

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЯЗАНСКОЙ ОБЛАСТИ
Областное государственное бюджетное учреждение
дополнительного профессионального образования
«Рязанский институт развития образования»
ОГБУ ДПО «РИРО»

П Р И К А З

от 02.05.2017 г.

№ 46

Рязань

Об утверждении положения «О защите персональных данных в информационных системах персональных данных в институте», о назначении администраторов безопасности информационных систем персональных данных и утверждении инструкции администратора информационных систем персональных данных

В соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных», Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 г. №1119 **п р и к а з ы в а ю:**

1. Утвердить положение «О защите персональных данных в информационных системах персональных данных в институте» согласно приложения № 1.

2. Назначить администраторами безопасности информационных систем персональных данных (ИСПДн) института заведующего информационно-техническим центром Дубовицкого Игоря Валентиновича и методиста отдела мониторинговых исследований центра оценки качества образования Кольчугина Олега Дмитриевича.

3. Утвердить инструкцию администратора информационных систем персональных данных (ИСПДн) института на 2 листах согласно приложения № 2.

Контроль за исполнением настоящего приказа оставляю за собой.

Ректор

 А.А. Кашаев

С приказом ознакомлены:

Дубовицкий И.В.

Кольчугин О.Д.



**Областное государственное бюджетное учреждение
дополнительного профессионального образования
«Рязанский институт развития образования»**

(ОГБУ ДПО «РИРО»)

РАССМОТРЕНО
на заседании ученого совета
ОГБУ ДПО «РИРО»
Протокол
от «18» 04 2017 г. № 2



ПОЛОЖЕНИЕ

**О защите персональных данных
в информационных системах персональных данных
Областного государственного бюджетного учреждения
дополнительного профессионального образования
«Рязанский институт развития образования»**

2017 г.

г. Рязань

1. Общие положения

Настоящее «Положение о защите персональных данных в информационных системах персональных данных в Областном государственном бюджетном учреждении дополнительного профессионального образования «Рязанский институт развития образования» (ОГБУ ДПО «РИРО») (далее – Положение, далее – институт) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012г., методическими рекомендациями ФСТЭК России и ФСБ России. Положение разработано в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений при их обработке, порядок обучения персонала практике работы в ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

2. Порядок предоставления допуска пользователей к работе в ИСПДн

Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

Первоначальный допуск пользователей к работе в ИСПДн осуществляется на основании приказа, который издается ректором института. В приказе определяется список сотрудников, допущенных к работе в ИСПДн.

С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации и выполнения необходимых мероприятий по обеспечению безопасности в ИСПДн ректором назначается администратор безопасности.

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

Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя **запрещено**.

В дальнейшем, процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой (Приложение 1).

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 отдела), 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).

Заявку рассматривает и визирует ректор, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем заявка передается администратору безопасности для внесения необходимых изменений в списки пользователей ИСПДн.

На основании заявки администратор безопасности производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля, а также регистрацию персонального идентификатора и другие необходимые действия, указанные в заявке.

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

Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и пароль, может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации).

Исполненная заявка хранится у администратора безопасности.

Она может впоследствии использоваться:

- для восстановления полномочий пользователей после возникновения внештатных ситуаций;

- 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.

3. Порядок работы пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн

Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

Перед началом работы в ИСПДн, сотрудники института, допущенные к работе с ПДн, принимают под роспись обязательство о неразглашении персональных данных (Приложение 2).

Вход пользователя в систему должен осуществляться по выдаваемому ему электронному идентификатору и по персональному паролю.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, имеющих необходимые сертификаты, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

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 правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;
- хранить в тайне свой пароль (пароли). В соответствии с п. 7.5. данного Положения и с установленной периодичностью менять свой пароль (пароли);
- хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в недоступном для посторонних месте;
- выполнять требования Положения по организации антивирусной защиты в полном объеме;
- немедленно известить администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- фактов совершения попыток несанкционированного доступа (далее - НСД) к ИСПДн;
- несанкционированных 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.

Пользователю 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 ПДн на неучтенных машинных носителях информации;
- 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 ПДн;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению конфиденциальности ПДн;
- размещать средства отображения информации (монитор, принтер и т.п.) таким образом, чтобы с них существовала возможность визуального считывания информации посторонними лицами.

Администратор безопасности **обязан**:

- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;
- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;
- производить необходимые настройки подсистемы управления доступом установленных в ИСПДн 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.);
- проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;
- контролировать своевременное (не реже чем один раз в течение 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;
- обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;
- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных пользователями ИСПДн;
- восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;
- периодически обновлять антивирусные средства (базы данных), 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;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание персональных данных на носителях информации);
- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;
- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

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

Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные в Журнале учета носители.

Администратор безопасности **обязан** осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных пользователями ИСПДн.

Носители информации, предназначенные для создания резервной копии и хранения персональных данных, выдаются установленным порядком администратором безопасности. По окончании процедуры резервного копирования электронные носители сдаются на хранение руководителю структурного подразделения.

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

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

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.

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.

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

5. Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных

Перед началом работы в ИСПДн пользователи должны ознакомиться с требованиями настоящего Положения под роспись.

Пользователи должны продемонстрировать администратору безопасности наличие необходимых знаний и умений для выполнения требований настоящего Положения.

Ответственным за организацию обучения и оказание методической помощи в институте является администратор безопасности.

6. Правила антивирусной защиты

Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения, компьютерных вирусов и устанавливает ответственность

руководителя и сотрудников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение.

