МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ЖЕЛЯБОВСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА» НИЖНЕГОРСКОГО РАЙОНА РЕСПУБЛИКИ КРЫМ

ПРИКАЗ

18.12.2024 с Желябовка № 408-о

Об утверждении инструкций по защите персональных данных

Во исполнение Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», Федерального закона от 30 декабря 2020 г. № 519-ФЗ “О внесении изменений в Федеральный закон «О персональных данных». Федерального закона Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных» и прочих нормативных документов по защите информации, а также с целью обеспечения безопасности персональных данных,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Инструкцию пользователя информационных систем персональных данных в муниципальном бюджетном образовательном учреждении «Желябовская СОШ» Нижнегорского района Республики Крым (приложение 1).
2. Утвердить и ввести в действие Инструкцию по парольной защите информации в муниципальном бюджетном образовательном учреждении «Желябовская СОШ» Нижнегорского района Республики Крым (приложение 2).
3. Утвердить и ввести в действие Инструкцию по организации антивирусной защиты информации в муниципальном бюджетном образовательном учреждении «Желябовская СОШ» Нижнегорского района Республики Крым (приложение 3).
4. Утвердить и ввести в действие Инструкцию по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных в муниципальном бюджетном образовательном учреждении «Желябовская СОШ» Нижнегорского района Республики Крым (приложение 4).
5. Требования настоящего приказа довести до работников, осуществляющих обработку персональных данных в информационных системах персональных данных в муниципальном бюджетном образовательном учреждении «Желябовская СОШ» Нижнегорского района Республики Крым.
6. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МБОУ «Желябовская СОШ» Т.Ю.Тупальская

Приложение 1
к приказу МБОУ «Желябовская СОШ»
от 18.12.2024 № 408-о

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных в муниципальном бюджетном образовательном учреждении « Желябовская СОШ» Нижнегорского района Республики Крым

1. Термины и определения

1.1. *Автоматизированное рабочее место* – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

1.2. *Антивирусная защита* – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование «зараженных» объектов, удаление вредоносных компьютерных программ (вирусов) из «зараженных» объектов).

1.3. *Информационная система персональных данных* – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.4. *Обработка персональных данных* – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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

1.7. *Пользователь информационной системы персональных данных* – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.

1.8. *Средство антивирусной защиты* – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

1.9. *Средство защиты информации* – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция пользователя информационных систем персональных данных муниципального бюджетного образовательного учреждения «Желябовская СОШ» Нижнегорского района Республики Крым (далее – Инструкция) определяет обязанности, права и ответственность работников при работе в информационных системах персональных данных (далее – ИСПДн).

2.2. Требования настоящей Инструкции являются обязательными для всех работников, осуществляющих обработку и защиту персональных данных (далее – ПДн) в ИСПДн – пользователей ИСПДн (далее – Пользователи).

2.3. К защищаемой информации, обрабатываемой в ИСПДн в муниципальном бюджетном образовательном учреждении «Желябовская СОШ» Нижнегорского района Республики Крым (далее – Учреждение), относятся ПДн, служебная (технологическая) информация системы защиты и другая информация ограниченного доступа.

2.4. Все пользователи ИСПДн Учреждения должны быть ознакомлены с требованиями настоящей Инструкции под подпись.

2.5. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Допуск пользователей к информационным системам персональных данных

3.1. Допуск пользователей к работе с ПДн в ИСПДн осуществляется в соответствии с «Перечнем должностей работников муниципального бюджетного образовательного учреждении «Желябовская СОШ» Нижнегорского района Республики Крым», допущенных к обработке персональных данных».

3.2. К самостоятельной работе на автоматизированных рабочих местах (далее – АРМ), входящих в состав ИСПДн, допускаются лица, изучившие требования настоящей Инструкции и локальных нормативных актов по защите информации, освоившие правила эксплуатации АРМ и технических средств защиты.

3.3. Допуск производится после проверки знания настоящей Инструкции и практических навыков в работе.

4. Обязанности пользователя

4.1. Каждый Пользователь имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

4.1.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн.

4.1.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн.

4.1.3. Выполнять требования по антивирусной защите в части, касающейся действий Пользователей.

4.1.4. Немедленно ставить в известность ответственного за обеспечение безопасности ПДн в ИСПДн или администратора ИСПДн:

- при подозрении компрометации личного пароля;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн;
- некорректного функционирования установленных средств защиты;
- обнаружения непредусмотренных отводов кабелей и подключенных устройств;
- обнаружения фактов, попыток несанкционированного доступа и случаев нарушения установленного порядка обработки ПДн.

