывается система доступа к данным сотрудников к информационным ресурсам ИСПДн.

Права доступа администратору безопасности и пользователям оформляются в виде матрицы доступа к защищаемым информационным ресурсам.

Формируется «Список пользователей ИСПДн и установленные им права доступа к информационным ресурсам». Они приведены в документе:

– Список пользователей и установленные им права доступа к информационным ресурсам ИСПДн;

2.1.6. Организация доступа в помещения, где осуществляется обработка персональных данных.

Порядок охраны помещений ИСПДн, организация доступа в эти помещения определены в разделе 11.

2.1.7. Обучение сотрудников.

Требования по обучению лиц, обеспечивающих безопасность обработки персональных данных, а также сотрудников ФГБОУ ВО «Орловский государственный университет им. И.С. Тургенева», допущенных к обработке персональных данных, правила обработки персональных данных в соответствии с утвержденными требованиями, приведены в разделе 5.

2.1.8. Установление персональной ответственности за нарушения правил обработки персональных данных.

В должностные инструкции сотрудников, допущенных к обработке персональных данных, вносятся дополнения в части персональной ответственности за нарушение правил обработки персональных данных.

2.1.9. Учет применяемых технических средств защиты персональных данных.

При выборе технических (аппаратных, программных и программно-аппаратных) средств защиты следует использовать сертифицированные средства защиты информации. Перечень используемых средств защиты с указанием их заводского номера, сведений о сертификате соответствия, месте и дате установки приводится в техническом паспорте на соответствующую ИСПДн.

2.1.10. Учет носителей персональных данных.

В обязательном порядке должен быть организован учет всех защищаемых носителей персональных данных с помощью их маркировки и с занесением учетных данных в «Журнал регистрации, учета и выдачи носителей информации».

2.1.11. Разработка организационно–распорядительных документов.

Процесс получения, обработки, хранения, передачи и защиты персональных данных регламентируется данным Положением и необходимыми организационно-распорядительными документами.

2.2. Технические мероприятия

Технические меры защиты персональных данных предполагают использование программно–аппаратных средств защиты информации (далее – СЗИ). Количество СЗИ и степень защиты определяется нормативными документами в сфере защиты персональных данных.

Технические и программные средства, используемые для обработки персональных данных в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

2.3. Управление обеспечением безопасности персональных данных

Управление обеспечением безопасности персональных данных осуществляется Ответственными лицами, которые координируют действия подразделений ФГБОУ ВО «Орловский государственный университет им. И.С. Тургенева», контролируют реализацию требований безопасности персональных данных в ИСПДн.

2.3.1. Система управления обеспечением безопасности персональных данных

Систему управления обеспечением безопасности персональных данных (далее – ОБ ПДн) составляют:

ответственный за защиту информации в ИСПДн;

администратор безопасности ИСПДн;

руководители структурных подразделений ФГБОУ ВО «Орловского государственного университета им. И.С. Тургенева».

Основными задачами Ответственных лиц по вопросам защиты информации являются:

координация действий подразделений ФГБОУ ВО «Орловского государственного университета им. И.С. Тургенева», использующих ПДн, по вопросам ОБ ПДн;

организация работ по защите персональных данных в ИСПДн;

организация работы по обеспечению физической сохранности технических средств, программного обеспечения ИСПДн;

обеспечение защиты от несанкционированного доступа к персональным данным, обрабатываемым в ИСПДн;

регистрация событий, влияющих на безопасность персональных данных, обеспечение полной подконтрольности и подотчетности выполнения всех операций, совершаемых в ИСПДн;

обеспечение режима безопасности персональных данных при проведении всех видов деятельности;

своевременное выявление, оценка и прогнозирование источников угроз безопасности персональным данным;

анализ причин и условий, способствующих нанесению ущерба интересам ФГБОУ ВО «Орловский государственный университет им. И.С. Тургенева», нарушению нормального функционирования и развития ИСПДн;

выявление и локализация возможных каналов утечки персональных данных в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;

обеспечение возможности восстановления актуального состояния информационных ресурсов при нарушении безопасности персональных данных и ликвидации последствий этих нарушений;

определение потребностей ИСПДн, распределение имеющихся ресурсов и планирование финансового обеспечения работ по защите персональных данных;

контроль результативности системы ОБ ПДн;

организация обучения, переподготовки и повышения квалификации специалистов.

2.3.2. Функциональные обязанностями Ответственных лиц.

Функциональными обязанностями Ответственных лиц являются:

планирование работ по защите персональных данных в ИСПДн;

составление и ведение схемы информационных потоков, проведение их анализа с целью выявления недостатков в организации СЗПДн, составление и выполнение мероприятий по их устранению;

анализ состояния безопасности персональных данных и выработка подходов к обеспечению безопасности персональных данных в ИСПДн;

организация единой системы контроля состояния работ в области защиты персональных данных в ИСПДн и эффективности реализуемых мер защиты на объектах информатизации;

координация деятельности всех подразделений, использующих ИСПДн, по вопросам обеспечения безопасности персональных данных на всех этапах жизненного цикла;

разработка и внедрение нормативных и методических документов, регулирующих отношения в области защиты персональных данных;

подготовка проектов организационно–распорядительных документов и нормативных актов ИСПДн по вопросам обеспечения безопасности персональных данных;

методическое обеспечение деятельности по защите персональных данных при проведении работ по развитию и совершенствованию автоматизированной системы обработки информации;

взаимодействие со сторонними организациями, не входящих в систему ИСПДн, но использующих ПДн, по обеспечению безопасности персональных данных;

непосредственное обеспечение защиты информационных ресурсов ИСПДн с применением технических средств обработки, управление средствами защиты информации;

проведение инструктажей работников ФГБОУ ВО «Орловский государственный университет им. И.С. Тургенева» по мерам обеспечения безопасности персональных данных, обучение их работе с использованием средств защиты информации;

учет, хранение, и выдача носителей персональных данных, генерация паролей, ключей пользователей, используемых в средствах защиты информации, контроль соответствия программного обеспечения ИСПДн эталонному;

контроль правильности выполнения работниками ФГБОУ ВО «Орловский государственный университет им. И.С. Тургенева» требований безопасности персональных данных, учет случаев их нарушения, контроль эффективности принятых мер по защите персональных данных;

оказание консультационной и технической поддержки работникам ФГБОУ ВО «Орловского государственного университета им. И.С. Тургенева» при выполнении ими обязанностей по обеспечению безопасности персональных данных.

