МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ ОТДЕЛЬНЫХ ПРЕДМЕТОВ №104 г. ЧЕЛЯБИНСКА»
Ул. Братьев Кашириных, 103-б, тел. (351) 797-23-15, факс 8(351) 7 930-322, эл. почта: mou-104@mail.ru

ПРИКАЗ

№51 п 6 «13» мая 2020г.

Об утверждении инструкций по проведению работ по защите информации МАОУ «СОШ №104 г. Челябинска» основного здания и филиала

В целях выполнения требований Федеральных Законов от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 N 152-ФЗ «О персональных данных» приказываю.

1. Утвердить прилагаемые инструкции:

1) Инструкцию администратора информационной безопасности МАОУ «СОШ №104 г. Челябинска» основного здания и филиала;

2) Инструкцию администратора информационной системы персональных данных МАОУ «СОШ №104 г. Челябинска» основного здания филиала

3) Инструкцию оператора информационной системы персональных данных МАОУ «СОШ №104 г. Челябинска» основного здания филиала;

4) Инструкцию по организации антивирусной защиты на объектах вычислительной техники МАОУ «СОШ №104 г. Челябинска» основного здания филиала;

6) Инструкцию по реагированию на инциденты информационной безопасности в информационных системах персональных данных МАОУ «СОШ №104 г. Челябинска» основного здания филиала;

7) Инструкцию о порядке обеспечения конфиденциальности при обработке персональных данных в МАОУ «СОШ №104 г. Челябинска» основного здания филиала;

2. Руководителю информатизации МАОУ «СОШ №104 г. Челябинска» Фадюшину О.С. обеспечить выполнение работ в соответствии с инструкциями, утвержденными пунктом 1 настоящего приказа.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МАОУ "СОШ №104 г. Челябинска" Петрова О.В.

13 мая 2020

ИНСТРУКЦИЯ

Администратора информационной безопасности в МАОУ «СОШ №104 г. Челябинска» основного здания и филиала.

УТВЕРЖДЕНА
приказом директора МАОУ «СОШ №104 г. Челябинска»

1. Определения

Информационная технология-процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Несанкционированный доступ (НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Пользователь - лицо, которое использует действующую информационную систему для выполнения конкретной функции.

Средство защиты информации (СЗИ) - техническое, программное, программно-техническое средство, вещество и/или материал, предназначенные или используемые для защиты информации.

2. Общие положения

Настоящая Инструкция определяет общие функции, обязанности, права и ответственность Администратора информационной безопасности МАОУ «СОШ №104 г. Челябинска» филиал по вопросам организации системы менеджмента информационной безопасности.

Администратор информационной безопасности назначается из числа МАОУ «СОШ №104 г. Челябинска» филиал и обеспечивает правильное функционирование
ИСПДн.

Администратор информационной безопасности несет ответственность за обеспечение безопасности персональных данных при их обработке в МАОУ «СОШ №104 г. Челябинска» .

Администратор информационной безопасности в своей работе руководствуется настоящей Инструкцией, законодательством Российской Федерации, руководящими и нормативными документами ФСТЭК России, ФСБ России и локальными правовыми актами МАОУ «СОШ №104 г. Челябинска» .

Настоящая Инструкция разработана на основании действующих нормативных документов МАОУ «СОШ №104 г. Челябинска» по защите персональных данных.

3. Должностные обязанности Администратора информационной безопасности

Администратор информационной безопасности обязан:
- Знать, выполнять требования действующих нормативных, правовых актов Российской Федерации и локальных актов МАОУ «СОШ №104 г. Челябинска» в области защиты персональных данных;
- Проводить анализ и мониторинг инцидентов нарушения ИСПДн;
- Обеспечивать учет включения требований ИСПДн во все проекты, связанные с обработкой и использованием персональных данных;
- Оценивать адекватность и координировать внедрение конкретных мероприятий ИСПДн для новых систем или услуг;
- Проводить работу по выявлению возможных каналов утечки персональных данных, вести их учёт и принимать меры к их устранению;
- Определять и подтверждать необходимость и достаточность принимаемых мер по защите персональных данных;
- Разрабатывать программу повышения осведомленности работников в области информационной безопасности;
- Совместно с Администратором информационной системы персональных данных:
Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках, возложенных на него функций;
В случае отказа работоспособности технических средств и программного обеспечения информационной системы персональных данных (далее - ИСПДн), в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;
Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий;
Проводить периодический контроль принятых мер по защите в пределах, возложенных на него функций;
Осуществлять выдачу временных или основных паролей пользователей;
Осуществлять контроль за правильностью использования основного пароля операторами ИСПДн;
Проводить полную плановую смену паролей доступа не реже одного раза в год;
Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации;
Осуществлять работу с учетными записями пользователей ИСПДн (блокировка, удаление, регистрация новых пользователей). Производить их правильную настройку и разграничение прав доступа пользователей к ИСПДн в соответствии с разрешительной системой доступа;
Разрабатывать разрешительную систему доступа в помещения, к ресурсам ИСПДн МАОУ «СОШ №104 г. Челябинска» ;
Осуществлять своевременную корректировку разрешительной системы доступа (изменение списка пользователей ресурсами ИСПДн, изменение прав доступа пользователей к ресурсам ИСПДн). Корректировка разрешительной системы доступа осуществляется на основании служебной записки (заявки) пользователя, согласованной с лицом, ответственным за эксплуатацию ресурсов ИСПДн и утвержденной приказомМАОУ «СОШ №104 г. Челябинска» ;