4.1.5. Экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами.

4.2. Пользователям ИСПДн запрещается:

- отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на ИСПДн;
- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав Пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные атрибуты и пароли доступа к ресурсам ИСПДн;
- работать в ИСПДн при обнаружении каких-либо неисправностей;
- оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц;
- производить перемещения технических средств АРМ без согласования с ответственным за обеспечение безопасности ПДн в ИСПДн;
- вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств.

5. Организация работы со съемными машинными носителями информации

5.1. Организация работы со съемными машинными носителями информации (далее – СМНИ), содержащие ПДн и иную информацию конфиденциального характера, осуществляется в соответствии с «Порядком обращения со съемными машинными носителями информации» муниципального бюджетного образовательного учреждения «Желябовская СОШ» Нижнегорского района Республики Крым.

5.2. Пользователи обязаны знать и соблюдать установленные требования по учету и хранению СМНИ.

5.3. СМНИ должны быть зарегистрированы в «Журнале учета съемных машинных носителей информации».

5.4. СМНИ закрепляется за определенным лицом, несущим ответственность за сохранность и местонахождение данного СМНИ.

5.5. При необходимости передачи информации на СМНИ, лицо ответственное за хранение уведомляет ответственного за обеспечение безопасности ПДн в ИСПДн о необходимости передачи информации с помощью СМНИ, доставляет СМНИ по месту назначения, передает информацию с него и возвращает его на место хранения.

5.6. Хранение СМНИ осуществляется:

- для флеш-карт, смарт-карт, компакт дисков и др.) в защищенных сейфах;
- для СМНИ, входящих в состав ИСПДн, производится опечатывание корпуса АРМ.

5.7. Пользователям запрещается:

- записывать и хранить ПДн и иную информацию конфиденциального характера на неучтенных СМНИ;
- оставлять СМНИ без присмотра, передавать их другим лицам и выносить за пределы контролируемой зоны, за исключением случаев, в которых разрешена передача СМНИ;
- хранить СМНИ вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;
- хранить на учтенных СМНИ программы и данные, не относящиеся к рабочей информации.

6. Организация парольной защиты

6.1. Организация парольной защиты производится в соответствии с «Инструкцией по парольной защите информации в муниципальном бюджетном образовательном учреждении «Желябовская СОШ» Нижнегорского района Республики Крым.

6.2. Лица, использующие пароли, обязаны:

- хранить в тайне свой пароль
- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов;
- своевременно сообщать ответственному за обеспечение безопасности ПДн в ИСПДн обо всех нештатных ситуациях, нарушениях работы систем защиты от несанкционированного доступа, возникающих при работе с паролями.

6.3. Во время ввода паролей необходимо исключить возможность его просмотра посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или отражённом свете) или техническими средствами (видеокамеры, фотоаппараты и др.)

6.4. Для предотвращения доступа к персональным данным, пользователь во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации Ctrl+Alt+Delete и кнопки «Блокировать» или нажатием комбинации Win+L.

6.5. Блокирование сеанса доступа пользователя в ИСПДн осуществляется после 15 минут его бездействия (неактивности).

6.6. В случае утери пароля работник ставит в известность своего непосредственного руководителя и ответственного за обеспечение безопасности ПДн в ИСПДн для принятия последующих решений.

6.7. В случае компрометации пароля (просмотр посторонними, разглашение пароля и др.) необходимо известить своего непосредственного руководителя и ответственного за обеспечение безопасности ПДн в ИСПДн для принятия последующих решений.

7.

8. Правила работы в сетях общего доступа и (или) международного обмена

7.1. Работа в сетях общего доступа и на элементах ИСПДн, должна осуществляться исключительно в служебных целях.

7.2. При работе в сетях общего доступа запрещается:

- осуществлять работу при отключенных средствах защиты;
- передавать по сетям общего доступа защищаемую информацию без использования средств шифрования;

- запрещается скачивать из сети Интернет программное обеспечение и другие файлы, если это не определено его должностными обязанностями;
- запрещается посещение и использование сети Интернет в личных целях.

9. Порядок установки обновлений программного обеспечения

8.1. Установке крупных обновлений программного обеспечения должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий от устанавливаемых обновлений.

