СОГЛАСОВАНО
на Педагогическом совете
МОУ "ССОШ"
Протокол №1 от “30.08.2022”

Утверждаю
Директор школы
Г.Н.Смирнова
«30» августа 2022 г.
Приказ № 35

ПРИКАЗ

О назначении ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных и утверждении внутренних нормативных правовых актов по защите персональных данных в МОУ «Станская средняя общеобразовательная школа»

В целях обеспечения безопасности персональных данных при их обработке в МОУ «ССОШ» (далее – школа), во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» приказываю**:**

1. Назначить ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных школы (администратором безопасности ИСПДн) учителя информатики Кретову Юлию Владимировну.

2. Утвердить прилагаемый перечень следующих внутренних нормативных правовых актов:

Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных школы (Приложение 1);

Инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных школы (Приложение 2);

Инструкцию по организации антивирусной защиты школы (Приложение 3);

Инструкцию по порядку учета и хранению документов, содержащих персональные данные школы(Приложение 4);

Инструкцию по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗ0 школы (Приложение 5);

Инструкцию по порядку учета и хранения съемных носителей конфиденциальной информации (персональных данных) школы (Приложение 6);

Инструкцию пользователя информационных систем персональных данных по обеспечению безопасности персональных данных школы (Приложение 7).

4. Настоящий приказ вступает в силу со дня его подписания, подлежит размещению на официальном сайте МОУ «ССОШ» в сети Интернет.

Директор школы:  /Г.Н. Смирнова/

Приложение 1
к приказу от 15.03.2022 №

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных МОУ «ССОШ»

1. Общие положения

1. Настоящая Инструкция определяет обязанности, полномочия и ответственность ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных ШКОЛЫ (администратора безопасности ИСПДн).

2. Администратор безопасности ИСПДн (далее – Администратор ИСПДн) назначается приказом директора МОУ «ССОШ» .

3. Администратор ИСПДн подчиняется директору школы.

4. Администратор ИСПДн в своей работе руководствуется настоящей Инструкцией, документами, определяющими политику школы в отношении обработки персональных данных, утвержденными приказом № от в отношении обработки персональных данных» и другими утвержденными внутренними организационно-распорядительными документами в области обработки персональных данных.

5. Администратор ИСПДн отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты при обработке персональных данных.

2. Обязанности по обеспечению безопасности информации

6. Администратор ИСПДн обязан:

1) знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации;

2) обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

программного обеспечения автоматизированных рабочих мест (далее – АРМ) и серверов (операционные системы, прикладное и специальное ПО);

аппаратных средств;

аппаратных и программных средств защиты;

3) обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети;

4) осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов (если не назначен другой ответственный);

5) обеспечивать функционирование и поддерживать работоспособность средств защиты;

6) в случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

7) осуществлять регистрацию пользователей, выдачу временных паролей пользователей, осуществлять контроль за правильностью использования пароля пользователем ИСПДн;

8) обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации;

9) требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты;

10) обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт;

11) присутствовать при выполнении технического обслуживания элементов ИСПДн сторонними физическими лицами и компаниями;

12) принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Ответственность

7. В случае нарушения положений настоящей Инструкции Администратор ИСПДн несёт ответственность в соответствии с действующим законодательством.

Приложение 2
к приказу директора МОУ «ССОШ» от
15.03.2022 №

ИНСТРУКЦИЯ
о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в МОУ «ССОШ»

1. Назначение и область действия

1.1. Данная Инструкция определяет действия, связанные с мерами и средствами поддержания непрерывной работы и восстановления работоспособности информационных систем в МОУ «ССОШ» (далее – Школа).

1.2. Настоящая Инструкция регламентирует:

меры защиты от потери информации;

действия по восстановлению в случае потери информации.

1.3. Действие настоящей Инструкции распространяется на ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных Школы (далее – Администратор ИСПДн) при осуществлении резервного копирования информации.

2. Меры обеспечения надежной работы и восстановления ресурсов при возникновении инцидентов

2.1 Технические меры.

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства системы, используемые для предотвращения возникновения Инцидентов, такие как:

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

пожарные сигнализации и системы пожаротушения;

системы вентиляции и кондиционирования;

системы резервного питания.

Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для предотвращения потери информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от

необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

резервные линии электропитания в пределах комплекса зданий;

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на носитель (ленту, жесткий диск и т.п.).