2.3.3. Права Ответственных лиц.

Ответственные лица имеют право:

осуществлять контроль деятельности структурных подразделений, использующих ИСПДн, по выполнению ими требований обеспечения безопасности персональных данных;

требовать от пользователей и обслуживающего персонала ИСПДн безусловного соблюдения установленной технологии обработки и требований нормативных актов по обеспечению безопасности персональных данных;

давать работникам, использующим ИСПДн, обязательные для исполнения указания по вопросам, входящим в компетенцию Ответственных лиц;

запрашивать и получать от структурных подразделений, использующих ИСПДн, сведения, справочные и другие материалы, необходимые для осуществления деятельности Ответственных лиц;

принимать меры при обнаружении несанкционированного доступа к информации ИСПДн, и незамедлительно докладывать о принятых мерах начальнику службы информационной безопасности, с представлением информации о субъектах, нарушивших режим доступа;

привлекать экспертов и специалистов в сфере защиты персональных данных для консультаций, подготовки заключений, рекомендаций и предложений;

обращаться к руководителю структурного подразделения с требованием о прекращении обработки персональных данных в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации.

На Ответственных лиц возлагается персональная ответственность за полноту и качество проводимых ими работ по обеспечению защиты персональных данных.

2.3.4. Основные обязанности лиц, обеспечивающих функционирование и использование ИСПДн

2.3.4.1 Ответственный за защиту информации Университета.

Ответственный за защиту информации ФГБОУ ВО «Орловский государственный университет им. И.С. Тургенева» назначается приказом Ректора. В пределах своих функциональных обязанностей он обеспечивает безопасность персональных данных, обрабатываемых, передаваемых и хранимых в ИСПДн.

В своей работе он руководствуется положениями федеральных законов и нормативных актов органов государственной власти Российской Федерации, нормативных документов ФСТЭК России, а также организационно–распорядительными документами организации по вопросам обеспечения безопасности персональных данных.

Ответственный за защиту информации:

осуществляет разработку требований по ОБ ПДн, а также контроль выполнения этих требований в ИСПДн;

организует и руководит выполнением работ по защите персональных данных в ИСПДн, обеспечивая эффективное применение организационных и инженерно-технических мер;

участвует в разработке технической политики и определении перспектив развития технических средств контроля, организует внедрение новых технических, аппаратных и программных средств защиты, исключающих или существенно затрудняющих несанкционированный доступ к защищаемой информации;

готовит предложения для включения в планы и программы работ организационных и инженерно-технических мер по защите информационных систем, в которых обрабатываются персональные данные;

организует проведение работ в области совершенствования систем защиты персональных данных и повышения их эффективности;

организует выполнение всего комплекса работ, связанных с защитой персональных данных, на основе разработанных программ и методик;

организует работу по сбору и систематизации необходимой информации об объектах, подлежащих защите, и охраняемых сведениях;

готовит данные о потребности в технических, аппаратных и программных средствах защиты информации;

обеспечивает контроль за выполнением требований нормативно-технической документации, за соблюдением установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты персональных данных;

координирует деятельность специалистов по защите персональных данных в ИСПДн.

2.3.4.2. Администратор безопасности персональных данных.

Администратор безопасности персональных данных в пределах своих функциональных обязанностей обеспечивает безопасность персональных данных, обрабатываемой, передаваемой и хранимой в подсистемах ИСПДн.

Администратор безопасности персональных данных руководствуется организационно-распорядительными документами организации по вопросам обеспечения безопасности персональных данных, «Инструкцией администратора безопасности ИСПДн (Приложение 1), настоящим положением.

Администратор безопасности персональных данных:

организует эксплуатацию технических и программных средств и систем защиты персональных данных;

обеспечивает контроль за администрированием и эффективным применением штатных средств защиты информации для операционных систем и систем управления

базами данных, администрирование дополнительных специализированных средств защиты и анализа защищенности ресурсов ИСПДн, а также поддержку функционирования средств, технологий и процессов ОБ ПДн;

обеспечивает контроль за работой пользователей ИСПДн, выявление попыток НСД к АРМ и защищаемым информационным ресурсам;

выполняет работы, связанные с обеспечением защиты персональных данных на основе разработанных программ и методик, соблюдения конфиденциальности;

участвует в обследовании объектов защиты, их классификации, аттестации и контроле;

формирует и распределяет ключевую информацию пользователей по средствам защиты;

обеспечивает допуск пользователей к работе в подсистеме ИСПДн путем настройки соответствующих средств защиты;

ведет учет наступления системных событий, связанных с инициализацией функций подсистемы ИСПДн, изменением ее конфигурации, а также изменением прав доступа сетевых сущностей (пользователей, информационных узлов, сетевых приложений и т.п.);

ведет контроль текущего функционального состояния ИСПДн, включающий просмотр журнала активных сеансов, контроль за работой конкретного АРМ и конкретного пользователя;

проводит обучение персонала и пользователей АРМ правилам работы со средствами защиты персональных данных;

осуществляет организацию антивирусной защиты, включая: централизованное управление средствами антивирусной защиты (далее – САЗ), установку, настройку и администрирование САЗ, а также контроль машинных носителей информации и файлов электронной почты, поступающих из подразделений организации и сторонних организаций;

обеспечивает текущий и периодический контроль работоспособности средств и систем защиты персональных данных, контроль соответствия настроек средств вычислительной техники и связи требованиям нормативных документов;

выполняет периодический аудит защищенности подсистем ИСПДн с использованием технических средств;

обеспечивает текущий контроль работоспособности средств контроля целостности эксплуатируемого на АРМ программного обеспечения с целью выявления несанкционированных изменений в нем;

докладывает непосредственному руководителю о выявленных нарушениях и несанкционированных действиях пользователей и персонала;

совместно с другими сотрудниками отдела информационных технологий принимает меры по восстановлению работоспособности средств и систем защиты информации;

2.3.4.3. Руководители структурных подразделений.

Руководители структурных подразделений организации, обеспечивающих эксплуатацию ИСПДн, выполняют обязанности по обеспечению и контролю за реализацией и выполнением требований по ОБ ПДн, применению мер защиты в своих подразделениях.