8.2. В случае обнаружения негативного воздействия устанавливаемого обновления на штатное функционирование информационной инфраструктуры, данное обновление устанавливаться не должно по согласованию с администратором ИСПДн.

8.3. Установке новых версий программного обеспечения или внесению серьезных изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий указанного программного обеспечения.

8.4. Установка протестированных обновлений, новых версий программного обеспечения или внесение изменений и дополнений в действующее программное обеспечение может быть произведено только по согласованию с администратором ИСПДн и ответственным за обеспечение безопасности ПДн в ИСПДн.

10. Технология обработки персональных данных

9.1. При первичном допуске к работе в ИСПДн Пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, изучает Инструкцию, получает персональный идентификатор или личный пароль у ответственного за обеспечение безопасности ПДн в ИСПДн.

9.2. В процессе работы Пользователь производит обработку ПДн в ИСПДн.

9.3. При необходимости вывод ПДн из ИСПДн осуществляется следующим образом:

- копированием ПДн на учтенные СМНИ;
- передача ПДн по каналам связи с обязательным применением криптографической защиты.

11. Срок действия и порядок внесения изменений

10.1. Настоящая Инструкция вступает в силу с момента его утверждения и действует бессрочно.

10.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

10.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.

Приложение 2
к приказу МБОУ «Желябовская СОШ»
от 18.12.2024 № 408-о

ИНСТРУКЦИЯ
по парольной защите информации в муниципальном бюджетном образовательном учреждении «Желябовская СОШ» Нижнегорского района Республики Крым

1. Термины и определения

1.1. *Автоматизированное рабочее место* – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

1.2. *Информационная система персональных данных* – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.3. *Обработка персональных данных* – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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

1.6. *Пользователь информационной системы персональных данных* – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.

1.7. *Средство защиты информации* – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по парольной защите информации в муниципальном бюджетном образовательном учреждении «Желябовская СОШ» Нижнегорского района Республики Крым (далее – Инструкция) устанавливает требования и ответственность при организации парольной защиты информации, а также определяет порядок контроля за действиями пользователей и обслуживающего персонала информационных систем персональных данных (далее – ИСПДн) при работе с паролями.

2.2. Требования настоящей Инструкции являются обязательными для исполнения всеми пользователями и администраторами ИСПДн муниципального бюджетного образовательного учреждения «Желябовская СОШ» Нижнегорского района Республики Крым (далее – Учреждение), использующими в своей работе средства вычислительной техники.

2.3. Все пользователи и администраторы ИСПДн Учреждения, использующие в своей работе средства вычислительной техники, должны быть ознакомлены с требованиями настоящей Инструкции под подпись.

2.4. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных (далее – ПДн), и не исключает обязательного выполнения их требований.

3. Требования, предъявляемые к идентификаторам (кодам) и паролям (порядок формирования и обращения с ними)

3.1. Авторизация пользователей ИСПДн осуществляется путем ввода идентификатора и/или пароля.

3.2. Требования к формированию паролей и обращению с ними.

3.2.1. Пароль формируется при создании учетной записи ответственным обеспечение безопасности ПДн в ИСПДн или администратором ИСПДн, при первичном входе в учетную запись пароль должен быть изменен владельцем.

3.2.2. Владельцы личных паролей обязаны обеспечить их тайну.

3.2.3. Пароли генерируются с учетом следующих требований:

- пароль должен знать только его владелец;
- длина пароля должна быть не менее 8 символов;
- в пароле обязательно должны присутствовать как цифры, так и буквы на верхнем и нижнем регистрах;
- пароль не должен включать смысловую нагрузку (имена, фамилии, наименования организаций, улиц, городов и т.д.), общепринятые сокращения (userOl, password02 и т.п.) и последовательные сочетания клавиш клавиатуры (qwertyOl, Ицукен12);
- максимальный срок действия пароля составляет 120 дней;
- минимальный срок действия пароля составляет 2 дня;
- количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя должно быть не более 6.

3.2.4. Требования к формированию паролей обеспечиваются техническими возможностями используемых операционных систем, средств защиты информации и информационных ресурсов.

3.2.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полгода. Внеплановая смена пароля производится в случае его компрометации, а также по просьбе пользователя ИСПДн.

3.2.6. Хранение пользователями ИСПДн значений своих паролей на бумажном носителе ЗАПРЕЩЕНО.