2.2 Организационные меры:

1) резервное копирование и хранение данных должно осуществлять на периодической основе:

для обрабатываемых персональных данных – не реже раза в неделю или по требованию пользователя ИСПДн;

для системной информации – не реже раза в месяц;

эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн каждый раз при внесении изменений в эталонные копии (выход новых версий).

2) данные о проведении процедуры резервного копирования должны отражаться в специально созданном Журнале учета.

3) носители, на которые произведено резервное копирование, должны быть пронумерованы номером носителя, датой проведения резервного копирования.

4) носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

5) носители и резервные копии данных должны храниться не менее года для возможности восстановления данных.

3. Порядок проведения резервирования информации

3.1. Перед проведением процедуры резервного копирования необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

3.2. Резервирование информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

3.3. Все файлы, входящие в состав резервной копии, должны архивироваться в один архив с присвоением имени архива в формате время_дата (например, 18.00_21.11.2020).

3.4. Архивация может производиться как штатными средствами, поставляемыми в составе специализированного программного обеспечения для

построения информационной системы, так и сторонним программным обеспечением (например, 7zip, WinRar).

3.5. Резервные копии должны сохраняться на носители, не входящие в состав технических средств информационной системы персональных данных (внешние жесткие диски, CD/DVD диски, USB-флэш-накопитель).

3.6. После завершения процедуры резервного копирования информации и записи резервной копии на носитель необходимо поместить носитель с резервной копией в специально отведённое для хранения место и проставить соответствующую отметку в Журнале.

4. Порядок проведения восстановления информации

4.1. Перед проведением процедуры восстановления информации необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

4.2. Восстановление информации следует проводить из наиболее актуальной резервной копии.

4.3. В случае, если специализированное программное обеспечение для построения информационной системы не позволяет работать с заархивированными резервными копиями, то перед восстановлением информации необходимо разархивировать файлы резервной копии при помощи стороннего программного обеспечения (например, 7zip, WinRar).

4.4. Восстановление информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

4.5. После завершения процедуры восстановления необходимо убедиться в работоспособности информационной системы персональных данных.

4.6. В случае успешного восстановления оповестить пользователей информационной системы о возможности продолжения работы. В противном случае необходимо изучить документацию, прилагаемую к программному обеспечению либо обратиться в службу технической поддержки.

5. Ответственность

5.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение 3
к приказу директора МОУ «ССОШ» от
15.03.2022 №

ИНСТРУКЦИЯ
по организации антивирусной защиты в Администрации Лихославльского муниципального округа

1. Общие положения

1. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в МОУ «ССОШ» (далее - Школа) и предотвращения возникновения фактов заражения вредоносным программным обеспечением.

2. Данная Инструкция распространяется на всех пользователей и ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных Школы (далее – Администратор ИСПДн) в школе.

2. Установка и обновление антивирусных средств

3. Установка и настройка антивирусных средств осуществляются только Администратором ИСПДн.

4. Обновление антивирусных баз осуществляется по расписанию в автоматическом режиме, либо вручную при необходимости.

3. Требования к проведению мероприятий по антивирусной защите

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 (магнитных дисках, USB-флэш-накопителях, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие заражения вредоносным программным обеспечением.

7. Контроль информации на съёмных носителях производится непосредственно перед её использованием.

8. Особое внимание следует обратить на недопустимость использования съёмных носителей, принадлежащих лицам, временно допущенным к работе на ЭВМ. Работа этих лиц должна проводиться под непосредственным контролем сотрудника или Администратора ИСПДн.

9. Ежедневно, в начале работы, должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех загружаемых в память файлов персонального компьютера.

10. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

11. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

непосредственно после установки (изменения) программного обеспечения компьютера;

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.).

4. Действия сотрудников при обнаружении компьютерного вируса

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

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора ИСПДн;

провести лечение или уничтожение зараженных файлов.

13. При возникновении подозрения на наличие компьютерного вируса пользователь или Администратор ИСПДн должны провести внеочередной антивирусный контроль.

5. Ответственность при организации антивирусной защиты

14. Ответственность за организацию антивирусной защиты возлагается на Администратора ИСПДн.

15. Ответственность за выполнение требований данной Инструкции возлагается на пользователей и Администратор ИСПДн.