Обеспечивают координацию взаимодействия ответственного и администраторов безопасности по защите персональных данных и своего подразделения, в котором происходит обработка персональных данных.

Обеспечивают и контролируют выполнение требований ОБ ПДн.

2.3.4.4. Пользователи ИСПДн.

Непосредственно реализуют эксплуатацию ИСПДн, используя установленные режимы защиты персональных данных, обеспечивают строгое выполнение требований нормативных и организационно-распорядительных документов, определяющих порядок обеспечения безопасности персональных данных в ИСПДн.

Пользователи ИСПДн не имеют права использовать в неслужебных целях информационные ресурсы ИСПДн и обязаны хранить охраняемые законом персональные данные и не разглашать ставшую им известной в связи с исполнением должностных обязанностей информацию ограниченного доступа.

Порядок действий пользователей ИСПДн в части обеспечения безопасности персональных данных при их обработке в ИСПДн приведены в «Инструкции по работе пользователей ИСПДн» (Приложение 2).

3. Порядок резервирования информации

Настоящий порядок определяет организацию резервного копирования персональных данных, восстановления работоспособности технических средств и программного обеспечения системы управления базами данных и средств защиты персональных данных.

3.1. Порядок обеспечения резервного копирования персональных данных

Резервное копирование персональных данных применяется для оперативного восстановления данных в случае их повреждения, утраты, или по другим причинам.

Резервное копирование персональных данных осуществляется администратором безопасности в пределах своих полномочий в соответствии с графиком резервного копирования. График резервного копирования составляется для каждого вида персональных данных, подлежащей периодическому резервному копированию, и утверждается начальником службы информационной безопасности. Резервное копирование персональных данных производится в соответствии с документацией на используемое программное обеспечение. Носители, на которые осуществляется резервное копирование, периодически проверяются на отсутствие сбоев. Резервные копии персональных данных хранятся в отдельном помещении от используемых данных.

Восстановление персональных данных из резервной копии производится администраторами безопасности в пределах своих полномочий в соответствии с документацией на используемое программное обеспечение с составлением акта.

С целью поддержания возможности восстановления персональных данных в установленном порядке и за гарантированный промежуток времени проводятся регулярные проверки процедур восстановления. Периодичность проведения проверок устанавливает Ответственный за защиту информации.

Инструкция по архивированию и резервированию информации в ИСПДн представлена в Приложении 7.

3.2. Организация резервирования и восстановления работоспособности программного обеспечения баз данных и средств защиты персональных данных

Для обеспечения работоспособности программного обеспечения системы управления базами данных и средств защиты информации персональных данных в ИСПДн осуществляется резервирование специального программного обеспечения и программных средств защиты от НСД.

Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения возлагается на Администратора безопасности персональных данных.

4. Порядок контроля защиты персональных данных

Контроль защиты персональных данных в ИСПДн – комплекс организационных и технических мероприятий, которые осуществляются в целях исключения возможности несанкционированного доступа техническими и программными средствами к ПДн, а так же хищения технических средств и носителей информации, предотвращения программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности ИСПДн.

Основными задачами проверки защиты ПДн являются:

контроль выполнения мероприятий по защите персональных данных в ИСПДн;

выявление возможных каналов утечки персональных данных и несанкционированного доступа к ним программно-техническими средствами;

оценка результативности мероприятий по защите персональных данных;

проверка выполнения требований по антивирусной защите автоматизированных рабочих мест и серверов;

проверка знаний сотрудников по вопросам защиты персональных данных и их соответствия требованиям уровня подготовки для конкретного рабочего места;

оперативное принятие мер по пресечению нарушений требований защиты персональных данных в ИСПДн;

разработка предложений по устранению возможных каналов утечки информации, содержащей персональные данные.

При проведении проверки могут привлекаться специалисты органа по аттестации ИСПДн.

Невыполнение мероприятий по защите персональных данных считается потенциальной угрозой утечки информации

По каждому выявленному такому случаю для выяснения обстоятельств и причин невыполнения установленных требований по решению ответственного за проводится расследование. Для проведения расследования назначается комиссия с привлечением специалистов по защите информации.

Комиссия обязана установить:

имела ли место утечка персональных данных;

обстоятельства, ей сопутствующие;

лиц, виновных в нарушении предписанных мероприятий по защите персональных данных;

причины и условия, способствовавшие нарушению.

После окончания расследования ответственный за защиту информации информирует Ректора ФГБОУ ВО «Орловский государственный университет им. И.С. Тургенева» для разработки необходимых мероприятий по устранению недостатков.

Контроль защиты персональных данных осуществляется путем проведения проверок подсистем ИСПДн.

В ходе проверок устанавливается:

соответствие состава программно-технических средств, обрабатывающих персональные данные, данным «Технического паспорта на ИСПДн» и «Формуляра на АРМ»;

соответствие фактических пользователей и их прав доступа «Списку пользователей ИСПДн и установленные им права доступа к информационным ресурсам»;

проверка выполнения требований по размещению АРМ в рабочих помещениях, которые исключали бы возможность несанкционированного просмотра информации с экранов мониторов, с распечаток принтеров и с других устройств ввода/вывода информации лицами, не имеющими права доступа к персональным данным;

знания инструкций пользователя ИСПДн.

По результатам проверки составляется акт, который содержит выводы о состоянии обеспечения безопасности персональных данных и рекомендации по ее совершенствованию.

Одной из форм контроля защиты персональных данных является периодический контроль. Периодический контроль проводится с целью определения соответствия помещений, основных и вспомогательных технических средств и систем требованиям по защите персональных данных. Оно проводится не реже одного раза в год рабочей группой в составе администраторов безопасности, специалистов службы информационной безопасности и руководителя структурного подразделения, эксплуатирующего ИСПДн.

В ходе обследования проверяется:

соответствие категории обследуемой ИСПДн;

соблюдение требований к помещениям, где обрабатываются ПДн;

соответствие выполняемых мероприятий по защите персональных данных, изложенным в техническом паспорте;

выполнение требований по защите ИСПДн от несанкционированного доступа;

выполнение требований по антивирусной защите.