3.2.7. Пользователь не имеет права сообщить личный пароль другим лицам (разрешается только с согласования ответственного за обеспечение безопасности или администратора ИСПДн при наличии технологической необходимости использования имен и паролей работников в их отсутствие в случае возникновения нештатбных ситуаций, форс-мажорных обстоятельств и т.п. По возвращению работники обязаны сразу же сменить свои пароли на новые значения согласно данной Инструкции).

3.3. Порядок смены паролей и идентификаторов при изменениях в организационно-штатной структуре (кадровые перестановки, увольнение работников):

3.3.1. При прекращении действия трудового договора с работником все созданные для этого работника учетные записи (пользовательское имя) подлежат блокированию не позднее, чем в день увольнения работника. Полное удаление учетных записей производится в течении 5 рабочих дней со дня увольнения работника. Основанием для

блокирования и последующего удаления учетных записей работника является заявка, представленная непосредственным руководителем увольняемого не позднее, чем за 3 рабочих дня до дня его увольнения.

3.3.2. При проведении организационно-штатных мероприятий (кадровые перестановки) непосредственный руководитель структурного подразделения обязан представить администратору ИСПДн заявку на изменение в правах доступа.

3.4. Порядок действий при компрометации идентификаторов и паролей.

3.4.1. Под компрометацией понимается: утрата пароля учетной записи и (или) пароля идентификатора, разглашение учетной записи пароля или пароля идентификатора (явная компрометация), или иная ситуация, которая дает основание для предположения о нарушении конфиденциальности паролей и идентификаторов (неявная компрометация).

3.4.2. При выявлении факта утраты пароля, разглашения пароля, пароля идентификатора, самого идентификатора пользователь обязан незамедлительно сообщить о данных фактах своему непосредственному руководителю и ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн.

3.4.3. В случае выявления факта компрометации идентификаторов и паролей пользователя администратор ИСПДн или ответственный за обеспечение безопасности ПДн в ИСПДн обязан немедленно заблокировать учетную запись данного пользователя и незамедлительно произвести внеплановую смену пароля для этого пользователя.

4. Права и обязанности

4.1. Основные задачи администратора ИСПДн:

- организация установки средств идентификации и аутентификации;
- организация парольной защиты во всех ИСПДн;
- выдача первичных паролей, и электронных персональных идентификаторов и паролей к ним;
- осуществление контроля за состоянием системы парольной защиты информации в ИСПДн.

4.2. Администратор ИСПДн имеет право:

- вносить предложения по совершенствованию системы парольной защиты информации в ИСПДн;
- принимать участие в планировании мероприятий по парольной защите информации в ИСПДн и планировании оснащения средствами идентификации и аутентификации;
- осуществлять контроль состояния средств идентификации и аутентификации в ИСПДн;
- инициировать служебные проверки и участвовать в проведении расследований по фактам компрометации;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств идентификации и аутентификации.

4.3. Обязанности в части парольной защиты информации отражены в инструкции администратора ИСПДн.

4.4. Пользователям ИСПДн в своей работе запрещается:

- сообщать кому-либо свой личный пароль и/или пароль к электронному персональному идентификатору;
- передавать кому-либо выданный электронный персональный идентификатор;

- осуществлять вход в операционные системы ИСПДн и в информационные ресурсы под чужими идентификаторами и паролями;
- отключать средства идентификации и аутентификации.

4.5. В случае появления подозрений на факт компрометации пароля, а также в случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств идентификации и аутентификации, пользователи обязаны немедленно проинформировать об этом ответственного за обеспечение безопасности ПДн в ИСПДн или администратора ИСПДн.

5. Ответственность должностных лиц в рамках системы парольной защиты информации

5.1. Пользователи, ответственный за обеспечение безопасности ПДн в ИСПДн и администратор ИСПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

5.2. Пользователи, ответственный за обеспечение безопасности ПДн в ИСПДн и администратор ИСПДн несут ответственность по действующему законодательству Российской Федерации за разглашение сведений конфиденциального характера, ставших известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

6.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

6.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

6.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.

Приложение 3
к приказу МБОУ «Желябовская СОШ»
от 18.12 .2024 № 408-о

ИНСТРУКЦИЯ
по антивирусной защите в муниципальном бюджетном образовательном учреждении «Желябовская СОШ» Нижнегорского района Республики Крым

1. Термины и определения

1.1. *Автоматизированное рабочее место* – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

1.2. *Антивирусная защита* – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование «зараженных» объектов, удаление вредоносных компьютерных программ (вирусов) из «зараженных» объектов).