16. Периодический контроль за соблюдением положений данной Инструкции возлагается на Администратора ИСПДн.

Приложение 4
к приказу директора МОУ «ССОШ» от
15.03.2022 №

ИНСТРУКЦИЯ
по порядку учета и хранению документов, содержащих персональные данные, в МОУ «Станская средняя общеобразовательная школа»

1. Общие положения

1. Настоящая Инструкция разработана с целью обеспечения безопасности персональных данных при работе с документами, содержащими персональные данные.

2. Действие настоящей Инструкции распространяется на сотрудников МОУ «ССОШ» (далее – Школа), допущенных к обработке персональных данных.

2. Порядок учета, хранения и обращения с документами, которые содержат персональные данные

3. Все находящиеся на хранении и в обращении документы с персональными данными в Школе подлежат учёту.

4. Каждый документ, личное дело или журнал должны иметь уникальный учетный номер.

5. Учет и выдачу документов с персональными данными осуществляют сотрудники структурных подразделений, на которых возложены функции хранения документов, содержащих персональные данные. Факт выдачи документов фиксируется в журнале учета.

6. При работе с документами, которые содержат персональные данные необходимо:

соблюдать требования настоящей Инструкции;

использовать полученные документы исключительно для выполнения своих служебных обязанностей;

ставить в известность ответственного за обработку персональных данных о любых фактах нарушения требований настоящей Инструкции;

бережно относиться к документам, содержащим персональные данные;

обеспечивать физическую безопасность документов всеми разумными способами;

обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

извещать ответственного за организацию обработки персональных данных о фактах утраты (кражи) документов, содержащих персональные данные;

осуществлять вынос документов с персональными данными для непосредственной передачи адресату только с письменного разрешения директора МОУ «ССОШ»(далее – Директор);

при передаче персональных данных передаётся минимальный объем данных, который необходим для выполнения служебных обязанностей адресата;

в случае утраты или уничтожения документов, которые содержат персональные данные либо разглашении содержащихся в них сведений, немедленно ставится в известность главу муниципального округа. Отметки об утрате вносятся в журнал учета документов с персональными данными.

в случае увольнения или перевода работника в другое структурное подразделение, предоставленные документы, содержание персональные данные, изымаются.

3. Запрещается

7. Использовать документы с персональными данными в личных целях.

8. Передавать документы с персональными данными третьим лицам без соответствующего разрешения Директора.

9. Хранить документы с персональными данными вместе с документами с открытой информацией на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

10. Выносить документы с персональными данными из служебных помещений для работы с ними на дому.

11. Оставлять документы с персональными данными без присмотра.

12. Изготавливать и хранить копии паспортов или иных документов, удостоверяющих личность, за исключением случаев, предусмотренных законодательством.

4. Ответственность

14. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение 5
к приказу директора МОУ «ССОШ» от
15.03.2022 №

ИНСТРУКЦИЯ
по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в МОУ «Станская средняя общеобразовательная школа»

1. Общие положения

1. Настоящая Инструкция определяет порядок учета, хранения и использования средств криптографической защиты информации (СКЗИ) и криптографических ключей, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации в МОУ «ССОШ» (далее – Школа).

2. Пользователь должен выполнять все требования настоящей Инструкции, правила, изложенные в эксплуатационной документации на СКЗИ, а также другие документы, регламентирующие порядок работы с СКЗИ.

2. Обязанности Пользователя

3. Пользователь обязан соблюдать требования по обеспечению безопасности функционирования СКЗИ.

4. Пользователь обязан обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей.

5. Пользователь обязан сдать носители ключевой информации (далее - НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, ответственному за обработку персональных данных.

6. Пользователь обязан сдать носители ключевой информации (далее – НКИ) по окончании срока действия сертификата ключа, а также в случае компрометации ключа.

7. Пользователь обязан немедленно уведомлять ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных Администрации (далее – Администратор ИСПДн) о компрометации криптографических ключей.

8. Пользователь обязан немедленно уведомлять Администратора ИСПДн о фактах утраты или недостачи СКЗИ, НКИ.

3. Порядок обращения со средствами криптографической защиты информации

9. Монтаж и установка СКЗИ осуществляются только уполномоченным лицом, либо организацией, имеющей необходимые лицензии.

10. Все СКЗИ и НКИ должны учитываться в журнале.