Обеспечивать сетевую безопасность (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия;
Осуществлять антивирусную защиту ресурсов ИСПДн;
Вести электронный журнал сообщений в электронных системах;
Производить действия по внесению изменений в базовую конфигурацию информационных систем и систем защиты информации МАОУ «СОШ №104 г. Челябинска» ;
Выявлять инциденты информационной безопасности и реагировать на них.
- Осуществлять контроль за выполнением требований действующих нормативных, правовых и руководящих документов по защите персональных данных;
- Осуществлять контроль доступа к работе с ресурсами ИСПДн в соответствии с разрешительной системой доступа;
- Осуществлять периодический контроль за соблюдением пользователями Инструкции по организации парольной защиты;
- Осуществлять периодический контроль за соблюдением пользователями Инструкции по организации антивирусной защиты;
- Осуществлять контроль и/или программирование выданных пользователям электронных ключей СЗИ от НСД к информации (при их наличии);
- Осуществлять контроль за ведением журналов учета носителей персональных данных в структурных подразделениях, осуществляющих обработку;
- Осуществлять контроль действий пользователей по гарантированному уничтожению информации на внешних носителях информации;
- Осуществлять контроль за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусе ПЭВМ, технических средств и других устройств;
- Осуществлять контроль за вскрытием и ремонтом (модернизацией) ПЭВМ, недопущением доступа посторонних лиц к персональным данным во время вскрытия, ремонта, модернизации ПЭВМ, технических средств и других устройств, последующим их опечатыванием, составлением соответствующих актов;
- Осуществлять контроль за сроком действия сертификатов соответствия безопасности информации ФСТЭК России, ФСБ России на СЗИ, установленных в МАОУ «СОШ №104 г. Челябинска» ;
- Заблокировать учетные записи пользователей на ПЭВМ в случае окончания срока действия сертификата соответствия безопасности информации ФСТЭК России, ФСБ России на любое СЗИ, из установленных в МАОУ «СОШ №104 г. Челябинска» , до момента его продления. В случае не продления сертификата соответствия безопасности информации ФСТЭК России, ФСБ России на СЗИ он обязан поставить в известность орган по аттестации, проводивший аттестацию Объекта, для принятия совместного решения;
- Требовать прекращения обработки информации, как в целом, так и от отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.
4. Права Администратора информационной безопасности
Администратор информационной безопасности имеет право:

- Требовать от работников МАОУ «СОШ №104 г. Челябинска» соблюдения установленных правил СМИБ и исполнения локальных актов МАОУ «СОШ №104 г. Челябинска» в области защиты информации;
- Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и расследованиях фактов (попыток) несанкционированного доступа к информации;
- Участвовать в управляющем совете или иной действующей комиссии по вопросам информационной безопасности МАОУ «СОШ №104 г. Челябинска» ;
- Участвовать в утверждении и пересмотре политики информационной безопасности МАОУ «СОШ №104 г. Челябинска» и соответствующих обязанностей по ее выполнению;
- Участвовать в утверждении основных проектов в области информационной безопасности МАОУ «СОШ №104 г. Челябинска» ;
- Участвовать в комитете или иной действующей комиссии по координации вопросов информационной безопасности МАОУ «СОШ №104 г. Челябинска» ;
- Контролировать мероприятия связанные с выбором, приобретением и внедрением СЗИ;
- Участвовать, давать комментарии по реализации мероприятий по физической защите Объектов информатизации МАОУ «СОШ №104 г. Челябинска» .

5. Ответственность Администратора информационной безопасности

Администратор информационной безопасности несет ответственность:
- За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией - в пределах, определенных действующим трудовым законодательством Российской Федерации;
- За правонарушения, совершенные в процессе осуществления своей деятельности - в пределах, определенных действующим административным, гражданским и уголовным законодательством Российской Федерации;
- За причинение материального ущерба - в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

Администратора

информационной системы персональных данных в МАОУ «СОШ №104 г. Челябинска» основного здания и филиала

УТВЕРЖДЕНА
приказом директора МАОУ «СОШ №104 г. Челябинска»

1. Определения

Информационная технология -процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Программное обеспечение (ПО)-совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

Пользователь - лицо, которое использует действующую информационную систему для выполнения конкретной функции.

2. Общие положения

Настоящая Инструкция определяет обязанности, права и ответственность Администратора информационной системы персональных данных (далее - Администратор ИСПДн) по вопросам установки, настройки, обновления, удаления информационных систем персональных данных (далее - ИСПДн).

Администратор ИСПДн назначается из числа работников приказом директора МАОУ «СОШ №104 г. Челябинска» и обеспечивает правильное функционирование ИСПДн.

Администратор ИСПДн подчиняется Администратору информационной безопасности МАОУ «СОШ №104 г. Челябинска» в части защиты персональных данных.

Администратор ИСПДн в своей работе руководствуется настоящей Инструкцией, законодательством Российской Федерации, руководящими и нормативными документами ФСТЭК России, ФСБ России и локальными правовыми актами по вопросам защиты персональных данныхМАОУ «СОШ №104 г. Челябинска» .

Настоящая Инструкция разработана на основании действующего законодательства Российской Федерации и локальных нормативных актов МАОУ «СОШ №104 г. Челябинска» .

3. Должностные обязанности Администратора ИСПДн

Администратор ИСПДн обязан:

- Знать и выполнять требования действующих нормативных и руководящих документов Российской Федерации, а также локальных правовых актов МАОУ «СОШ №104 г. Челябинска» , в области защиты персональных данных;
- Ознакомить всех пользователей ИСПДн с Инструкцией Оператора ИСПДн и другими локальными правовыми актами МАОУ «СОШ №104 г. Челябинска» ;
- Устанавливать на серверы и ПЭВМ операционные системы и необходимое для работы программное обеспечение;
- Осуществлять конфигурацию программного обеспечения на серверах и ПЭВМ;

- Поддерживать в работоспособном состоянии программное обеспечение серверов, ПЭВМ и технические средства ИСПДн;
- Осуществлять техническую и программную поддержку пользователей, консультировать пользователей по вопросам работы с ресурсами ИСПДн и другим программным обеспечением;
- Доводить до пользователей требования Инструкций по работе с программным обеспечением;
- Обеспечивать своевременное архивирование и резервирование данных;
- Совместно с Администратором информационной безопасности:
Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках, возложенных на него функций;
В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;
Принимать меры по ликвидации последствийвнештатных и аварийных ситуаций;
Проводить периодический контроль мер, принятых для защиты персональных данных, в пределах, возложенных на него обязанностей;
Осуществлять выдачу временных или основных паролей пользователей;
Осуществлять контроль за правильностью использования основного пароля Операторами ИСПДн;
Проводить полную плановую смену паролей доступа не реже одного раза в год;
Обеспечивать постоянный контроль за выполнением Операторами ИСПДн правил, установленныхдля обеспечения безопасности персональных данных;
Осуществлять работу с учетными записями пользователей ИСПДн (блокировка, удаление, регистрация новых пользователей). Производить их правильную настройку и разграничение прав доступа пользователей к ИСПДн в соответствии с разрешительной системой доступа;
Разрабатывать разрешительную систему доступа в помещения, к ресурсам ИСПДн МАОУ «СОШ №104 г. Челябинска» ;
Осуществлять своевременную корректировку разрешительной системы доступа (изменение списка пользователей ресурсами ИСПДн, изменение прав доступа пользователей к ресурсам ИСПДн). Корректировка разрешительной системы доступа осуществляется на основании служебной записки (заявки) пользователя, согласованной с лицом, ответственным за эксплуатацию ресурсов ИСПДн;
Обеспечивать сетевую безопасность (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия;
Осуществлять антивирусную защиту ресурсов ИСПДн;
Вести электронный журнал сообщений в электронных системах;
Производить действия по внесению изменений в базовую конфигурацию информационных систем и систем защиты информации МАОУ «СОШ №104 г. Челябинска» ;
Выявлять инциденты информационной безопасности и реагировать на них.
- Информировать ответственного за организацию обработки персональных данных и Администратора информационной безопасности о фактах нарушения установленного

порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн;
- Требовать прекращения обработки информации, как в целом, так и от отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты;
- Обеспечивать строгое выполнение требований по обеспечению безопасности персональных данных при организации обслуживания технических средств и отправке их в ремонт;
- Присутствовать при выполнении технического обслуживания ресурсов ИСПДн, средств защиты информации и других технических средств сторонними специалистами.

