МИНИСТЕРСТВО ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ РЯЗАНСКОЙ ОБЛАСТИ

Областное государственное бюджетное учреждение дополнительного профессионального образования
«РЯЗАНСКИЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ»

ОГБУ ДПО «РИРО»

П Р И К А З

от « 20 » января 2023 г. № 9/1

г. Рязань

Об утверждении инструкции
по идентификации и аутентификации и инструкции по организации антивирусной защиты в институте

В соответствии с Постановлением Правительства Российской Федерации от 21.03.2012 г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», в целях обеспечения соблюдения информационной безопасности работниками ОГБУ ДПО «РИРО», допущенных к работе с персональными данными:

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию по идентификации и аутентификации, согласно Приложению №1.
2. Утвердить Инструкцию по организации антивирусной защиты, согласно Приложению № 2.
3. Администратору ИСПДн обеспечить исполнение вышеназванных инструкций.
4. Контроль за исполнением настоящего приказа возложить на Миловзорова А.В., проректора по научно-исследовательской работе и инновационной деятельности.

Ректор А.А. Кашаев

С приказом ознакомлен(а,ы): подпись дата

Миловзоров А.В. 20.01.2023

Дубовицкий И.В 20.01.2023

Приложение № 1
к приказу ОГБУ ДПО «РИРО»
№ 9/1от 20 января 2023 года

ИНСТРУКЦИЯ

по идентификации и аутентификации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет: порядок идентификации и аутентификации пользователей, обрабатывающих персональные данные в информационных системах персональных данных (ИСПДн) в ОГБУ ДПО «РИРО» (далее - институт), порядок управления аппаратными средствами аутентификации, порядок идентификации/аутентификации устройств, а также обязанности пользователя и администратора безопасности.

2. ПОРЯДОК ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

2.1. Всем пользователям ИСПДн, являющимся работниками института, допущенным к работе с ИСПДн, в которой обрабатываются персональные данные, присваиваются учетные записи в виде персональных идентификаторов (логины, имена пользователей).

2.2. Персональный идентификатор пользователя создается администратором безопасности и сообщается пользователю. Персональному идентификатору пользователя соответствуют определенные полномочия в ИСПДн и пароли, обеспечивающие аутентификацию (проверку подлинности) в ИСПДн Права пользователя по доступу к информационным ресурсам ИСПДн, определяется должностью пользователя и матрицей доступа.

2.3. Персональные идентификаторы должны быть заблокированы при превышении времени неиспользования более 90 дней подряд с момента присвоения. Персональные идентификаторы должны быть удалены при увольнении работника института немедленно по окончании последнего сеанса работы работника, а уволенный работник должен быть исключен из числа пользователей.

2.4. При приеме изменении полномочий (временно или бессрочно) действующего работника института, изменения в его доступе к информационным ресурсам ИСПДн, производит администратор безопасности.

2.5. Первичные пароли генерируются администратором безопасности в момент создания идентификаторов и выдаются пользователю под роспись в

журнале учета выдачи первичных паролей (Приложение № 1 к настоящей инструкции).

2.6. При первом доступе к ИСПДн пользователь обязан изменить выданный первичный пароль, руководствуясь требованиями к сложности пароля, указанными в настоящей инструкции (п. 2.8).

2.7 Требования к сложности пароля:

2.7.1 длина пароля должна быть не менее шести символов;

2.7.2. в числе символов пароля обязательно должны присутствовать строчные и прописные буквы, цифры и специальные символы;

2.7.3. пароль не должен включать в себя легко вычисляемые значения символов (имена, фамилии, имена детей или домашних животных, наименования информационных систем, типичных для организации профессиональных терминов, номера телефонов, номера или марки автомобилей, адреса и т. д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

2.7.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в трех символах;

2.7.5. Пароль действует не более 90 дней, по истечении которых пользователь обязан заменить его новым.

2.8. Администратор безопасности осуществляет настройку в ИСПДн параметров количества вводов неправильного пароля. Количество вводов неправильного пароля устанавливается равным 3. Разблокирование пароля осуществляет администратор безопасности при обращении к нему пользователя с заблокированным паролем.

3. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

3.1. Пользователь является частью системы защиты информациии обязан соблюдать следующие правила информационной безопасности:

3.1.1. Помнить свой идентификатор и пароль.