11. Служебные помещения, в которых размещаются СКЗИ, должны оборудоваться охранной сигнализацией, по убытии сотрудников закрываться и сдаваться под охрану.

12. Для хранения носителей ключевой информации помещения обеспечиваются сейфами (металлическими шкафами).

13. Несанкционированное изготовление дубликатов ключей ЗАПРЕЩЕНО. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.

14. К эксплуатации СКЗИ допускаются лица, изучившие правила пользования данным СКЗИ.

15. Все программное обеспечение ПЭВМ, предназначенной для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую СКЗИ, не допускается.

4. Порядок обращения с ключами ЭЦП

16. Криптографический ключ применяется для подписания (проверки электронной цифровой подписи) электронных документов до окончания срока его действия или наступления события, трактуемого как компрометация криптографических ключей.

17. Изготовление и выдача ключей ЭЦП осуществляется только Удостоверяющим центром.

18. Выработанные закрытые (конфиденциальные) криптографические ключи хранятся исключительно в электронном виде на цифровых носителях информации, которые получают статус НКИ.

19. НКИ являются объектами особой важности, т.к. они содержат информацию, предназначенную для гарантированной идентификации владельца ключа, защиты электронного документа от подделки и обеспечения конфиденциальности документа.

20. Владельцы ключей несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту НКИ от несанкционированного использования.

21. Хранение носителей ключевой информации обеспечивается в сейфе.

5. Запрещается

22. Осуществлять несанкционированное и безучётное копирование ключевых данных.

23. Хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность.

24. Передавать НКИ третьим лицам.

25. Во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ).

26. Хранить на НКИ какую-либо информацию, кроме ключевой.

27. Использование выведенных из действия криптографических ключей.

6. Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

28. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

утрата (хищение) НКИ, в том числе – с последующим их обнаружением;

увольнение (переназначение) сотрудников, имевших доступ к ключевой информации;

передача закрытых (конфиденциальных) ключей по линии связи в открытом виде;

нарушение правил хранения криптографических ключей;

вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

отрицательный результат при проверке наложенной ЭЦП;

несанкционированное или безучётное копирование ключевой информации;

все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

29. При наступлении любого из перечисленных выше событий Владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) в Удостоверяющий центр, производивший генерацию ключей ЭЦП.

30. При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей.

31. Для восстановления конфиденциальной связи после компрометации действующих ключей Пользователь получает в Удостоверяющем центре новые ключи ЭЦП.

7. Ответственность Пользователя

32. Владелец ключа несет персональную ответственность за конфиденциальность личных ключевых носителей.

33. В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Пользователь несёт ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 6
К приказу директора МОУ «ССОШ» от 15.03.2022 №

ИНСТРУКЦИЯ
по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в МОУ «Станская средняя общеобразовательная школа»

1. Общие положения

1. Настоящая Инструкция разработана с целью обеспечения безопасности персональных данных при их хранении на съемных носителях.

2. Действие настоящей Инструкции распространяется на сотрудников МОУ «ССОШ» (далее - Школа), допущенных к обработке персональных данных.

2. Основные термины, сокращения и определения

Администратор информационной системы персональных данных – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.

АРМ – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.

ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

ИС – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

Носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации.

ПК – персональный компьютер.

ПО – программное обеспечение вычислительной техники.

ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

Пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработке персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

3. Порядок использования носителей информации

3. Под использованием носителей информации в ИС понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

4. В ИС допускается использование только учтенных носителей информации, которые являются собственностью Администрации и подвергаются регулярной ревизии и контролю.

5. Носители конфиденциальной информации предоставляются сотрудникам Школы на основании письменного разрешения директора МОУ «Станская средняя общеобразовательная школа» при:

необходимости выполнения вновь принятым работником своих должностных обязанностей;

возникновения у сотрудника Школы производственной необходимости.

4. Порядок учета, хранения и обращения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации

6. Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) в школе подлежат учёту.