4. Права Администратора ИСПДн

Администратор ИСПДн имеет право:
- Требовать от работников МАОУ «СОШ №104 г. Челябинска» соблюдения установленных правил и исполнения локальных актов и Инструкций МАОУ «СОШ №104 г. Челябинска» ;
- Участвовать в анализе ситуаций, касающихся функционирования ресурсов ИСПДн, ПЭВМ и других технических средств;
- Участвовать в утверждении и пересмотре политики информационной безопасности МАОУ «СОШ №104 г. Челябинска» и соответствующих обязанностей по ее выполнению;
- Готовить предложения по модернизации и приобретению сетевого оборудования, ПЭВМ и других технических средств;
- Готовить предложения по обновлению и приобретению программного обеспечения;
- Контролировать мероприятия связанные с выбором, приобретением, и внедрением серверов, ПЭВМ и других технических средств, а также программного обеспечения.

Ответственность Администратора ИСПДн

Администратор ИСПДн несет ответственность:
- За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией - в пределах, определенных действующим трудовым законодательством Российской Федерации;
- За правонарушения, совершенные в процессе осуществления своей деятельности - в пределах, определенных действующим административным, гражданским и уголовным законодательством Российской Федерации;
- За причинение материального ущерба - в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

ИНСТРУКЦИЯ

Оператора информационной системы персональных данных в приказом директора МАОУ «СОШ №104 г. Челябинска»

УТВЕРЖДЕНА
приказом директора МАОУ «СОШ №104 г. Челябинска»

1. Определения

Информационная технология - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2. Общие положения

Оператор информационной системы персональных данных (далее - Оператор ИСПДн) осуществляет обработку персональных данных в информационной системе персональных данных.

Оператором является каждый работник МАОУ «СОШ №104 г. Челябинска», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

Оператор несет персональную ответственность за свои действия.

Оператор в своей работе руководствуется настоящей Инструкцией, Концепцией и Политикой безопасности персональных данных, обрабатываемых в информационных системах персональных данных, руководящими и нормативными документами ФСТЭК России, ФСБ России и регламентирующими документами МАОУ «СОШ №104 г. Челябинска» .

Методическое руководство работой операторов в структурных подразделениях МАОУ «СОШ №104 г. Челябинска» осуществляется лицами, ответственными за обработку и обеспечение безопасности персональных данных при их обработке.

3. Должностные обязанности Оператора ИСПДн

Оператор ИСПДн обязан:

- 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;
- Выполнять только те действия, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным в МАОУ «СОШ №104 г. Челябинска»;
- Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и передаче носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов;
- Выполнять требования Инструкции по организации парольной защиты;
- Выполнять требования Инструкции по организации антивирусной защиты;

- Соблюдать правила при работе в сетях общего доступа и (или) международного обмена - Интернет и других;
- Докладывать Администратору информационной безопасности обо всех выявленных нарушениях, связанных с безопасностью персональных данных МАОУ «СОШ №104 г. Челябинска». По всем вопросам информационной безопасности необходимо обращаться к Администратору информационной безопасности;
- Для получения консультаций по вопросам работы информационной системы персональных данных (далее - ИСПДн) и настройке ее элементов необходимо обращаться к Администратору информационной системы персональных данных (далее - Администратор ИСПДн);
- При отсутствии визуального контроля за рабочей станцией блокировать доступ к рабочей станции;
- Во время работы располагать экран монитора в помещении так, чтобы исключить возможность просмотра информации посторонними лицами. С целью исключения просмотра информации с монитора необходимо завешивать шторы на оконных проемах (закрывать жалюзи);
- Прекратить обработку данных и доложить ситуацию Администратору ИСПДн в случае возникновения внештатных и аварийных ситуаций.

Оператору запрещается:
- Разглашать защищаемую информацию третьим лицам;
- Копировать защищаемую информацию на внешние носители без разрешения руководителя структурного подразделения;
- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- Без разрешения администратора ИСПДн открывать общий доступ к защищаемой информации на своей рабочей станции;
- Подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- Отключать (блокировать) средства защиты информации;
- Обрабатывать на рабочей станции не служебную информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- Привлекать посторонних лиц для производства ремонта или настройки рабочей станции, без согласования с Администратором информационной безопасности.

4. Ответственность Оператора ИСПДн

Оператор ИСПДн несет ответственность:
- За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией - в пределах, определенных действующим трудовым законодательством Российской Федерации;
- За правонарушения, совершенные в процессе осуществления своей деятельности - в пределах, определенных действующим административным, гражданским и уголовным законодательством Российской Федерации;
- За причинение материального ущерба - в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

ИНСТРУКЦИЯ

по организации антивирусной защиты на объектах вычислительной техники в МАОУ «СОШ №104 г. Челябинска»

УТВЕРЖДЕНА
приказом директора МАОУ «СОШ №104 г. Челябинска»

1. Определения

Антивирусное программное обеспечение - набор программ для обнаружения компьютерных вирусов и других вредоносных программ и лечения инфицированных файлов, а также для профилактики, т.е. предотвращения заражения файлов или операционной системы вредоносным кодом. **Антивирусные базы** - файлы, используемые антивирусным программным обеспечением при поиске вредоносных программ, периодически обновляемые разработчиком антивирусного программного обеспечения.

Антивирусный контроль - проверка информации (файла, сообщения и т.п.) на предмет наличия вредоносных программ.

Антивирусный мониторинг-часть антивирусного программного обеспечения, предназначенная для непрерывного контроля ситуаций, при которых может произойти заражение вредоносной программой.

Вредоносная программа - компьютерная программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информационные ресурсы.

Защищаемый компьютер - электронно-вычислительная машина (персональный компьютер или сервер), используемая для обработки данных.