5. Порядок обучения персонала работе в ИСПДн

Обучение практике и методике обработки персональных данных в ИСПДн должно быть непрерывным, систематическим, разделенным по категориям, при этом наибольшее внимание следует уделять практике работы пользователя в ИСПДн.

5.1. Обучение персонала

Обучение происходит в форме совещания, практических занятий, семинаров, инструктажей, проведением консультаций, иных форм повышения квалификации.

Инструктажи, практические занятия по вопросам обеспечения безопасности персональных данных в ИСПДн могут проводиться в ходе проведения проверок состояния обеспечения безопасности ИСПДн на местах.

Первичные инструктажи проводятся ответственным за защиту информации с пользователями ИСПДн:

после проведения аттестационных испытаний ИСПДн и получении «Аттестата соответствия» по требованиям безопасности ИСПДн;

при поступлении на работу сотрудника в структурное подразделение организации, в котором происходит обработка персональных данных в ИСПДн.

Ответственным за организацию обучения и оказание методической помощи пользователям в структурном подразделении организации является его руководитель.

Для проведения занятий, семинаров и совещаний могут привлекаться специалисты органов по аттестации объектов ИСПДн.

К работе в ИСПДн допускаются только сотрудники, прошедшие первичный инструктаж обеспечения безопасности персональных данных в ИСПДн.

6. Порядок проверки электронного журнала обращений к ИСПДн

Настоящий раздел Положения определяет порядок проверки электронного журнала обращений к ИСПДн.

Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к персональным данным в ИСПДн.

Право проверки электронного журнала обращений имеют:

администратор безопасности ИСПДн;

ответственный за защиту информации ПДн.

На АРМ ИСПДн, где установлены программные и программно-аппаратные средства защиты информации от несанкционированного доступа, проверка электронного журнала производится в соответствии с прилагаемым к указанным средствам Руководством.

Если в ходе проверок ИСПДн выявлены случаи НСД к персональным данным, то необходимо выполнить действия, изложенные в разделе 4 Положения «Порядок контроля защиты персональных данных».

7. Порядок защиты от вредоносных программ

Настоящий раздел Положения определяет требования к организации защиты ИСПДн от воздействия вредоносного программного обеспечения, вирусов и устанавливает ответственность руководителей и сотрудников, эксплуатирующих АРМ, за их выполнение.

7.1. Требования, предъявляемые к средствам антивирусной защиты

Средства антивирусной защиты должны обеспечивать:

обнаружение вредоносных воздействий на ИСПДн;

блокирование возможного распространения вирусов и уничтожение обнаруженных вредоносных программ (далее – ВП);

централизованное получение обновлений версий антивирусного ПО и баз данных вирусов от производителя и последующее обновление всех средств антивирусной защиты на рабочих местах, а также управление процессом обновлений;

ведение отчетов о работе средств антивирусной защиты в целом, об обнаружении вирусной деятельности, фиксируемой средствами антивирусной защиты;

управление и определение порядка (политики) антивирусной защиты отдельных АРМ, серверов и других информационных узлов ИСПДн;

возможность удаленного управления и централизованного мониторинга, а также администрирования средств антивирусной защиты с отдельного рабочего места (администратора безопасности);

ведение отчетов в удобной форме;

наличие действенных средств оповещения о происходящих событиях.

Кроме того, средства антивирусной защиты не должны значительно понижать производительность ИСПДн. По возможности необходимо предусмотреть регулирование уровня загрузки системных ресурсов средствами антивирусной защиты.

7.2. Организационные и административные меры

При использовании средств антивирусной защиты должны выполняться следующие организационные и административные меры:

запрет на несанкционированное использование носителей информации (оптических дисков, флэш-карт и т.п.);

запрет на использование чужих носителей при работе в ИСПДн;

запрет на запуск программ с внешних носителей при работе в ИСПДн

использование в ИСПДн только лицензионных дистрибутивов программных продуктов;

обязательная проверка всех программных продуктов;

ограничение доступа к ИСПДн посторонних лиц;

проверка всех файлов, полученных по электронной почте, специальными антивирусными средствами;

систематическая проверка содержимого дисков файловых хранилищ самыми новыми версиями антивирусных программ;

централизованное управление средствами антивирусной защиты.

Ответственность за эксплуатацию средств антивирусной защиты возлагается на сотрудников службы информационной безопасности.

Порядок защиты от ВП приведен в «Инструкция по организации антивирусной защиты в ИСПДн ОГУ (Приложение 6).

8. Порядок и правила парольной защиты, регистрации пользователей и назначения им прав доступа

8.1. Правила парольной защиты

При использовании паролей в ИСПДн должны выполняться следующие основные правила:

длина паролей должна быть не менее 6 символов;

пароль обязательно должен содержать любую комбинацию минимум из двух следующих групп (маленьких букв, больших букв, цифр и специальных символов);

пароли обязаны меняться с установленной периодичностью.

обязательно применение индивидуальных паролей, применение групповых паролей не допускается.

при вводе пароль не должен отображаться на мониторе.

При создании пароля пользователя администратором необходимо предусмотреть возможность его изменения самим пользователем после первого же его входа в систему.

8.2. Порядок использования паролей пользователей

Порядок использования паролей пользователей в ИСПДн приведен в «Инструкции по организации парольной защиты в ИСПДн (Приложение 5).

8.3. Порядок регистрации пользователей и назначения им прав доступа

При регистрации и назначении прав доступа пользователей ИСПДн должны быть выполнены следующие требования:

каждому пользователю должен быть присвоен уникальный идентификатор пользователя;

проведена проверка соответствия уровня доступа возложенным на пользователя задачам

В ИСПДн должно быть предусмотрен доступ к сервисам только аутентифицированным пользователям.

При изменении должностных обязанностей (увольнении) пользователя должно проводиться немедленное блокирование (удаление) прав его доступа к информационным ресурсам.

Администраторами ИСПДн должно проводиться блокирование или удаление всех неиспользуемых учетных записей.

9. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

Настоящие правила регламентируют обеспечению безопасности персональных данных при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

Все изменения конфигураций технических и программных средств АРМ должны производиться только на основании заявок ответственного за эксплуатацию конкретной подсистемы ИСПДн (пользователя конкретного АРМ).

