

###### – трудовая книжка работника;

###### – трудовой договор с работником и дополнительные соглашения к нему;

###### – медицинская книжка;

###### – личная карточка работника (форма № Т-2);

###### – приказы по личному составу;

###### – документы по оплате труда;

###### – документы об аттестации работников;

###### – классные журналы, журналы обучения на дому, журналы внеурочной деятельности;

###### – табели учета рабочего времени.

###### 2.6. Специалист по кадрам БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению» обрабатывает следующие персональные данные родственников работников: сведения, предоставленные работником в объеме карты Т-2.

###### 2.7. Персональные данные родственников работников содержатся в личных делах работников и базах данных кадровых информационных систем.

###### 3. Сбор, обработка и хранение персональных данных

###### 3.1. Сбор персональных данных соискателей осуществляет должностное лицо БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению», которому поручен подбор кадров, в том числе из общедоступной информации о соискателях в интернете.

###### 3.2. Сбор персональных данных работников осуществляет специалист по кадраму самого работника. Если персональные данные работника можно получить только у третьих лиц, инспектор уведомляет об этом работника и берет у него письменное согласие на получение данных.

###### 3.3. Сбор персональных данных родственников работника осуществляет инспектор отдела кадров из документов личного дела, которые представил работник.

###### 3.4. Обработка персональных данных соискателей ведется исключительно в целях определения возможности их трудоустройства.

###### 3.5. Обработка персональных данных работников ведется исключительно в целях обеспечения соблюдения законодательства РФ, содействия работникам в трудоустройстве, получении образования, продвижении по службе, обеспечения их личной безопасности и сохранности имущества, контроля количества и качества выполняемой ими работы.

###### 3.6. Обработка персональных данных родственников работников ведется исключительно в целях обеспечения соблюдения законодательства РФ, реализации прав работников, предусмотренных трудовым законодательством и иными актами, содержащими нормы трудового права.

###### 3.7. Сбор и обработка персональных данных, которые относятся к специальной категории (сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни) возможны только с согласия субъекта персональных данных либо в следующих случаях:

###### – персональные данные общедоступны;

###### – обработка персональных данных ведется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством РФ;

###### – обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц, а получить согласие у субъекта персональных данных невозможно;

###### – обработка персональных данных ведется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработку персональных данных осуществляет лицо, профессионально занимающееся медицинской деятельностью и обязанное в соответствии с законодательством РФ сохранять врачебную тайну;

###### – обработку персональных данных регламентирует законодательство РФ об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве либо уголовноисполнительное законодательство РФ.

###### 3.8. Сбор и обработка персональных данных родственников работников, которые относятся к специальной категории (сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни), не допускаются.

###### 3.9. Сбор и обработка персональных данных соискателей, работников и их родственников о членстве в общественных объединениях или профсоюзной деятельности не допускаются, за исключением случаев, предусмотренных федеральными законами.

###### 3.10. Личные дела, трудовые и медицинские книжки работников хранятся в бумажном виде в папках в сейфе, обеспечивающего защиту от несанкционированного доступа.

###### 3.11. Документы, содержащие личную информацию о работнике, кроме указанных в пункте 3.10 Положения, хранятся в бумажном виде в кабинете директора и в электронном виде в информационных системах БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению».

###### 3.12. Документы соискателя, который не был трудоустроен, уничтожаются в течение трех дней с момента принятия решения об отказе в трудоустройстве.

###### 3.13. Документы, содержащие персональные данные работников и родственников работников, подлежат хранению и уничтожению в сроки и в порядке, предусмотренные номенклатурой дел и архивным законодательством РФ.

###### 3.14. Работники вправе требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушениями требований Трудового кодекса или иного федерального закона. Персональные данные оценочного характера работник вправе дополнить заявлением, выражающим его собственную точку зрения. По требованию работника специалист по кадрам БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению» обязан известить всех лиц, которым ранее были сообщены неверные или неполные персональные данные этого работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

###### 4. Доступ к персональным данным

###### 4.1. Доступ к персональным данным соискателя имеют:

###### – директор – в полном объеме;

###### – заместители директора – в полном объеме;

###### – специалист по кадрам – в полном объеме.

###### 4.2. Доступ к персональным данным работника имеют:

###### – директор – в полном объеме;

###### – заместители директора – в полном объеме;

###### - специалист по кадрам - в полном объеме.

###### 4.3. Доступ к персональным данным родственников работника имеют:

###### – директор – в полном объеме;

###### – заместители директора – в полном объеме;

###### – специалист по кадрам– в полном объеме.

###### 4.4. Перечень лиц, допущенных к обработке персональных данных соискателей и работников, утверждается приказом директора БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению»