Информационная технология - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Компьютерный вирус - разновидность вредоносных программ, отличительной особенностью которых является способность к размножению.

Локальная вычислительная сеть (ЛВС)- система объектов вычислительной техники, содержащих информационные ресурсы, созданная в целях обеспечения учебной, научной, хозяйственной и других видов деятельности.

Объект вычислительной техники (ОВТ)- стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации.

Пользователь - лицо, которое использует действующую систему для выполнения конкретной функции.

Программное обеспечение (ПО) - совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

Съемный носитель информации - носитель информации, предназначенный для ее автономного хранения и независимого от места записи использования (съемные винчестеры, карты флэш-памяти, CD, DVD, дискеты и др.).

2. Общие положения

Настоящая Инструкция определяет требования к организации защиты объектов вычислительной техники приказом директора МАОУ «СОШ №104 г. Челябинска»
от разрушающего воздействия вредоносных программ и устанавливает ответственность руководителей и работников структурных подразделений, эксплуатирующих и сопровождающих ОВТ (пользователей), за невыполнение требований настоящей Инструкции.

Требования настоящей Инструкции обязательны для выполнения всеми пользователями ресурсами ЛВС, информационными ресурсами приказом директора МАОУ «СОШ №104 г. Челябинска» и ресурсами информационной системы персональных данных (далее - ИСПДн).

Используемые в приказом директора МАОУ «СОШ №104 г. Челябинска» антивирусные средства должны быть лицензионными, централизованно закупленными у разработчиков (поставщиков) указанных средств. Допускается использование бесплатных антивирусных средств при условии соблюдения лицензионного соглашения разработчиков. Установка средств антивирусного контроля осуществляется Администратором информационной системы персональных данных (далее - Администратор ИСПДн) совместно с Администратором информационной безопасности в соответствии с Инструкциями по использованию программного обеспечения. Настройка параметров средств антивирусного контроля (политик) осуществляется Администратором ИСПДн совместно с Администратором информационной безопасностис помощью сервера централизованного управления в соответствии с руководствами по применению конкретных антивирусных средств.

3. Порядок обновления антивирусных баз

Обновление антивирусных баз на ресурсах ЛВС, информационных ресурсах и ИСПДн, должно происходить в автоматическом режиме при загрузке ОВТ. Допускается работа средств антивирусного контроля с обновлениями не старше 72 часов. Актуализация антивирусных баз на защищаемых компьютерах, подключенных к ЛВС, контролируется пользователем самостоятельно ежедневно и в случае выявления нарушений пользователь должен сообщить о данном факте руководителю своего структурного подразделения иАдминистратору ИСПДн.

4. Применение средств антивирусного контроля

Антивирусный контроль всех дисков и файлов ОВТ должен проводиться еженедельно (для серверов - при перезапуске, но не реже одного раза в месяц) в автоматическом режиме.

Проверка критических областей защищаемых ОВТ, заражение которых вредоносными программами может привести к серьезным последствиям, должна проводиться автоматически при каждом запуске ОВТ.

Внеочередной антивирусный контроль всех дисков и файлов ОВТ должен выполняться:

- непосредственно после установки (изменения) программного обеспечения на ОВТ;

- после подключения автономного компьютера к ресурсам ЛВС;
- при возникновении подозрения на наличие вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

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.

На каждом ОВТ в резидентном режиме должен быть запущен антивирусный монитор.

Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема.

Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании Инструкций по установке конкретного ПО. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вредоносной программы. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения регистрируется в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение, и/или автоматизированными средствами информационных систем.

Пользователям запрещается отключать средства антивирусного контроля и самостоятельно вносить изменения в настройки антивирусного программного обеспечения.

5. Действия при обнаружении вредоносных программ

При возникновении подозрения на наличие вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно должен провести внеочередной антивирусный контроль ОВТ, при необходимости привлечь Администратора ИСПДн для определения ими факта наличия или отсутствия вредоносной программы.

В случае обнаружения при проведении антивирусной проверки зараженных вредоносными программами файлов пользователи обязаны:
- приостановить все операции, связанные с обработкой файлов на защищаемом компьютере; - немедленно поставить в известность о факте обнаружения зараженных вредоносными программами файлов руководителя своего структурного подразделения и/или Администратора ИСПДн;
- совместно с Администратором ИСПДн провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов, при необходимости привлечь Администратора ИСПДн.

6. Обязанности и ответственность

Администратор ИСПДн несет ответственность за:

- нарушение организации проведения антивирусного контроля на серверах;
- нарушение работоспособности централизованного средства управления и мониторинга (сервер администрирования);
- своевременное обновление антивирусных баз и получение новых лицензионных ключей при истечении их срока действия.

Администратор информационной безопасности несет ответственность за:

- формирование политик антивирусного контроля;
- осуществление контроля за соблюдением пользователями настоящей Инструкции.

Администратор информационной безопасности, Администратор ИСПДн несут ответственность за нарушение:

- организации проведения мероприятий антивирусного контроля в подразделениях;
- установленного порядка антивирусного контроля;
- установленного порядка периодического контроля за состоянием антивирусной защиты.

Руководитель структурного подразделения несет ответственность за:

- проведение мероприятий антивирусного контроля в подразделениях;
- своевременное ознакомление пользователей с настоящей Инструкцией.

Ответственность за соблюдение требований настоящей Инструкции возлагается на всех пользователей.

ИНСТРУКЦИЯ
по реагированию на инциденты информационной безопасности в информационных системах персональных данных в приказом директора МАОУ «СОШ №104 г. Челябинска»

УТВЕРЖДЕНА
приказом директора МАОУ «СОШ №104 г. Челябинска»

1. Общие положения

Настоящая Инструкция устанавливает перечень практических рекомендаций по реагированию на возникшие инциденты информационной безопасности в информационных системах персональных данных МАОУ «СОШ №104 г. Челябинска» Настоящая Инструкция разработана на основаниипостановления Правительства Российской Федерации от 1 ноября 2012 года N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», типовых требований ФСБ России от 21.02.2008 N 149/6/6-622 «По организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведения, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных».

Внутренний инцидент - инцидент, источником которого является нарушитель, связанный с пострадавшей стороной непосредственным образом (трудовым договором или иным способом). Среди системных событий такого типа можно выделить следующие наиболее распространенные:

- утечка персональных данных;
- неправомерный доступ к информации;
- удаление информации;
- компрометация информации;
- саботаж;
- мошенничество с помощью информационных технологий;
- аномальная сетевая активность;
- аномальное поведение программного обеспечения;
- использование активов МАОУ «СОШ №104 г. Челябинска» в личных целях или в мошеннических операциях.