1.3. *Информационная система персональных данных* – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.4. *Обработка персональных данных* – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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

1.7. *Пользователь информационной системы персональных данных* – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.

1.8. *Средство антивирусной защиты* – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

1.9. *Средство защиты информации* – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по антивирусной защите в муниципальном бюджетном образовательном учреждении дополнительного образования «Центр детского и юношеского творчества» Нижнегорского района Республики Крым (далее – Инструкция)

регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля.

2.2. Инструкция устанавливает требования и ответственность при организации защиты информации от разрушающего воздействия вредоносных программ – компьютерных вирусов.

2.3. Требования настоящей Инструкции являются обязательными для исполнения всеми работниками муниципального бюджетного образовательного учреждения «Желябовская СОШ» Нижнегорского района Республики Крым (далее – Учреждения), использующими в своей работе средства вычислительной техники.

2.4. Все работники Учреждения, использующие антивирусные средства, должны быть ознакомлены с требованиями настоящей Инструкцией под подпись.

2.5. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных (далее – ПДн), и не исключает обязательного выполнения их требований.

3. Требования к антивирусным средствам

3.1. В Учреждении к применению допускаются лицензионные антивирусные программные и (или) программно-аппаратные средства (антивирусные средства), закупленные у разработчика указанных средств или его официальных дилеров.

3.2. Антивирусные средства должны функционировать в течение всего времени работы средств вычислительной техники (от момента загрузки операционной системы до момента ее выгрузки).

3.3. Антивирусное средство не должно существенно затруднять работоспособность средств вычислительной техники информационных систем персональных данных (далее – ИСПДн).

4. Права и обязанности

4.1. Антивирусной защите подлежит вся, обрабатываемая в Учреждении при помощи средств вычислительной техники, информация, независимо от ограничений доступа к ней.

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

4.3. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

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

4.5. Сопровождение (регулярное обновление, антивирусный контроль, выявление фактов заражения и проведение служебных расследований) правил антивирусной защиты возлагаются на ответственного за обеспечение безопасности ПДн в ИСПДн.

4.6. Основные задачи ответственного за обеспечение безопасности ПДн в ИСПДн:

- организация процесса установки антивирусных средств в ИСПДн;
- сопровождение антивирусных средств (обновление, антивирусный контроль, сопровождение действий пользователей в случаях обнаружения вирусов, обеспечение работоспособности антивирусных средств);

- контроль состояния системы антивирусной защиты информации в Учреждении.

4.7. Ответственный за обеспечение безопасности ПДн в ИСПДн несет ответственность за:

- за своевременную установку антивирусных средств;
- за эксплуатацию (антивирусный контроль, работоспособность антивирусных средств, сопровождение действий пользователей в случаях обнаружения вирусов) системы антивирусной защиты информации;
- за своевременное обновление лицензий на антивирусные средства;
- за своевременное обновление антивирусных баз.

4.8. Ответственный за обеспечение безопасности ПДн в ИСПДн имеет право:

- вносить предложения по совершенствованию системы антивирусной защиты информации;
- принимать участие в планировании мероприятий по антивирусной защите информации и планировании оснащения антивирусными средствами;
- осуществлять контроль состояния средств антивирусной защиты информации в Учреждении;
- инициировать служебные проверки и участвовать в проведении расследований по фактам заражения вирусами ИСПДн и средств вычислительной техники;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты.

4.9. Пользователь антивирусного средства – лицо, на рабочем месте которого применяется антивирусное средство.

4.10. Пользователям антивирусных средств запрещается:

- менять настройки или отключать средства антивирусной защиты во время работы;
- использовать средства антивирусной защиты, отличные от установленных средств;
- без разрешения ответственного за обеспечение безопасности ПДн в ИСПДн копировать любые файлы на съемные носители информации, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

5. Порядок и периодичность обновления антивирусных баз

5.1. Своевременное обновление баз данных средств антивирусной защиты информации является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

5.2. Установке обновлений должно предшествовать тестирование ИСПДн на отсутствие негативных воздействий от вновь устанавливаемых обновлений.

5.3. Установке новых версий программного обеспечения или внесению изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование ИСПДн на отсутствие негативных воздействий указанного программного обеспечения.