7. Каждый съемный носитель с записанной на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

8. Учет и выдачу съемных носителей конфиденциальной информации (персональных данных) осуществляет ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных Школы (далее - Администратор ИСПДн). Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

5. Использование сотрудниками носителей конфиденциальной информации

9. При использовании сотрудниками носителей конфиденциальной информации необходимо:

соблюдать требования настоящей Инструкции;

использовать носители информации исключительно для выполнения своих служебных обязанностей;

ставить в известность Администратора ИСПДн о любых фактах нарушения требований настоящей Инструкции;

бережно относится к носителям конфиденциальной информации (персональных данных);

обеспечивать физическую безопасность носителей информации всеми разумными способами;

извещать Администратора ИСПДн о фактах утраты (кражи) носителей конфиденциальной информации;

перед работой проверять носители конфиденциальной информации на наличие вредоносного ПО;

осуществлять вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату только с письменного разрешения руководителя;

при отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных носителях осуществляется в порядке, установленном для документов данного типа;

в случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность директора МОУ «ССОШ». На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных);

съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт;

в случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются.

6. Запрещается

10. Использовать носители конфиденциальной информации в личных целях.

11. Передавать носители конфиденциальной информации другим лицам (за исключением администраторов ИС).

12. Хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

13. Выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому.

7. Ответственность

14. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение 7
к приказу директора МОУ «ССОШ» от
15.03.2022 №

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в МОУ «Станская средняя общеобразовательная школа»

1. Общие положения

1. Пользователь информационной системы персональных данных (далее – Пользователь) осуществляет обработку персональных данных в информационных системах персональных данных в МОУ «ССОШ» (далее – Школа).

2. Пользователем является каждый работник Школы, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

3. Пользователь несет персональную ответственность за свои действия.

4. Пользователь в своей работе руководствуется настоящей Инструкцией, руководящими и нормативными документами Федеральной службы по техническому и экспортному контролю (ФСТЭК) России и другими внутренними нормативно - правовыми документами Школы по защите информации.

2. Обязанности пользователя

5. Пользователь обязан:

знать и выполнять требования настоящей Инструкции и других внутренних нормативно – правовых документов по защите персональных данных.

выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.

соблюдать требования парольной политики;

соблюдать правила при работе в сетях общего доступа и международного обмена – Интернет;

экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нём информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

6. Обо всех выявленных нарушениях, связанных с информационной безопасностью в школе, а также для получений консультаций по вопросам

информационной безопасности, необходимо обратиться к Администратору ИСПДн или ответственном за обработку персональных данных.

7. Для получения консультаций по вопросам работы и настройке элементов информационной системы персональных данных необходимо обращаться к Администратору ИСПДн.

8. Пользователям запрещается:

разглашать защищаемую информацию третьим лицам;

копировать защищаемую информацию на внешние носители без письменного разрешения директора МОУ «ССОШ»;

самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

несанкционированно открывать общий доступ к ресурсам;

запрещено подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства;

отключать (блокировать) средства защиты информации;

обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационной системе персональных данных;

сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системе персональных данных;

привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с Администратора ИСПДн.

9. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>

10. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных на него функций.

3. Организация парольной защиты

11. Личные пароли доступа к элементам информационной системы персональных данных создаются пользователем самостоятельно, за исключением временного пароля, который выдает Администратор ИСПДн.

12. Пользователь обязан сменить временный пароль, выданный Администратором ИСПДн при первом входе в систему.

13. Полная плановая смена паролей в информационной системе персональных данных проводится не реже одного раза в 3 месяца.

14. Правила формирования пароля:

пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

пароль должен состоять не менее чем из 8 символов.

в пароле должны присутствовать символы трех категорий из числа следующих четырех:

прописные буквы английского алфавита от A до Z;

строчные буквы английского алфавита от a до z;

десятичные цифры (от 0 до 9);

символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

запрещается выбирать пароли, которые уже использовались ранее.

15. Правила ввода пароля:

ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

16. Правила хранения пароля:

запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем;

17. Лица, использующие паролирование, обязаны:

четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

своевременно сообщать Администратору ИСПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

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

18. Работа в сетях общего доступа и международного обмена (сети Интернет) (далее – Сеть) на элементах информационной системы персональных данных должна проводиться при служебной необходимости.

19. При работе в Сети запрещается:

осуществлять работу при отключенных средствах защиты (антивирус и других);

передавать по Сети защищаемую информацию без использования средств шифрования;

запрещается скачивать из Сети программное обеспечение и исполняемые файлы (файлы с расширением exe, dll, msi);

запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие);

запрещается нецелевое использование подключения к Сети.

4. Ответственность

20. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.