Внешний инцидент - инцидент, источником которого является нарушитель, не связанный с пострадавшей стороной непосредственным образом. Среди системных событий такого типа можно выделить следующие наиболее распространенные:

- атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS);
- перехват и подмена трафика;
- неправомерное использование корпоративного бренда в сети Интернет;
- фишинг (вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям);
- размещение конфиденциальной/провокационной информации в сети Интернет;
- взлом, попытка взлома, сканирование портала МАОУ «СОШ №104 г. Челябинска» ;
- сканирование сети, попытка взлома сетевых узлов;
- вирусные атаки;

- неправомерный доступ к персональным данных;
- анонимные письма (письма с угрозами).

Действия компьютерных злоумышленников вступают в противоречие с действующим уголовным законодательством и посягают на охраняемые уголовным законом общественные отношения. При этом важно отметить, что только правоохранительные или судебные органы могут квалифицировать инцидент информационной безопасности в качестве преступления в сфере компьютерной информации. В главе 28 УК РФ закреплены квалифицирующие признаки компьютерных преступлений и прописаны соответствующие санкции: *«Глава 28. Преступления в сфере компьютерной информации*

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо арестом на срок до шести месяцев, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения,

- наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.
2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.
3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.
Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, - наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.
2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, - наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.»

2. Общий алгоритм действий работников МАОУ «СОШ №104 г. Челябинска» в случае наступления инцидента информационной безопасности в информационных системах персональных данных

Реагирование на инцидент информационной безопасности включает в себя технические мероприятия, обеспечивающие целостность криминалистически значимых данных и возможность судебного исследования этих данных в будущем, а также организационные мероприятия, которые позволяют снизить ущерб от инцидента и составить необходимые

для правоохранительных органов документы. Сущностью технических мероприятий является немедленное обеспечение целостности данных, потенциально имеющих отношение к инциденту, путем отключения, упаковки и опечатывания, а затем и должного хранения соответствующих носителей информации. Отключение носителей информации позволяет свести к нулю риск уничтожения криминалистически значимых данных в результате работы вредоносных программ и действий злоумышленника, а их упаковка, опечатывание и должное хранение обеспечивают достаточный уровень оцениваемой достоверности результатов криминалистического исследования в суде.
Организационные мероприятия заключаются в уведомлении руководства МАОУ «СОШ №104 г. Челябинска» и иных заинтересованных организаций о факте инцидента. Документы, составленные при проведении организационных мероприятий, могут использоваться как основания для рассмотрения вопросов о возбуждении уголовных дел или для уточнения вопросов, выносимых на разрешение при назначении судебных экспертиз носителей информации.
После реагирования на инцидент информационной безопасности начинается расследование инцидента и восстановление информационной системы МАОУ «СОШ №104 г. Челябинска»МАОУ «СОШ №104 г. Челябинска» филиал. Восстановление информационной системы МАОУ «СОШ №104 г. Челябинска» заключается в замене изъятых, упакованных и опечатанных носителей информации на новые, установке требуемого ПО и конфигурации информационной системы с учетом повышенных требований информационной безопасности.
Типовой сценарий при нарушениях информационной безопасности может быть основан на приведенных ниже базовых действиях:
- Идентифицировать инцидент и убедиться, что он действительно имеет место быть.
- Локализовать объекты информатизации, задействованные в инциденте.
- Ограничить доступ к объектам информатизации, задействованным в инциденте.
- Оперативно поставить в известность Администратора информационной безопасности, руководителя подразделения о факте инцидента.
- Оформить служебную записку на имя директора МАОУ «СОШ №104 г. Челябинска», информировать о факте инцидента и описать произошедшее.
- Привлечь компетентных специалистов для консультации.
- Создать группу по расследованию инцидента и составить план работ по сбору доказательств и восстановлению систем. Протоколировать все действия, которые осуществляются в ходе реагирования на инцидент.
- Обеспечить сохранность и должное оформление доказательств:
Снять энергозависимую информацию с работающей системы;
Собрать информацию о протекающем в реальном времени инциденте;
Отключить от сети питание.
- В присутствии третьей независимой стороны произвести изъятие и опечатывание носителей информации с доказательной базой, а также снятие образов и другой информации для последующего анализа и сохранения:
Оформить протоколом все операции с носителями информации;
Провести детальную опись объектов с информацией, извлекаемых данных, а также мест их сохранения;
Задокументировать процесс на фото/видеокамеру;

Сохранить опечатанные объекты вместе с протоколом в надежном месте до передачи носителей на исследование или в правоохранительные органы.

- После сохранения и оформления вещественных доказательств восстановить работоспособность информационных систем.
- При проведении исследования источников информации обеспечить неизменность доказательств. Работать только с копией.
- При проведении расследования обеспечить корректное взаимодействие с заинтересованными подразделениями органов правопорядка, безопасности и внешними организациями (компаниями, предоставляющие услуги в области расследования инцидентов информационной безопасности и обеспечения информационной безопасности).
- По завершении расследования оформить соответствующий отчет и составить рекомендации по снижению рисков возникновения подобных инцидентов в будущем.
- При обращении в правоохранительные органы представить им подробное описание инцидента, описание собранных доказательств и результаты их анализа.
- Учет инцидентов информационной безопасности регистрируется в Журнале учета инцидентов информационной безопасности.

3. Инструкция для работников МАОУ «СОШ №104 г. Челябинска» в случае возникновения инцидентов информационной безопасности в информационных системах персональных данных

- Оперативно связаться с Администратором информационной безопасности и сообщить о факте инцидента.
- В зависимости от степени инцидента выключить рабочую станцию (сервер), на которой осуществлялась обработка, либо не выполнять никаких действий, если выключение рабочей станции (сервера) может привести к потере данных.
- Ограничить доступ к рабочей станции (серверу) со стороны персонала.
- Составить служебную записку на имя директора МАОУ «СОШ №104 г. Челябинска» , информировать о факте инцидента и описать произошедшее.

ИНСТРУКЦИЯ

о порядке обеспечения конфиденциальности при обработке персональных данных в МАОУ «СОШ №104 г. Челябинска» основного здания и филиала

УТВЕРЖДЕНА
Директором МАОУ «СОШ №104 г. Челябинска»

1. Общие положения

Настоящая Инструкция устанавливает применяемые способы обеспечения безопасности персональных данных в МАОУ «СОШ №104 г. Челябинска» при их обработке, включая: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, с целью соблюдения конфиденциальности сведений, содержащих персональные данные работников, обучающихся, участников единого государственного экзамена (за исключением обучающихся), граждан, привлекаемых к проведению государственной итоговой аттестации, членов предметных комиссий, общественных наблюдателей, слушателей и других лиц.