Право внесения изменений в конфигурацию аппаратно-программных средств защищенных АРМ предоставляется:

в отношении системных и прикладных программных средств–администратору безопасности по согласованию с органом по аттестации;

в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты–уполномоченными сотрудниками органа по аттестации ИСПДн.

Изменение конфигурации аппаратно-программных средств АРМ кем-либо, кроме вышеперечисленных уполномоченных сотрудников и подразделений, запрещено.

10. Порядок контроля соблюдения условий использования средств защиты информации

Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации.

Средства защиты информации являются важным компонентом ОБ ПДн. Порядок работы со средствами защиты информации определен в соответствующих Инструкциях, обязательных для исполнения как сотрудникам, обрабатывающим персональные данные, так и администраторам безопасности ИСПДн.

Право проверки соблюдения условий использования средств защиты информации имеют:

администратор безопасности ИСПДн;

ответственный за ОБ ПДн.

Пользователю ИСПДн категорически запрещается:

обработка персональных данных с отключенными средствами защиты информации;

изменение настройки средств защиты информации.

Администратору безопасности запрещается менять настройки программно-аппаратных средств защиты информации, предустановленные сотрудником органа по аттестации в ходе настройки системы защиты информации в ходе аттестации ИСПДн.

Если в ходе периодических, плановых или внеплановых проверок ИСПДн выявлено нарушение требования п. 10, то необходимо выполнить действия, изложенные в разделе 4 Положения «Порядок контроля защиты персональных данных».

11. Порядок охраны и допуска посторонних лиц в помещения ИСПДн

При обработке персональных данных в ИСПДн необходимо исключить неконтролируемое пребывание посторонних лиц в пределах границ контролируемой зоны ИСПДн.

Доступ в помещения, где обрабатываются персональные данные, лицам, не допущенным к обработке персональных данных, должен быть, по–возможности запрещен. В случае невозможности запретить доступ в помещения, необходимо исключить

возможность несанкционированного доступа к техническим средствам обработки персональных данных, хищение носителей информации и документов.

Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях, согласно установленному в Организации порядку.

При обнаружении признаков, указывающих на возможное проникновение в помещение посторонних лиц, принимаются меры по охране места происшествия и вызываются администратор безопасности и ответственный за обеспечение безопасности персональных данных.

Администратор безопасности и ответственный за защиту информации ПДн организуют проверку АРМ, ИСПДн на предмет несанкционированного доступа к персональным данным и наличие документов и машинных носителей информации.

12. Заключительные положения

Требования настоящего Положения обязательны для всех сотрудников, обрабатывающих персональные данные, и ответственных за обеспечение их безопасности.

Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско–правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Нарушения, связанные с выполнением требований руководящих документов по информационной безопасности, применению средств защиты персональных данных 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) персональных данных, 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) персональных данных 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.

Приложение 1
утверждено Приказом Ректора ОГУ имени И.С. Тургенева
от 12.10.2017 года № 627

Инструкция Администратора безопасности информации (БИ) Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева»

1. Общие положения

1.1. Инструкция администратора безопасности информации автоматизированных информационных систем, в том числе информационных систем персональных данных (далее – АИС и ИСПДн соответственно), Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – ОГУ имени И.С. Тургенева), обрабатывающих конфиденциальную информацию, в том числе персональные данные (далее – Администратор БИ), определяет задачи, обязанности, права и ответственность Администратора БИ по вопросам обеспечения информационной безопасности при обработке конфиденциальной (в том числе персональных данных) информации в АИС и ИСПДн ОГУ имени И.С. Тургенева.

1.2. Обязанности Администратора БИ возлагаются на сотрудника ОГУ имени И.С. Тургенева приказом Ректора.

1.3. По вопросам обеспечения безопасности информации (персональных данных) Администратор БИ подчиняется ректору, ответственному по защите информации (по безопасности персональных данных) ОГУ имени И.С. Тургенева.

1.4. Администратор БИ руководствуется положениями настоящей Инструкции, «Специальнми требованиями и рекомендациями по технической защите конфиденциальной информации», утвержденными приказом Гостехкомиссии России от 30 августа 2002 г. № 282, приказами ФСТЭК России 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и других руководящих документов ФСТЭК и ФСБ России по защите информации (персональных данных), а также требованиями эксплуатационных документов на систему защиты информации от несанкционированного доступа.

2. Основная задача и обязанности Администратора БИ

2.1. Основными задачами Администратора БИ являются:

2.1.1. Организация эксплуатации технических и программных средств защиты информации АИС и ИСПДн в соответствии с установленными требованиями по защите информации.

2.1.2. Текущий контроль работы средств и систем защиты информации АИС и ИСПДн .

2.1.3. Контроль за работой пользователей АИС и ИСПДн, выявление и регистрация попыток несанкционированного доступа к защищаемым информационным ресурсам.

2.2. В соответствии с возложенными задачами Администратор БИ осуществляет следующие функции:

2.2.1. Выполняет работу по внедрению и эксплуатации в АИС и ИСПДн общесистемных программных средств, сертифицированных по требованиям безопасности информации:

- выполняет контроль за установкой на серверном оборудовании и рабочих станциях АИС и ИСПДн общесистемных программных средств;

- выполняет настройку общесистемных программных средств в соответствии с сертифицированными шаблонами безопасности;

- выполняет установку и настройку специального программного обеспечения для контроля и настройки общесистемных программных средств, сертифицированных по требованиям безопасности информации.

2.2.2. Организовывает работу по внедрению и эксплуатации СЗИ в соответствии с установленными требованиями по защите информации:

- выполняет работу по установке и настройке технических и программных средств защиты информации АИС и ИСПДн от несанкционированного доступа к ней;

- обеспечивает эксплуатацию технических и программных средств защиты информации АИС и ИСПДн, контролирует работоспособность и эффективность функционирования этих средств;

- осуществляет систематический контроль работы средств защиты информации АИС и ИСПДн;

- распределяет между пользователями АИС и ИСПДн необходимые реквизиты криптографической защиты (пароли, ключи защиты и т.п.), формирует и распределяет между пользователями необходимые реквизиты защиты от НСД;

- выполняет ввод описаний пользователей АИС и ИСПДн в информационную базу СЗИ от НСД;

- выполняет своевременное удаление описаний пользователей АИС и ИСПДн из базы данных СЗИ от НСД при изменении списка сотрудников ОГУ имени И.С. Тургенева, допущенных к обработке конфиденциальной информации (далее - КИ) и персональных данных (далее - ПДн).