3.1.2. Держать свои пароли в тайне, а именно не сообщать, не разглашать и любым другим способом не доводить до чьего-либо сведения (в том числе других сотрудников Организации, в т.ч. руководителей) личные пароли.

3.1.3. Осуществлять ввод паролей только в условиях, исключающих их просмотр.

3.1.4. Не хранить записки-памятки с личными паролями на видном и/или легкодоступном месте: на столе, на мониторе, под клавиатурой, в верхнем ящике стола и т.п.

3.1.5. Своевременно сообщать администратору безопасности о фактах компрометации паролей, об утере или повреждении аппаратного идентификатора.

4. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

4.1. Администратор безопасности осуществляет организационное и техническое обеспечение процессов создания, использования, изменения и прекращения действия персональных идентификаторов и паролей доступа в ИСДн, контроль действий пользователей ИСПДн при их работе с персональными идентификаторами и паролями доступа.

4.2. Администратор безопасности обязан:

4.2.1. Создавать, вести учет, закрепление и выдачу пользователям персональных идентификаторов и паролей доступа к техническим средствам и информационным ресурсам ИСПДн.

4.2.2. Обеспечивать смену паролей пользователей с периодичностью не реже одного раза в 90 дней с момента очередной смены.

4.2.3. Свой собственный пароль администратор безопасности должен изменять не реже одного раза в месяц.

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1.Пользователи ИСПДн должны быть предупреждены об ответственности за действия с персональными идентификаторами и паролями доступа, нарушающие требования настоящей инструкции.

5.2. Пользователи ИСПДн должны быть ознакомлены с настоящей инструкцией до начала работы в ИСПДн под роспись. Обязанность ознакомления пользователей с настоящей инструкцией лежит на администраторе безопасности.

5.3. Работники института, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

6. НОРМАТИВНЫЕ И ПРАВОВЫЕ ДОКУМЕНТЫ

6.1. Федеральный закон от 27 июля 2006г. № 152-ФЗ «О персональных данных».

6.2. Приказ Федеральной службы по техническому и экспортному контролю Российской Федерации 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».

6.3. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Приложение № 1
к Инструкции по идентификации и аутентификации

ЖУРНАЛ

учета выдачи первичных паролей

№ пп.	ФИО работника	Должность	Структурное подразделение	ИСПДн	Первичный пароль	Дата выдачи	Подпись
1	2	3	4	5	6	7	8
1.							
2.							

Приложение № 2
к приказу ОГБУ ДПО «РИРО»
№ 9/1 от «20» января 2023 года

ИНСТРУКЦИЯ

по организации антивирусной защиты

1. Настоящая Инструкция определяет требования к организации защиты от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и работников института за их выполнение.

2. К использованию в организации допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

3. Установка средств антивирусного контроля на компьютерах осуществляется уполномоченным сотрудником организации. Настройка параметров средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.

4. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.

5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (флэш-накопитель, CD-ROM и т.п.).

6. Контроль входящей и исходящей информации на защищаемых серверах и персональных компьютерах (далее ПК) осуществляется непрерывно посредством постоянно работающего компонента антивирусного программного обеспечения («монитора»). Полная проверка информации, хранящейся на серверах и ПК должна осуществляться не реже одного раза в месяц.

7. Обновление баз вирусов антивирусного программного обеспечения, установленного на ПК и серверах, должно осуществляться еженедельно.

8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка на защищаемом автоматизированном рабочем месте (АРМ) - ответственным за обеспечение информационной безопасности.

9. 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.) сотрудник организации самостоятельно или вместе с ответственным за антивирусную защиту организации должен провести внеочередной антивирусный контроль своей рабочей станции.

10. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

-приостановить работу;

-немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе;

-совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования:

-провести лечение или уничтожение зараженных файлов.

11. Ответственность за антивирусный контроль в организации, в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИСПДн.

12. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками осуществляется ответственным за антивирусную защиту организации.

ЛИСТ ОЗНАКОМЛЕНИЯ

с инструкцией по идентификации и аутентификации
с инструкцией по антивирусной защите

№ п/п	Фамилия, имя, отчество работника	Дата ознакомления	Ознакомлен, обязуюсь соблюдать (подпись работника)
1	*2*	*3*	*4*
1	Дубовицкий И.В.	20.01.2023	
2	Миловзоров А.В.	20.01.2023	