Настоящая Инструкция разработана на основании положений Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 19.12.2005 N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и иных нормативно-правовых актов Российской Федерации, а также Положения об обработке персональных данных в МАОУ «СОШ №104 г. Челябинска» филиал.

В соответствии с законодательством Российской Федерации под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Требование обеспечения конфиденциальности при обработке персональных данных означает обязательное для соблюдения должностными лицами МАОУ «СОШ №104 г. Челябинска» , допущенными к обработке персональных данных, иными получившими доступ к персональным данным лицами требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Обеспечение конфиденциальности персональных данных не требуется в случае:

- обезличивания персональных данных;
- общедоступных персональных данных.

Перечень обрабатываемых категорий персональных данных и перечень категорий субъектов персональных данных указан в Положении об обработке персональных данных в МАОУ «СОШ №104 г. Челябинска» филиал.

Лица, допущенные к обработке персональных данных в МАОУ «СОШ №104 г. Челябинска», указаны в Разрешительной системе допуска работников МАОУ «СОШ

№104 г. Челябинска», допущенных к обработке персональных данных работников, обучающихся, участников единого государственного экзамена (за исключением обучающихся), граждан, привлекаемых к проведению государственной итоговой аттестации, членов предметных комиссий, общественных наблюдателей, слушателей и других лиц с использованием средств автоматизации и без использования таких средств, утвержденной приказом директора МАОУ «СОШ №104 г. Челябинска». Обработка персональных данных лицами, не указанными в Разрешительной системе допуска работников МАОУ «СОШ №104 г. Челябинска» , допущенных к обработке персональных данных работников, обучающихся, участников единого государственного экзамена (за исключением обучающихся), граждан, привлекаемых к проведению государственной итоговой аттестации, членов предметных комиссий, общественных наблюдателей, слушателей и других лиц с использованием средств автоматизации и без использования таких средств, запрещается.

В целях обеспечения требований соблюдения конфиденциальности и безопасности при обработке персональных данных Учреждение предоставляет должностным лицам, работающим с персональными данными, необходимые условия для выполнения указанных требований: принимает необходимые правовые, организационные и технические меры в соответствии с действующим законодательством. Должностным лицам МАОУ «СОШ №104 г. Челябинска» , работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа файлы черновиков и вариантов документа переносятся подготовившим их работником на маркированные носители, предназначенные для хранения персональных данных.

Без согласования с Администратором информационной безопасности МАОУ «СОШ №104 г. Челябинска» формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

Должностные лица МАОУ «СОШ №104 г. Челябинска» , работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, связанных с выполнением своих трудовых обязанностей.

При прекращении выполнения трудовой функции, связанной с обработкой персональных данных, все носители информации, содержащие персональные данные (оригиналы и копии документов, машинные и бумажные носители и пр.), которые находились в распоряжении должностного лица в связи с выполнением должностных обязанностей, данный работник должен передать своему непосредственному руководителю.

Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством Российской Федерации, в соответствии с Положением об обработке персональных данных в МАОУ «СОШ №104 г. Челябинска» филиал, настоящей Инструкцией, должностными Инструкциями и иными локальными нормативно-правовыми актами МАОУ «СОШ №104 г. Челябинска».

Передача персональных данных осуществляется ответственным за обработку персональных данных должностным лицом МАОУ «СОШ №104 г. Челябинска» с обязательной регистрацией факта передачи в Журнале учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих

государственных органов при обработке персональных данных в МАОУ «СОШ №104 г. Челябинска».
Передача сведений и документов, содержащих персональные данные, оформляется путем составления акта по установленной настоящей Инструкцией форме (Приложение N 1).
Должностное лицо, предоставившее персональные данные третьим лицам, направляет письменное уведомление субъекту персональных данных о факте передачи его данных третьим лицам.
Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими в МАОУ «СОШ №104 г. Челябинска» локальными нормативно-правовыми актами.
Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках. Образец ответа на запрос о предоставлении персональных данных работника представлен в Приложении N 3.
Должностные лица МАОУ «СОШ №104 г. Челябинска» , работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю и (или) ответственному за организацию обработки персональных данных обо всех ставших им известными фактах получения третьими лицами несанкционированного доступа, либо попытки получения доступа к персональным данным, об утрате или недостаче носителей информации, содержащих персональные данные, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинах и условиях возможной утечки этих сведений.
Должностные лица, осуществляющие обработку персональных данных, за невыполнение требований конфиденциальности, защиты персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.
Отсутствие контроля со стороны МАОУ «СОШ №104 г. Челябинска» за надлежащим исполнением работником своих обязанностей в области обеспечения конфиденциальности и безопасности персональных данных не освобождает работника от таких обязанностей и предусмотренной законодательством Российской Федерации ответственности.
2. Порядок обеспечения безопасности при обработке персональных данных, осуществляемой без использования средств автоматизации
Обработка персональных данных, в том числе содержащихся в информационной системе персональных данных, либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такая обработка осуществляется при непосредственном участии человека.
Руководитель структурного подразделения, осуществляющего обработку персональных данных без использования средств автоматизации:
- определяет места хранения персональных данных (материальных носителей);
- осуществляет контроль наличия в структурном подразделении условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;

- информирует лиц, осуществляющих обработку персональных данных без использования средств автоматизации, о перечне обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;
- организует раздельное, т.е. не допускающее смешение, хранение материальных носителей персональных данных (документов, дисков, дискет, flash-накопителей, пр.), обработка которых осуществляется в различных целях.
При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных цели обработки, которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.
При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, руководитель структурного подразделения должен обеспечить раздельную обработку персональных данных, исключающую одновременное копирование иных персональных данных, не подлежащих распространению и использованию.
Работники структурных подразделений в работе должны использовать Журнал учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных в МАОУ «СОШ №104 г. Челябинска» .
Для ведения Журнала учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных в МАОУ «СОШ №104 г. Челябинска» назначается лицо(а), ответственное(ые) за ведение и хранение Журнала.
Ответственным(и) лицом(ами) за ведение и хранение Журнала учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных в МАОУ «СОШ №104 г. Челябинска» филиалявляется лицо(а), ответственное(ые) за обработку персональных данных, назначенные приказом МАОУ «СОШ №104 г. Челябинска» .
Журнал учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных должен быть пронумерован, прошнурован и скреплен подписью Администратора информационной безопасности.
Хранение Журнала учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных должно исключать несанкционированный доступ к нему.
Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, должно производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).
Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на

материальном носителе, а если это не допускается техническими особенностями материального носителя, путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Порядок обеспечения безопасности при обработке персональных данных, осуществляемой с использованием средств автоматизации

Обработка персональных данных с использованием средств автоматизации означает совершение действий (операций) с такими данными с помощью объектов вычислительной техники в локально-вычислительной сети МАОУ «СОШ №104 г. Челябинска» (далее- ЛВС).