###### 5. Передача персональных данных

###### 5.1. Работники БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению» имеющие доступ к персональным данным соискателей, работников и родственников работников, при передаче этих данных должны соблюдать следующие требования:

###### 5.1.1. Не передавать и не распространять персональные данные без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо: – для предупреждения угрозы жизни и здоровью субъекта персональных данных, если получить такое согласие невозможно; – для статистических или исследовательских целей (при обезличивании); – в случаях, напрямую предусмотренных федеральными законами.

###### 5.1.2. Передавать без согласия субъекта персональных данных информацию в государственные и негосударственные функциональные структуры, в том числе в налоговые инспекции, фонды медицинского и социального страхования, пенсионный фонд, правоохранительные органы, страховые агентства, военкоматы, медицинские организации, контрольно-надзорные органы при наличии оснований, предусмотренных в федеральных законах, или запроса от данных структур со ссылкой на нормативное правовое основание для предоставления такой информации.

###### 5.1.3. Размещать без согласия работников в целях обеспечения информационной открытости БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению»

###### на официальном сайте БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению»

###### 5.1.3.1. Информацию о директоре БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению», его заместителях, в том числе:

###### – фамилию, имя, отчество (при наличии);

###### – должность;

###### – контактные телефоны;

###### – адрес электронной почты.

###### 5.1.3.2. Информацию о персональном составе педагогических работников с указанием уровня образования, квалификации и опыта работы, в том числе:

###### – фамилию, имя, отчество (при наличии);

###### – занимаемую должность (должности);

###### – преподаваемые дисциплины;

###### – ученую степень (при наличии);

###### – ученое звание (при наличии);

###### – наименование направления подготовки и (или) специальности;

###### – данные о повышении квалификации и (или) профессиональной переподготовке (при наличии);

###### – общий стаж работы;

###### – стаж работы по специальности.

###### 5.1.4. Передавать персональные данные представителям работников и соискателей в порядке, установленном Трудовым кодексом, ограничивая эту информацию только теми персональными данными, которые необходимы для выполнения функций представителя, подтвержденных документально.

###### 5.2. Передача персональных данных соискателей, работников и их родственников работником одного структурного подразделения работнику другого структурного подразделения осуществляется в порядке и на условиях, определенных локальным актом БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению». Лица, которые получают персональные данные, должны быть предупреждены о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Директор БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению» и уполномоченные им лица вправе требовать подтверждения исполнения этого правила.

###### 6. Меры обеспечения безопасности персональных данных

###### 6.1. К основным мерам обеспечения безопасности персональных данных в БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению» относятся:

###### 6.1.1. Назначение ответственного за организацию обработки персональных данных. В обязанности ответственного входит организация обработки персональных данных, обучение и инструктаж работников, внутренний контроль за соблюдением в БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению» требований законодательства к защите персональных данных.

###### 6.1.2. Издание политики обработки персональных данных и локальных актов по вопросам обработки персональных данных.

###### 6.1.3. Ознакомление работников, осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями к защите персональных данных, политикой обработки персональных данных и локальными актами БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению» по вопросам обработки персональных данных.

###### 6.1.4. Определение угроз безопасности персональным данным при их обработке с использованием средств автоматизации и разработка мер по защите таких персональных данных.

###### 6.1.5. Установление правил доступа к персональным данным, обрабатываемым с использованием средств автоматизации, а также регистрация и учет всех действий, совершаемых с персональными данными в информационных системах, контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем.

###### 6.1.6. Учет машинных носителей персональных данных.

###### 6.1.7. Проведение мероприятий при обнаружении несанкционированного доступа к персональным данным, обрабатываемым с использованием средств автоматизации, в том числе восстановление персональных данных, которые были модифицированы или уничтожены вследствие несанкционированного доступа к ним.

###### 6.1.8. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства о персональных данных, оценка соотношения указанного вреда и принимаемых мер.