- проводит обучение пользователей АИС и ИСПДн правилам работы со средствами защиты информации;

- организовывает работу по эксплуатации СЗИ в АИС и ИСПДн.

- проводит контроль целостности СЗИ с целью выявления несанкционированных изменений в ней;

- выполняет восстановление программной среды, программных средств и настроек СЗИ от НСД при сбоях.

2.2.3. Организовывает работу по защите информации, циркулирующей в АИС и ИСПДн:

- осуществляет контроль разграничения прав доступа к защищаемой информации на несъемных носителях информации рабочих мест пользователей АИС и ИСПДн;

- принимает участие в разработке документов по обеспечению безопасности информации при эксплуатации АИС и ИСПДн;

- осуществляет контроль за проведением смены паролей пользователей АИС и ИСПДн;

- осуществляет настройку и сопровождение подсистемы регистрации и учета действий пользователей АИС и ИСПДн;

- принимает меры по предупреждению угроз безопасности информации, возникающих в результате случайных ошибок пользователей АИС и ИСПДн при обработке электронных документов;

- проводит периодический контроль средств вычислительной техники, подключенных к АИС и ИСПДн, на предмет исключения несанкционированного изменения в составе, конструкции, конфигурации, размещении средств вычислительной техники, а также в составе программного обеспечения;

- регулярно анализирует содержимое системных журналов, проводит работы по выявлению возможных каналов утечки КИ и персональных данных за счет несанкционированных доступов к информации и техническим средствам АИС и ИСПДн, ведет их учет;

- обобщает и анализирует сведения о противоправных устремлениях к информации, попытках преодоления СЗИ, используемых при этом методах и средствах;

- анализирует состояние защищенности информационных ресурсов АИС и ИСПДн, готовит предложения по совершенствованию СЗИ;

- принимает участие в оценке реальной опасности утечки информации, подлежащей защите при использовании технических средств, в разработке эффективных и экономически обоснованных мер по ее защите;

- осуществляет контроль за выводом документов пользователей АИС и ИСПДн на принтерах и за соблюдением установленных правил и параметров регистрации и учета бумажных носителей информации;

- осуществляет контроль соблюдения требований по безопасности информации при использовании машинных носителей информации;

- разрабатывает и вводит установленным порядком необходимую учетную и объектовую документацию (журнал учета идентификаторов, инструкции пользователям и т.д.);

- выполняет установку и настройку антивирусной системы защиты информации в АИС и ИСПДн, контроль за периодическим обновлением антивирусных баз (средств), осуществляет контроль за соблюдением пользователями АИС и ИСПДн порядка и правил проведения антивирусного тестирования;

- осуществляет контроль доступа лиц в помещение, где установлены рабочие станции и серверное оборудование АИС и ИСПДн, в соответствии с утвержденными списками сотрудников ОГУ имени И.С. Тургенева, допущенных к обработке КИ и ПДн;

- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток неправомерного доступа к охраняемым сведениям или попыток хищения, копирования, изменения сообщает ответственному за защиту информации (обработку ПДн) и ректору ОГУ имени И.С. Тургенева.

3. Обязанности Администратора БИ

Администратор БИ обязан:

3.1. Знать состав АИС и ИСПДн (серверное оборудование, рабочие станции, используемое программное обеспечение).

3.2. Знать состав пользователей АИС и ИСПДн и их производственную деятельность (выполняемые операции, права, привилегии).

3.3. Знать порядок и технологию включения и удаления пользователей в СЗИ от НСД.

3.4. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в соответствии с требованиями руководящих и нормативно-методических документов по защите информации.

3.5. Докладывать о выявленных нарушениях и НСД пользователей АИС и ИСПДн к защищаемой информации, принимать необходимые меры по устранению выявленных нарушений.

3.6. Проводить инструктаж пользователей АИС и ИСПДн по правилам работы с используемыми средствами и системами защиты информации.

3.7. Осуществлять контроль соответствия уровня конфиденциальности выводимой информации на внешние носители информации и грифа конфиденциальности этих носителей, а также правильности их учета.

3.8. Осуществлять контроль соответствия уровня конфиденциальности информации, выводимой на печать, и грифа конфиденциальности бумажных машинных носителей информации – листов бумаги, а также правильности их учета.

3.9. Осуществляет контроль за уничтожением конфиденциальной информации и ее носителей, гарантированного уничтожения информации средствами СЗИ от НСД.

4. Права Администратора БИ

Администратор БИ имеет право:

4.1. Иметь доступ к средствам обработки и передачи информации АИС и ИСПДн, постоянно осуществлять проверки состояния СЗИ, контролировать состояние защищенности АИС.

4.2. Требовать от пользователей АИС и ИСПДн соблюдения установленных правил обработки КИ и ПДн и выполнения требований руководящих и нормативно-методических документов по защите информации.

4.3. Обращаться к ответственному за защиту информации (за безопасность ПДн) ОГУ имени И.С. Тургенева, а в случае их отсутствия к ректору и с требованием о прекращении доступа пользователя к работам в АИС и ИСПДн в случае грубых нарушений требований руководящих и нормативно-методических документов по защите информации, порядка и правил обработки конфиденциальной информации или нарушения функционирования средств и систем защиты информации.

4.4. Требовать назначения служебного расследования в отношении пользователя АИС и ИСПДн по фактам нарушения безопасности информации и НСД к защищаемой информации.

5. Ответственность Администратора БИ

5.1. Администратор БИ ОГУ имени И.С. Тургенева несет ответственность в полном объеме по действующему законодательству Российской Федерации за разглашение сведений, составляющих КИ, ПДн и другой информации ограниченного доступа ставших известными ему в соответствии с родом работы.

Приложение 2
утверждено Приказом Ректора ОГУ имени И.С. Тургенева
от 12.10.2017 года № 627

Инструкция
по работе пользователей в ИСПДн

Допуск пользователей для работы в автоматизированных информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – АИС), в том числе в информационных системах персональных данных – ИСПДн, осуществляется в соответствии с приказом Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – ОГУ имени И.С. Тургенева) и разрешительной системой доступа, установленной в ОГУ имени И.С. Тургенева.