5.4. Периодичность обновления антивирусных баз:

- обновление антивирусных баз для всех ИСПДн, имеющих подключение к сетям общего пользования и сетям международного информационного обмена, должно быть ежедневным. Источник обновления – сервер разработчика

антивирусного средства, либо собственный централизованный сетевой источник обновлений, получающий обновления с сервера разработчика антивирусного средства.

- обновление антивирусных баз для ИСПДн, не имеющих подключение к сетям общего пользования и сетям международного информационного обмена, обновление должно быть не менее 1 раза в неделю. Источником обновления в данном случае являются антивирусные базы, записанные на предварительно учтенный в установленном порядке съемный машинный носитель информации.

6. Порядок и периодичность проведения антивирусного контроля

6.1. Объектами антивирусного контроля являются:

- жесткие магнитные диски рабочих станций и серверов ИСПДн;
- сетевые хранилища (системы хранения данных);
- оперативная и системная память средств вычислительной техники;
- съемные машинные носители информации;
- входящий и исходящий контент (веб-трафик);
- файлы, получаемые и передаваемые через сети общего пользования и международного информационного обмена;
- почтовые сообщения электронной почты.

6.2. Антивирусный контроль входящей информации со съемных машинных носителей информации необходимо проводить до переноса информации на жёсткий магнитный диск рабочей станции или сетевой диск. Информация, получаемая по телекоммуникационным каналам, должна проверятся вовремя, или сразу после получения. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

6.3. Виды и периодичность антивирусных проверок представлены в таблице 1.

Таблица 1

№ п/п	Объект контроля	Вид проверки	Периодичность проверки
1	Жесткие магнитные диски рабочих станций и серверов ИСПДн	Полная проверка	1 раз в месяц
		Быстрое сканирование	1 раз в неделю
2	Сетевые хранилища (системы хранения данных)	Полная проверка	1 раз в месяц
3	Оперативная и системная память средств вычислительной техники	Полная проверка	1 раз в месяц
		Быстрое сканирование	1 раз в неделю
4	Съемные машинные носители информации	Полная проверка	При каждом подключении

№ п/п	Объект контроля	Вид проверки	Периодичность проверки
5	Веб-трафик	Минимально необходимое требование - настройка антивирусного средства по умолчанию	Постоянно
6	Файлы, получаемые и передаваемые через сети общего пользования и международного информационного обмена	Полная проверка	При каждом получении и отправке
7	Почтовые сообщения электронной почты	Минимально необходимое требование - настройка антивирусного средства по умолчанию	При каждом получении и отправке

7. Порядок действий при обнаружении вирусов

7.1. Основными путями проникновения вирусов в ИСПДн являются: любые съемные машинные носители информации, электронные почтовые сообщения, трафик, получаемый из сетей общего пользования и сетей международного информационного обмена, ранее зараженные рабочие станции и сервера.

7.2. В случае обнаружения вирусов при входном контроле съемных машинных носителей информации, файлов или электронных почтовых сообщений, пользователь должен:

- немедленно приостановить все работы на своей рабочей станции;
- сообщить ответственному за обеспечение безопасности ПДн в ИСПДн о факте обнаружения вируса;
- принять согласованные с ответственным за обеспечение безопасности ПДн в ИСПДн меры по локализации и удалению вируса с использованием антивирусных средств.

7.3. При невозможности ликвидации последствий вирусного заражения ответственному за обеспечение безопасности ПДн в ИСПДн необходимо:

- сообщить о факте обнаружения программных вирусов в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;
- заархивировать зараженные файлы и направить с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации.

7.4. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется по решению ответственного за обеспечение безопасности ПДн в ИСПДн.

7.5. Факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ – все это относится к значимым нарушениям безопасности информации и должны быть проанализированы посредством проведения служебного расследования.

7.6. Служебное расследование проводится комиссией, назначаемой приказом Директора Учреждения. В состав комиссии в обязательном порядке включается администратор ИСПДн, ответственный за обеспечение безопасности ПДн в ИСПДн, непосредственный руководитель работника, допустившего факт компрометации. При необходимости в состав комиссии могут включаться другие работники.

7.7. Результаты работы комиссии оформляются актом. Акт подлежит утверждению Директора Учреждения.