###### 6.1.9. Внутренний контроль и (или) аудит соответствия обработки персональных данных требованиям законодательства.

###### 6.1.10. Публикация политики обработки персональных данных и локальных актов по вопросам обработки персональных данных на официальном сайте БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению».

###### 7. Ответственность

###### 7.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных соискателей на вакантные должности, работников, в том числе бывших, и их родственников, привлекаются к дисциплинарной и материальной ответственности, а в случаях, установленных законодательством РФ, – к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

###### 7.2. Моральный вред, причиненный соискателям на вакантные должности, работникам, в том числе бывшим, и их родственникам вследствие нарушения их прав, нарушения правил обработки персональных данных, а также несоблюдения требований к защите персональных данных, подлежит возмещению в порядке и на условиях, предусмотренных законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

###### Общие положения

1.1.Настоящее Положение разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных», 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»

1.2.Положение разработано в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению» (далее – ИСПДн).

1.3.Положение определяет порядок работы коллектива БОУ ВО «Грязовецкая школа-интернат для обучающихся с ОВЗ по зрению» (далее - ОУ) в 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 коллектива ОУ 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.

###### Порядок предоставления допуска пользователей к работе в ИСПДн

2.1.Первоначальный допуск пользователей к работе в ИСПДн осуществляется на основании приказа, который издается директором ОУ (далее директор). В приказе определяется список сотрудников, допущенных к работе в ИСПДн.

2.2.С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации и выполнения необходимых мероприятий по обеспечению безопасности в ИСПДн директором на основании приказа назначается ответственный за организацию обработки персональных данных и ответственный за безопасность при работ в ИС.

2.3.С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе в ИСПДн, присваивается 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.

2.4.Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется ответственным за безопасность при работ в ИС

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

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

3.2.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 ОУ, допущенные к работе с ПДн, принимают под роспись **обязательство о неразглашении персональных данных** (Приложение 4).

Пользователь обязан, ознакомится с **инструкцией пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники МБОУ «Вавожская СОШ»** (Приложение 5), а также с **инструкцией пользователя, по проведению антивирусного контроля на объектах вычислительной техники МБОУ «Вавожская СОШ»** (Приложение 6) под роспись.

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

Запись информации, содержащей ПДн, должна осуществляться только на машинные носители информации, соответствующим образом учтенные в Журнале учета защищаемых носителей информации. Ответственным за ведение Журнала учета является администратор безопасности;

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, 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. 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;

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.);

вводить описания пользователей ИСПДн в информационную базу системы разграничения доступа в ИСПДн;

своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

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;

настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;

организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации;

периодически тестировать функции СЗИ от НСД с использованием специальных средств анализа защищенности, особенно при изменении программной среды и полномочий исполнителей;

восстанавливать программную среду, программные средства и настройки СЗИ при

сбоях;

вести две копии программных средств СЗИ от НСД и контролировать их

работоспособность;

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.

###### 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 периодическое резервное копирование персональных данных.

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 администратору безопасности, или директору.

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.

Ответственность за проведение резервного копирования, мероприятий по восстановлению работоспособности технических средств, мероприятий по восстановлению средств защиты информации возлагается на администратора безопасности.

###### 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 ОУ является администратор безопасности;

###### 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.

###### 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 365 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 приказа директора.

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, хранения и использования возлагается на администратора безопасности.

###### 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.

Право внесения изменений в конфигурацию аппаратно-программных средств защиты информации предоставляется администратору безопасности, по согласованию с директором ОУ.

Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме администратора безопасности запрещено.

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 оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.).

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.

###### 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 учреждении, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

выявление демаскирующих признаков объектов ИСПДн;

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

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

проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

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

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

оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;

разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

###### Порядок охраны и допуска посторонних лиц в помещения ИСПДн

В ОУ должна быть 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.

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 сторожа. О происшествии немедленно сообщается директору.

###### Заключительные положения

Требования настоящего Положения обязательны для всего коллектива ОУ, обрабатывающих персональные данные.