Пользователь АИС имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам компьютера. При этом для хранения файлов, содержащих конфиденциальную информацию, разрешается использовать только специально выделенные каталоги на несъемных носителях информации, а также соответствующим образом учтенные съёмные носители информации.

Присвоение пользователю АИС полномочий доступа к ресурсам компьютера, состав необходимого системного и прикладного программного обеспечения для решения поставленных задач и определение возможного времени работы пользователя в АИС осуществляется при первичной регистрации пользователя Администратором безопасности информации.

Пользователь АИС отвечает за правильность включения и выключения технических средств и систем, входа в систему и все действия при работе в АИС.

Вход пользователя АИС в систему осуществляется на основе ввода имени, присвоенного при первичной регистрации и ввода личного пароля. Требования к парольной защите определяется Инструкцией по парольной защите.

В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется периодическая (раз в полгода) замена пароля постоянного пользователя. Замена личного пароля осуществляется пользователем АИС самостоятельно.

При работе со съемными носителями информации пользователь АИС каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием установленных антивирусных программ, в соответствии с Инструкцией по антивирусной защите.

Пользователь АИС обязан:

знать и строго выполнять установленные правила и обязанности по доступу к защищаемым ресурсам и соблюдению принятого режима информационной безопасности;

обеспечить правильность вводимых данных;

своевременно сообщать Администратору безопасности информации об изменениях статуса пользователя;

незамедлительно сообщить руководителю своего структурного подразделения и Администратору безопасности информации факты выявления инцидентов с доступом к конфиденциальной информации.

В процессе работы пользователю АИС запрещается:

использовать для постоянного хранения и обработки конфиденциальной информации каталоги несъемных носителей информации, за исключением выделенных каталогов;

осуществлять попытки несанкционированного доступа к ресурсам операционной системы;

в рамках выделенных ресурсов и полномочий доступа к ним обрабатывать информацию с уровнем конфиденциальности, выше заявленного при регистрации;

пытаться подменять функции администратора по перераспределению времени работы и полномочий доступа к ресурсам компьютера;

покидать помещение с незаблокированной учетной записью;

отключать установленные средства защиты информации;

использовать машинные носители без их предварительной проверки антивирусными средствами;

устанавливать программное обеспечение;

менять параметры конфигурации ранее установленных программных средств;

использование различными пользователями одной и той же учетной записи, даже если пользователи имеют одинаковые полномочия по доступу;

запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа другим лицам;

хранение пароля на любых носителях, позволяющих другим лицам получить информацию о пароле;

использовать информацию, полученную в результате доступа к БД, в целях, не предусмотренных его функциональными обязанностями.

Ответственность за сохранность и правильное использование информации, ставшей известной в процессе обработки конфиденциальной информации несет пользователь АИС.

Возможность получения технического доступа к конфиденциальной информации не дает права пользователям АИС обработки такой информации, если им не предоставлены права доступа к этой информации. Такие действия рассматриваются как попытки несанкционированного доступа.

При выявлении инцидентов с доступом к конфиденциальной информации доступ пользователей АИС к ней может быть ограничен до окончания расследования инцидента, о чем пользователь уведомляется в кратчайшие сроки. По результатам служебного расследования нарушитель может быть лишен прав доступа к конфиденциальной информации, материалы расследования могут быть направлены в соответствующие службы для привлечения нарушителя к ответственности.

Пользователь АИС несет ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования этой учетной записи.

При нарушениях пользователем АИС правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.

Приложение 3
утверждено Приказом Ректора ОГУ имени И.С. Тургенева
от 12.10.2017 года № 627

Инструкция
администратора системного ИСПДн

1. Общие положения

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность Администратора системного автоматизированной информационной системы (далее - АИС), в том числе информационной системы персональных данных (далее – ИСПДн), федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – ОГУ имени И.С. Тургенева).

1.2. Администратор системный АИС, ИСПДн (далее – Администратор) в пределах своих функциональных обязанностей, обеспечивает работоспособность технических средств АИС (ИСПДн) и установленного программного обеспечения.

1.3. Администратор назначается в установленном порядке приказом ОГУ имени И.С. Тургенева.

1.4. Администратор в своей работе должен руководствоваться настоящей Инструкцией и следующими основными законодательными и нормативными правовыми актами Российской Федерации:

- Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказы 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» и от 11.02.2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- локальные акты ОГУ имени И.С. Тургенева;
- иные нормативные акты Российской Федерации, Орловской области в области безопасности информации (персональных данных)

1.5. Основные понятия и термины, используемые в настоящей Инструкции, применяются в значениях, определенных статьей 3 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Обязанности:

а) знать и выполнять требования действующих нормативных правовых актов Российской Федерации, а также локальных актов ОГУ имени И.С. Тургенева, регламентирующих деятельность по защите конфиденциальной информации (персональных данных);

б) устанавливать, настраивать и сопровождать необходимое для работы АИС (ИСПДн) программное обеспечение;

в) обеспечивать функционирование и поддержание в рабочем состоянии программных средств и средств вычислительной техники в пределах возложенных на него обязанностей;

г) выполнять резервирование и восстановление программных средств;

д) контролировать физическую сохранность оборудования АИС (ИСПДн);

е) не допускать установку, использование, хранение и распространение в АИС (ИСПДн) программных средств, не связанных с выполнением функциональных задач;

ж) взаимодействовать с ответственным за защиту информации (организацию обработки персональных данных) и Администратором безопасности информации АИС (ИСПДн) при проведении работ, связанных с анализом и оценкой защищенности информации в АИС (ИСПДн);

з) докладывать ответственному за защиту информации (организацию обработки персональных данных), Администратору безопасности информации АИС (ИСПДн) об обнаруженных недекларированных возможностях программных средств, нарушениях и несанкционированных действиях пользователей;

и) взаимодействовать с ответственным за защиту информации (организацию обработки персональных данных), Администратором безопасности информации АИС (ИСПДн) по вопросам обеспечения правильной эксплуатации средств вычислительной техники АИС (ИСПДн);

к) проводить инструктаж и консультации пользователей АИС (ИСПДн) по правилам работы и эксплуатации используемых средств вычислительной техники.