Безопасность персональных данных при их обработке в ЛВС обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в ЛВС информационные технологии. Технические и программные средства защиты информации должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в ЛВС, в установленном порядке проходят процедуру оценки соответствия.

Допуск лиц к обработке персональных данных с использованием средств автоматизации осуществляется на основании Разрешительной системы допуска работников МАОУ «СОШ №104 г. Челябинска» , допущенных к обработке персональных данных работников, обучающихся и других лиц с использованием средств автоматизации и без использования таких средств, утвержденной приказом директора МАОУ «СОШ №104 г. Челябинска Положения об обработке персональных данных в МАОУ «СОШ №104 г. Челябинска» при наличии ключей (паролей) доступа.

Работа с персональными данными, содержащимися в ЛВС, осуществляется в соответствии с локальными нормативно-правовыми актами МАОУ «СОШ №104 г. Челябинска» в области персональных данных, с которыми работник, в должностные обязанности которого входит обработка персональных данных, знакомится под роспись и нормативно-правовыми актами Российской Федерации в области персональных данных.

Работа с персональными данными в ЛВС должна быть организована таким образом, чтобы обеспечивалась сохранность носителей персональных данных и средств защиты информации, а также исключалась возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, должны быть защищены в соответствии с требованиями Инструкции по организации парольной защиты на объектах вычислительной техники в МАОУ «СОШ №104 г. Челябинска» . Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

При обработке персональных данных в ЛВС пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

- недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

При обработке персональных данных в ЛВС должны быть выполнены следующие условия:
- обучение лиц, использующих средства защиты информации, применяемые в ЛВС, правилам работы с ними;
- учет лиц, допущенных к работе с персональными данными в ЛВС,учет паролей доступа;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

Специфические требования по защите персональных данных в отдельных информационных системах персональных данных МАОУ «СОШ №104 г. Челябинска» определяются утвержденными в установленном порядке Инструкциями по их использованию и эксплуатации.

4. Порядок учета, хранения, обращения и утилизации съемных носителей персональных данных

Все находящиеся на хранении и в обращении в МАОУ «СОШ №104 г. Челябинска» съемные носители (диски, дискеты, flash-накопители, пр.), содержащие персональные данные, подлежат учёту. Каждый съемный носитель с записанными персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

Учет и выдачу съемных носителей персональных данных осуществляет Администратор информационной безопасности.

Работники получают учтенный съемный носитель от Администратора информационной безопасности для выполнения работ на конкретный срок.

При получении съемного носителя делаются соответствующие записи в Журнале учета носителей, содержащих персональные данные.

По окончании работ пользователь сдает съемный носитель для хранения Администратору информационной безопасности, о чем делается соответствующая запись в Журнале учета носителей, содержащих персональные данные.

При работе со съемными носителями персональных данных, запрещается:
- хранить съемные носители, содержащие персональные данные, вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители, содержащие персональные данные, из служебных помещений для работы с ними на дому, в гостиницах и т.д.

При отправке или передаче персональных данных адресатам на съемные носители

записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей, содержащих персональные данные, для непосредственной передачи адресату осуществляется по согласованию с Администратором информационной безопасности МАОУ «СОШ №104 г. Челябинска» .
О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений должно быть немедленно сообщено Администратору информационной безопасности МАОУ «СОШ №104 г. Челябинска» .
На утраченные носители составляется акт. Соответствующие отметки вносятся в Журнал учета носителей, содержащих персональные данные.
Съемные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется комиссией, созданной приказом МАОУ «СОШ №104 г. Челябинска» . По результатам уничтожения носителей составляется акт по прилагаемой форме (Приложение N 2).
5. Заключительные положения
С положениями настоящей Инструкции должны быть ознакомлены под роспись все работники структурных подразделенийМАОУ «СОШ №104 г. Челябинска» и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке персональных данных работников и других лиц.

ПРИЛОЖЕНИЕ N 1 к инструкции по организации парольной защиты на объектах вычислительной техники в МАОУ «СОШ №104 г. Челябинска» филиал

УТВЕРЖДАЮ
_____
«____» _____ 201_ г.

АКТ
передачи персональных данных третьим лицам
_____
(должность, ФИО)
передал(а) следующие документы, содержащие персональные данные_____:
(ФИО работника)
_____
_____
_____
(перечислить наименования передаваемых документов, содержащих персональные данные)
по запросу_____
(ФИО, должность)

с
целью_____
_____
_____
_____.

_____ _____
Подпись расшифровка подписи

Документы, содержащие персональные данные принял(а), экземпляр акта получил(а):

_____ _____
подпись расшифровка подписи

«____» _____ 201__ года

ПРИЛОЖЕНИЕ N 2 к инструкции по организации парольной защиты на объектах вычислительной техники в МАОУ «СОШ №104 г. Челябинска» филиал

УТВЕРЖДАЮ
_____
«____» _____ 201_ г.

АКТ
уничтожения носителей, содержащих персональные данные

Комиссия, наделенная полномочиями приказом МАОУ «СОШ №104 г. Челябинска» от «__»_____ 201__года N ___ в составе:
_____
_____
_____
((должности, ФИО))
провела отбор носителей персональных данных, не подлежащих дальнейшему хранению:

N п/п	**Дата**	**Учетный номер носителя**	**Пояснения**
1	2	3	4

Всего съемных носителей_____
(цифрами и прописью)

Носители уничтожены путем сжигания/размагничивания/ физического уничтожения/иного способа.