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

Сведения о работниках БОУ ВО «Грязовецкая школа-интернат дл обучающихся с ОВЗ по зрению» (на 01.10.2019г)

|  |  |  |
| --- | --- | --- |
| № п\п | ФИО | Должность |
| 1 | Хамматова Наталья Николаевна | заместитель директора по учебной работе |
| 2 | Корчагова Людмила Валентиновна | Учитель |
| 3 | Ельцова Елена Александровна | Учитель |
| 4 | Зубова Нина Александровна | Учитель |
| 5 | Кудряшова Анастасия Владимировна | Учитель |
| 6 | Баланичева Ирина Генадьевна | учитель-логопед |
| 7 | Нечаева Елена Борисовна | Учитель |
| 8 | Козина Елена Анатольевна | Учитель |
| 9 | Столярчук Наталья Геральдовна | Учитель |
| 10 | Пешкова Наталия Сергеевна | Учитель |
| 11 | Чиркова Ольга Николаевна | Учитель |
| 12 | Желтова Галина Николаевна | Учитель |
| 13 | Смирнова Юлия Вениаминовна | учитель-логопед |
| 14 | Раскатова Анна Владимировна | учитель-психолог |
| 15 | Тютикова Наталья Алексеевна | учитель |
| 16 | Фунтова Татьяна Федоровна | Учитель |
| 17 | Шевченко Светлана Алексеевна | Учитель |
| 18 | Шишина Зинаида Александровна | Учитель |
| 19 | Серова Людмила Анатольевна | Воспитатель |
| 20 | Родионова Ираида Леонидовна | Воспитатель |
| 21 | Смирнова Алевтина Петровна | Воспитатель |
| 22 | Родионова Валентина Валентиновна | Воспитатель |
| 23 | Алешина Любовь Константиновна | Воспитатель |
| 24 | Джавадова Галина Александровна | Воспитатель |
| 25 | Пылаева Надежда Александровна | Воспитатель |
| 26 | Свиркунова Елена Вениаминовна | Воспитатель |
| 27 | Турок Татьяна Константиновна | Воспитатель |
| 28 | Цветкова Наталья Васильевна | Воспитатель |
| 29 | Цветкова Екатерина Михайловна | Воспитатель |
| 30 | Паничева Елена Алексеевна | старший воспитатель |
| 31 | Борисова Любовь Вячеславовна | Воспитатель |
| 32 | Ермакова Александра Всеволодовна | Учитель |
| 33 | Гладкова Светлана Юрьевна | заместитель директора по воспитательной работе |
| 34 | Баранов Владимир Валентинович | Электрик |
| 35 | Ратина Елена Александровна | медицинская сестра |
| 36 | Смирнова Нина Васильевна | Повар |
| 37 | Замолина Татьяна Вениаминовна | подсобный рабочий |
| 38 | Скулябина Юлия Михайловна | подсобный рабочий |
| 39 | Бобылев Сергей Валентинович | работник по комплесному обслуживанию |
| 40 | Шевелкина Любовь Ришадовна | Повар |
| 41 | Кочкарева Ольга Николаевна | шеф-повар |
| 42 | Тяпушкин Александр Николаевич | Водитель |
| 43 | Колесова Татьяна Валентиновна | уборщик служебных помещений |
| 44 | Шестакова Елена Александровна | уборщик служебных помещений |
| 45 | Леонова Татьяна Вадимовна | экономист |
| 46 | Шепелева Любовь Павловна | уборщик служебных помещений |
| 47 | Седунова Евгения Александровна | Кладовщик |
| 48 | Хахина Ирина Николаевна | уборщик служебных помещений |
| 49 | Швецова Екатерина Александровна | Лаборант |
| 50 | Травникова Наталья Витальевна | младший воспитатель |
| 51 | Ного Светлана Николаевна | уборщик служебных помещений |
| 52 | Хитрякова Наталья Юрьевна | заместитель директора по управлению ресурсами |
| 53 | Тарасенко Анна Вячеславовна | педагог-библиотекарь |
| 54 | Зверева Светлана Васильевна | Директор |
| 55 | Рогозина Светлана Степановна | специалист по кадрам |
| 56 | Уткина Наталья Сергеевна | Учитель |
| 57 | Щучкина Екатерина Николаевна | Учитель |
| 58 | Бряконогова Ольга Николаевна | младший воспитатель |
| 59 | Козлова Галина Васильевна | кастелянша |
| 60 | Салаев Шаназар Раджабович | уборщик территории |
| 61 | Коноплев Николай Александрович | учитель |
| 62 | Шашукова Ирина Николаевна | специалист по закупкам |
| 63 | Миранкова Елена Анатольевна | Уборщик служебных помещений |
| 64 | Шахов Владимир Александрович | Учитель |