3. Права

а) требовать от пользователей АИС (ИСПДн) точного соблюдения установленной технологии обработки информации и выполнения инструкций по работе с техническими и программными средствами АИС (ИСПДн);

б) обращаться к ответственному за защиту информации (организацию обработки персональных данных) и Администратору безопасности информации АИС (ИСПДн) с предложением о приостановке обработки конфиденциальной информации (персональных данных) в случаях грубых нарушений установленной технологии их обработки и/или функционирования программных и/или технических средств;

в) докладывать непосредственному руководителю о нарушениях или невыполнении пользователями инструкций по работе с техническими и программными средствами АИС (ИСПДн).

4. Ответственность

Системный администратор АИС (ИСПДн) несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Приложение 4
утверждено Приказом Ректора ОГУ имени И.С. Тургенева
от 12.10.2017 года № 627

Инструкция ответственного за защиту информации в Федеральном государственном бюджетном образовательном учреждении высшего образования «Орловский государственный университет имени И.С. Тургенева»

1. Общие положения

Инструкция лица, ответственного защиту информации в федеральном государственном бюджетном образовательном учреждении высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее - Инструкция), разработана в соответствии с требованиями существующих законодательно - нормативных документов Российской Федерации, Орловской области и документов федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее - ОГУ имени И.С. Тургенева) в области безопасности информации.

Настоящая Инструкция закрепляет обязанности, права и ответственность лица, ответственного за защиту информации (организацию обработки персональных данных) в ОГУ имени И.С. Тургенева.

Лицо, ответственное за организацию обработки персональных данных, в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами Российский Федерации, Орловской области, настоящей Инструкцией, а также иными локальными нормативными актами ОГУ имени И.С. Тургенева, регламентирующими вопросы обработки конфиденциальной информации (персональных данных).

2 Обязанности лица, ответственного за защиту информации (организацию обработки персональных данных)

2.1 Лицо, ответственное за защиту информации (организацию обработки персональных данных) в ОГУ имени И.С. Тургенева обязано:

- осуществлять внутренний контроль за соблюдением всеми сотрудниками ОГУ имени И.С. Тургенева законодательства Российской Федерации о защите информации (персональных данных), в том числе требований к защите информации (персональных данных);
- доводить до сведения сотрудников ОГУ имени И.С. Тургенева положения законодательства Российской Федерации о защите информации (персональных данных), локальных актов по вопросам обработки конфиденциальной информации (персональных данных), требований к защите информации (персональных данных);
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой указанных обращений и запросов.

3. Права лица, ответственного за организацию обработки персональных данных

3.1. Лицо, ответственное за защиту информации (персональных данных), имеет право:

- принимать решения в пределах совей компетенции; требовать от сотрудников ОГУ имени И.С. Тургенева соблюдения действующего законодательства Российской Федерации по защите информации, а также локальных нормативных актов ОГУ имени И.С. Тургенева по защите информации (персональных данных);
- контролировать в ОГУ имени И.С. Тургенева осуществление мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», другими нормативными правовыми

актами Российский Федерации, Орловской области по защите информации (персональных данных) и принятыми в соответствии с ними нормативными правовыми актами;

- взаимодействовать с руководством и иными структурными подразделениями ОГУ имени И.С. Тургенева по вопросам обработки конфиденциальной информации (персональных данных).

4. Ответственность лица, ответственного за защиту информации (организацию обработки персональных данных)

4.1. За ненадлежащее исполнение или неисполнение настоящей Инструкции, а также за нарушение требований законодательства о защите информации (персональных данных) лицо, ответственное за защиту информации (организацию обработки персональных данных) в ОГУ имени И.С. Тургенева, несет предусмотренную законодательством Российской Федерации ответственность.

Приложение 5
утверждено Приказом Ректора ОГУ имени И.С. Тургенева
от 12.10.2017 года № 627

Инструкция по парольной защите в автоматизированных информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева»

Данная инструкция призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированных информационных системах (далее – АИС) Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее - ОГУ имени И.С. Тургенева), в том числе в информационных системах персональных данных – ИСПДн, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех АИС и ИСПДн ОГУ имени И.С. Тургенева и контроль за действиями исполнителей и обслуживающего персонала АИС и ИСПДн ОГУ имени И.С. Тургенева при работе с паролями возлагается на Администратора безопасности информации.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

длина пароля должна быть не менее 8 символов;

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

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

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 8 позициях;

личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Для генерации «стойких» значений паролей могут применяться специальные программные средства.

При наличии технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение Администратору безопасности информации.

Опечатанные конверты с паролями исполнителей должны храниться в сейфе.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полгода.

Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий должна производиться Администратором безопасности информации немедленно.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий Администраторов и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой.

В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры по внеплановой смене паролей.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Приложение 6
утверждено Приказом Ректора ОГУ имени И.С. Тургенева
от 12.10.2017 года № 627

Инструкция по антивирусной защите в автоматизированных информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева»

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на Администратора безопасности информации Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – ОГУ имени И.С. Тургенева).

К применению в автоматизированных информационных системах ОГУ имени И.С. Тургенева (далее – АИС), в том числе в информационных системах персональных данных – ИСПДн, допускаются сертифицированные ФСБ и/или ФСТЭК России антивирусные средства.

На АРМ АИС используются только лицензионные антивирусные средства.

Настройка параметров средств антивирусного контроля осуществляется администратором безопасности в соответствии с руководствами по применению конкретных антивирусных средств.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая на съемных носителях (магнитных дисках, CD-ROM, флэш памяти и т.п.).

Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля.

Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

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

При работе с внешними носителями информации пользователи обязаны перед их применением осуществить проверку их на предмет отсутствия компьютерных вирусов.

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.) пользователи АИС должны провести внеочередной антивирусный контроль своего АРМ.

В случае обнаружения при проведении внеочередной антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и Администратора безопасности информации, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

провести лечение или уничтожение зараженных файлов;

в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, проинформировать Администратора безопасности информации для организации дальнейших действий по его изоляции.

Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящей Инструкции возлагается на Руководителя структурной службы ОГУ имени И.С. Тургенева, в котором функционирует АИС.

Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на Администратора безопасности информации и всех сотрудников подразделения, являющихся пользователями АИС.

Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделения, эксплуатирующего АИС, осуществляетс Администратора безопасности информации.

В АИС запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.