Председатель комиссии Подпись Дата
Члены комиссии Подпись Дата
(ФИО)

ПРИЛОЖЕНИЕ N 3 к инструкции по организации парольной защиты на объектах вычислительной техники в МАОУ «СОШ №104 г. Челябинска» филиал

И Н С Т Р У К Ц И Я

по действиям работников МАОУ «СОШ №104 г. Челябинска» образования, осуществляющих обработку персональных данных, на случай кризисных ситуаций

УТВЕРЖДЕНА
приказом МАОУ «СОШ №104 г. Челябинска»

1. Общие положения

В кризисных ситуациях (пожар, стихийное бедствие, внезапное нападение, угроза хищения или уничтожения документов и техники) работники МАОУ «СОШ №104 г. Челябинска», осуществляющие обработку персональных данных с использованием средств криптографической защиты информации (далее - ответственные за эксплуатацию криптосредств), обязаны руководствоваться настоящей инструкцией и принимать все необходимые меры по обеспечению безопасности средств криптографической защиты, эксплуатационной и технической документации к ним, носителей персональных данных.
Ответственность за выполнение мероприятий в кризисных ситуациях, наряду с ответственными за эксплуатацию криптосредств МАОУ «СОШ №104 г. Челябинска» , несут работники безопасности, осуществляющие пропуск в здание (далее - охранники, вахтеры).
Контроль за выполнением мероприятий и действиями охранников, вахтеров и ответственных за эксплуатацию криптосредств, по обеспечению безопасности криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных осуществляется зам.директора по АХЧ, в функциональные обязанности которого входит контроль за организацией работы по защите информации, не реже одного раза в год с практической отработкой возможных ситуаций.

2. Обязанности ответственных за эксплуатацию криптосредств в случае возникновения кризисных ситуаций в рабочее время

В случае возникновения кризисных ситуаций и угрозы зданию, ответственные за эксплуатацию криптосредств обязаны:
оценить возможность компрометации хранящихся ключевых и других документов;
сообщить о случившемся директору МАОУ «СОШ №104 г. Челябинска», вскрыть хранилища с криптосредствами, эксплуатационной и технической документацией к ним, носителями персональных данных, при необходимости составить акт;
подготовить криптосредства, эксплуатационную и техническую документацию к ним, носители персональных данных для эвакуации или уничтожения указанным ниже порядком.

2.1. Действия ответственных за эксплуатацию криптосредств в случае эвакуации криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных

При получении команды на эвакуацию криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных ответственные за эксплуатацию

криптосредствобязаны:
уложить в мешки содержимое хранилищ, список которых указан в приложении N 1;
опечатать мешки с эвакуируемыми криптосредствами, эксплуатационной и технической документацией к ним, носителями персональных данных;
совместно с вахтерами перенести мешки с криптосредствами, эксплуатационной и технической документацией к ним, носителями персональных данных в кабинет министра, соблюдая при этом режим охраны и безопасности.
В случае развития угрожающей ситуации в здании МАОУ «СОШ №104 г. Челябинска» эвакуируемые криптосредства, эксплуатационную и техническую документацию к ним, носители персональных данных вывезти в здание МАОУ «СОШ №104 г. Челябинска», расположенного по адресу: г. Челябинск, ул. Володарского, 14 (Комитет по делам образования г. Челябинска).
При эвакуации криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных должны быть приняты меры, исключающие возможность их просмотра посторонними лицами.

2.2. Действия ответственных за эксплуатацию криптосредств в случае уничтожения документов и техники

Если в кризисной ситуации при угрозе захвата здания МАОУ «СОШ №104 г. Челябинска» принять все необходимые меры по сохранности криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных не представляется возможным, то они должны быть уничтожены. Решение об уничтожении криптосредств, эксплуатационной и технической документации к ним принимает министр или лицо, уполномоченное им, курирующий организацию работы по защите информации, а в случае их отсутствия - администратор безопасности ИСПДн самостоятельно.
Порядок уничтожения криптосредств, эксплуатационной и технической документации к ним:
В первую очередь производится уничтожение криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных. Журналы учета уничтожаются в последнюю очередь.
Уничтожение оформляется актом, подписывается не менее чем двумя лицами, допущенными к работе с криптосредствами в МАОУ «СОШ №104 г. Челябинска» .
В особых, не терпящих отлагательства случаях, уничтожение криптосредств, эксплуатационной и технической документации к ним может производиться одним или двумя лицами без составления акта, с проставлением отметок в журналах учета, но с обязательным последующим оформлением документа, в котором указывается, что уничтожено и при каких обстоятельствах. Этот документ подписывается лицом (лицами), производившими уничтожение.
Об уничтоженных материалах срочно ставится в известность любым доступным способом директору и в бухгалтерию МАОУ «СОШ №104 г. Челябинска».

3. Обязанности службы охраны МАОУ «СОШ №104 г. Челябинска», в случае возникновения кризисных ситуаций по обеспечению безопасности криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных
3.1. При срабатывании охранной сигнализации в нерабочее время

При поступлении сигнала «Тревога» на центральный пункт охраны МАОУ «СОШ №104 г. Челябинска», группа быстрого реагированиядолжна немедленно прибыть на объект,сообщить об этом одному из работников МАОУ «СОШ №104 г. Челябинска» . После прибытия на место работник МАОУ «СОШ №104 г. Челябинска» и сотрудники охраны, немедленно приступают к визуальному осмотру целостности стекол и входных дверей здания. В случае обнаружения нарушений проходят в здание и осматривают помещения, указанные в приложении N 1.
При обнаружении посторонних лиц немедленно вызывают полицию по телефону 02 и принимают все меры к их задержанию.
При обнаружении нарушения целостности помещений, указанных в приложении N 1, вызывают сотрудников, ответственных за эксплуатацию криптосредств, указанных в приложении N 2.

3.2. При срабатывании пожарной сигнализации в помещениях, указанных в приложении N 1, в рабочее время

При срабатывании пожарной сигнализации работник МАОУ «СОШ №104 г. Челябинска», ответственный за пожарную безопасность проверяет помещения на признаки возгорания (задымление, запах гари, повышение температуры воздуха и т.п.) и наличие возгорания в других помещениях, их окружающих. В случае обнаружения очага возгорания действуют согласно п. 5 Инструкции о порядке охраны и организации пропускного режима:
вызывает по телефону 01 пожарную команду или аварийную службу;
информирует ответственных за эксплуатацию криптосредств, согласно приложению N 2.
Ответственные за эксплуатацию криптосредств решают вопрос об эвакуации криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных.
Работник МАОУ «СОШ №104 г. Челябинска» ответственный за пожарную безопасность, выполняя свои обязанности, организует, при необходимости, помощь ответственным за эксплуатацию криптосредств по эвакуации криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных.
При возникновении кризисной ситуации руководством МАОУ «СОШ №104 г. Челябинска» незамедлительно принимаются меры по ее ликвидации, последствий происшествия, а также информируется Комитет по делам образования г. Челябинска.

Директор МАОУ "СОШ №104 г. Челябинска" Петрова О.В.

13 мая 2020