7.8. В процессе работы комиссии обязательными для установления являются:

- дата и время заражения (обнаружения заражения);
- ФИО, должность и подразделение работника, техническое средство которого заражено вирусной программой;
- уровень критичности заражения;
- обстоятельства, способствовавшие заражению;
- информационные ресурсы, затронутые заражением;
- характер и размер реального и потенциального ущерба.

7.9. В ходе своей работы комиссия может запрашивать объяснительные записки от работников, подозреваемых в виновности заражения (путем письменного запроса их непосредственным руководителям). Объяснительная записка должна быть представлена комиссии в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа предоставить объяснительную записку, данный факт отражается в акте.

7.10. Уничтожение материалов расследования фактов заражения осуществляется в соответствии с установленными требованиями по делопроизводству и номенклатурой дел.

8. Ответственность

8.1. Пользователи и Ответственный за обеспечение безопасности ПДн в ИСПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

9. Срок действия и порядок внесения изменений

9.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

9.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

9.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.

Приложение 4
к приказу МБОУ «Желябовская СОШ»
от 18.12.2024 № 408-о

ИНСТРУКЦИЯ
по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных в муниципальном бюджетном образовательном учреждении «Желябовская СОШ» Нижнегорского района Республики Крым

1. Термины и определения

1.1. *Автоматизированное рабочее место* – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

1.2. *Информационная система персональных данных* – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.3. *Обработка персональных данных* – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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

1.6. *Пользователь информационной системы персональных данных* – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.

1.7. *Средство антивирусной защиты* – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

1.8. *Средство защиты информации* – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенные или используемые для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных в муниципальном бюджетном образовательном учреждении «Желябовская СОШ» Нижнегорского района Республики Крым (далее – Инструкция) устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных информационных систем персональных данных (далее –

ИСПДн) муниципального бюджетного образовательного учреждения «Желябовская СОШ» Нижнегорского района Республики Крым (далее – Учреждение), а также к резервированию аппаратных средств.

2.2. Настоящая Инструкция разработана с целью:

- определения категории информации, подлежащей обязательному резервному копированию;
- определения процедуры резервирования данных для последующего восстановления работоспособности ИСПДн при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- определения порядка восстановления информации в случае возникновения такой необходимости;
- упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

2.3. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн Учреждения, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения технических средств;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;

2.4. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности ИСПДн в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

2.5. Резервному копированию подлежит информация следующих основных категорий:

- информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в т.ч. систем управления базами данных (далее – СУБД) общего пользования и справочно-информационных систем общего использования;
- рабочие копии установочных компонентов программного обеспечения общего назначения и специализированного программного обеспечения серверов и рабочих станций;
- информация, необходимая для восстановления систем управления базами данных ИСПДн, локальной вычислительной сети, системы электронного документооборота;
- регистрационная информация систем защиты информации;
- другая информация ИСПДн, по мнению пользователей, администраторов ИСПДн и ответственного за обеспечение безопасности персональных данных (далее – ПДн) в ИСПДн, являющаяся критичной для работоспособности ИСПДн.

2.6. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности

сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Общие требования к резервному копированию

3.1. В Инструкции резервного копирования описываются действия при выполнении следующих мероприятий:

- резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);
- контроль резервного копирования;
- хранение резервных копий;
- полное или частичное восстановление данных.

4. Ответственность за состояние резервного копирования

4.1. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением соответствующей Инструкции, а также за выполнением требований по хранению резервных копий и предотвращению несанкционированного доступа к ним возлагается на ответственного за обеспечение безопасности ПДн в ИСПДн и администраторов ИСПДн.

4.2. В случае обнаружения попыток несанкционированного доступа к носителям резервной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается ответственному за обеспечение безопасности ПДн в ИСПДн в течение рабочего дня после обнаружения указанного события.

5. Периодичность резервного копирования

5.1. Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

5.2. Информация, содержащаяся в постоянно изменяемых базах данных, сохраняется в соответствии со следующим графиком:

- ежедневно проводится копирование измененной и дополненной информации (носители с ежедневной информацией должны храниться в течение недели);
- еженедельно проводится резервное копирование всей базы данных (носители с еженедельными копиями хранятся в течение месяца);
- ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

5.3. Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.).

6. Восстановление информации из резервных копий

6.1. В случае необходимости, восстановление данных из резервных копий производится ответственными работниками.

6.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

6.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

6.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

6.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

6.6. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

7. Срок действия и порядок внесения изменений

7.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

7.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

7.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.