К использованию на компьютерах допускаются только лицензионные антивирусные средства;

Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности;

Администратор безопасности осуществляет периодическое обновление антивирусных средств и контроль их работоспособности;

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

Еженедельно 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, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель);

Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль;

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

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

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) должен провести внеочередной антивирусный контроль компьютера.

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.

Ответственность за организацию антивирусного контроля в ИСПДн в

соответствии с требованиями настоящего Положения возлагается на администратора безопасности;

Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

7. Правила парольной защиты

Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

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.

При доступе пользователя в систему должна осуществляться идентификация и проверка подлинности по идентификатору и паролю, а также с использованием электронных идентификаторов.

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

- пароль должен быть длиной не менее шести буквенно-цифровых символов;
- 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 АРМ 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.

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

Удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри учреждения и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой, на основании указания ректора или начальника отдела кадров.

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

В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по изменению его пароля.

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

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

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

Право на установку, обновление и модификацию общесистемного и прикладного программного обеспечения компьютеров ИСПДн предоставляется администратору безопасности.

Заявку на внесение изменений в конфигурацию аппаратно-программных средств защищенных рабочих мест ИСПДн, рассматривает ректор, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

После чего заявка передается администратору безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке.

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

Установка и обновление ПО (системного, прикладного, тестового и т.п.) на компьютерах производится только с использованием оригинальных лицензионных дистрибутивов.

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

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

При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, администратор безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

9. Порядок контроля обеспечения защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления

Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются 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.

Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в институте, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;
- уточнение возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- 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;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;

10. Порядок охраны и допуска посторонних лиц в помещения ИСПДн

В институте предусмотрена физическая охрана технических средств ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации.

В помещениях должна быть установлена охранная и пожарная сигнализация.

Серверное и коммутационное оборудование ИСПДн должно находиться под надежным замком, в отдельном помещении или запирающемся шкафу, ключ должен храниться у администратора безопасности.

Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

Список сотрудников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения утверждается ректором и передается на пост охраны.

При закрытии помещений и сдачей их под охрану сотрудники, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации на которых содержатся персональные данные, убираются для хранения в запираемый ящик стола или сейф.

При обнаружении повреждения замков, дверей или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и (или) ответственному за защиту информации.

При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или ответственному за защиту информации, или ректору, или администратору безопасности.

11. Заключительные положения

Требования настоящего Положения обязательны для всех сотрудников, обрабатывающих персональные данные.

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

к Положению о защите персональных данных в ИСПДн
Областного государственного бюджетного учреждения
дополнительного профессионального образования
«Рязанский институт развития образования»

ЗАЯВКА

на внесение изменений в списки пользователей и наделение их
полномочиями доступа к ресурсам информационной системы персональных
данных

Прошу зарегистрировать пользователем (исключить из списка пользователей,
изменить полномочия пользователя) информационной системы персональных
данных

_____ ,

(должность с указанием подразделения)

(фамилия имя и отчество сотрудника)

предоставив ему полномочия, необходимые (лишив его полномочий,
необходимых) для решения задач:

(список задач, приложений)

на следующих рабочих местах (№ ПЭВМ)

_____ (фамилия, инициалы)

_____ (подпись)

« ____ » _____ Г.

к Положению о защите персональных данных в ИСПДн
Областного государственного бюджетного учреждения
дополнительного профессионального образования
«Рязанский институт развития образования»

ОБЯЗАТЕЛЬСТВО

о неразглашении информации, содержащей персональные данные

Я, _____

_____ ,

(Ф.И.О. сотрудника)

исполняющий (ая) должностные обязанности по замещаемой должности

_____ , (должность, наименование структурного подразделения)

предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к персональным данным, обрабатываемым в информационной системе « _____ ».

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.


5. В течение года после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____ (фамилия, инициалы)

_____ (подпись)

« ____ » _____ Г.

УТВЕРЖДАЮ
Ректор ОГБУ ДПО «РИРО»
 А.А. Кашаев
« 02 » _____ 05 _____ 2017 г.

**Инструкция
администратора безопасности информационных систем
персональных данных (ИСПДн)
в Областном государственном бюджетном учреждении дополнительного
профессионального образования «Рязанский институт развития
образования»**

1. Общие положения.

Настоящая инструкция определяет функции, права и обязанности администратора безопасности информационных систем персональных данных (ИСПДн) (далее - Администратор) по вопросам обеспечения информационной безопасности при работе с персональными данными в Областном государственном бюджетном учреждении дополнительного профессионального образования «Рязанский институт развития образования» (далее – Институт)

Администраторы назначаются из числа сотрудников Института и обеспечивают правильность использования и нормальное функционирование установленных систем защиты информации от НСД, резервное копирование персональных данных, обновление антивирусных баз, делает периодический анализ защищённости.

Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных и не исключает обязательного выполнения их требований.

2. Администратор имеет право:

2.1. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

2.2. Требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

3. Администратор обязан:

3.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

3.2. Осуществлять установку, настройку и сопровождение технических средств защиты.

3.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

3.4. Участвовать в приемке новых программных средств. 2.5. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

3.5. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.

3.6. Вести контроль над процессом осуществления резервного копирования объектов защиты.

3.7. Осуществлять контроль над выполнением Плана мероприятий по защите персональных данных.

3.8. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

3.9. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

3.10. Контролировать физическую сохранность средств и оборудования ИСПДн.

3.11. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты.

3.12. Контролировать исполнение пользователями парольной политики.

3.13. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

3.14. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.

3.15. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

3.16. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.17. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

Инструкция разработана по исполнению приказа по деятельности института № 46 от __.05.2017 г.

С инструкцией ознакомлен: _____

« » _____ 2017 года.