Подписано цифровой подписью: МАОУ СОШ № 9
DN: email=esokolova1970@mail.ru, 1.2.643.3.131.1.1=120C303036363637303039303633, 1.2.643.100.3=120B303237323034353131313130, 1.2.643.100.1=120D31303236363031333737383133, title=директор, o=МАОУ СОШ № 9, street=УЛ ИЛЬИЧА, ДОМ 12, l=Нижний Тагил, st=66 Свердловская область, c=RU, givenName=Елена Григорьевна, sn=Соколова, cn=МАОУ СОШ № 9
Дата: 2021.09.23 09:14:43 +05'00'

Приложение №3 к приказу
№ 60 от 07.04.2021 г.

Должностной регламент работы сотрудников МАОУ СОШ № 9 с персональными данными

1. Общие положения

1.1. Данный регламент составлен в соответствии с Федеральным законом от 27.07.2006 ФЗ-152 «О персональных данных» и устанавливает требования к обеспечению безопасности персональных данных при различных видах обработки, определяет основные цели, функции и права сотрудников МАОУ СОШ № 9, осуществляющих обработку персональных данных.

1.2. Обработка персональных данных в Муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 9 (далее – Учреждение) может осуществляться только в функциональных и образовательных целях.

1.3. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.4. Директором Учреждения утверждается перечень должностей сотрудников, осуществляющих от имени Оператора (МАОУ СОШ № 9) хранение, обработку и передачу персональных данных, пользователи уведомляются об ответственности за нарушение данного регламента, об особенностях и правилах такого рода обработки.

1.5. Для защиты персональных данных, подвергаемых автоматизированной обработке, предусматривается парольная система, используются программные средства предотвращения несанкционированной утечки информации (лицензионное ПО и антивирусные программы).

1.6. Для защиты мест хранения персональных данных, воспрепятствования незаконному проникновению в помещения, где хранятся персональные данные, усиливаются средства защиты помещений, определен порядок доступа в данные помещения.

1.7. При обращении физических и юридических лиц за персональными данными сотрудников и (или) обучающихся и их родителей факт обращения и характер запроса регистрируются в журнале установленной формы.

1.8. Ответственность за ненадлежащую подготовку информации, её несанкционированную передачу несет должностное лицо, результатом деятельности которого явились нарушения.

2. Порядок работы сотрудников, осуществляющих обработку персональных данных

2.1. Сотрудники, осуществляющие обработку персональных данных, обязаны:

2.1.1. Строго соблюдать правила и инструкции по работе с персональными данными, знать и выполнять требования действующих нормативных и локальных документов, регламентирующих порядок действий по защите информации.

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

2.1.3. Соблюдать требования парольной политики.

2.1.4. Соблюдать правила при работе в локальных сетях или сети Интернет.

2.1.5. Не допускать несанкционированное распространение персональных данных.

2.1.6. Располагать экран монитора в помещении во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.

2.1.7. Хранить предназначенные для обработки персональные данные на отдельных материальных носителях в соответствии с целями обработки.

2.1.8. Своевременно обновлять персональные данные при их изменении или дополнении.

2.1.9. Фиксировать факты передачи персональных данных в регистрационном журнале установленного образца.

2.1.10. Уведомлять о случаях несанкционированной передачи персональных данных администрацию Учреждения.

2.1.11. При необходимости блокировки или уничтожения персональных данных совершать действия только в отношении подлежащих уничтожению или блокировки данных, обеспечивая защиту иной информации.

2.1.12. При обнаружении нарушений порядка предоставления персональных данных уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных пользователям до выяснения причин нарушения и устранения этих причин.

2.1.13. Для получения консультаций по вопросам работы и настройке ПО необходимо обращаться к ответственному за администрирование ПК, ПО, ИСПДн.

2.2 Сотрудникам, осуществляющим обработку персональных данных, запрещено:

2.2.1. Разглашать защищаемую информацию третьим лицам.

2.2.2. Участвовать в передаче персональных данных, не определенной функциональными обязанностями и (или) запрещенной к передаче.

2.2.3. Копировать защищаемую информацию на внешние носители без разрешения директора Учреждения.

2.2.4. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

2.2.5. Пересылать по произвольным адресам не затребованную потребителями информацию, а также информацию, передача которой согласно положению о защите персональных данных не регламентирована.

2.2.6. При работе с документами, содержащими персональные данные, запрещается оставлять их на рабочем месте или оставлять шкафы (сейфы) с данными документами открытыми (незапертыми) в случае выхода из рабочего помещения.

2.2.7. Оставлять в помещении посторонних лиц, не имеющих доступа к персональным данным в данном структурном подразделении, без присмотра.

2.2.8. Запись, хранение и вынос за пределы учреждения на внешних носителях информации (диски, дискеты, USB флэш-карты и т.п.), передача по внешним адресам электронной почты или размещение в сети Интернет информации, содержащей персональные данные субъектов.

2.2.9. Передавать персональные данные по телефонной связи, факсу.

2.2.10. Искажать персональные данные при фиксации, передаче или копировании.

2.2.11. Использовать персональные данные сотрудников и (или) обучающихся, их законных представителей в целях, не предусмотренных должностными обязанностями.

3. Порядок работы ответственного за администрирование ПК, ПО, ИСПДн.

3.1. Ответственный за администрирование ПК, ПО, ИСПДн, обязан:

3.1.1. Знать и выполнять требования действующих нормативных и локальных документов, а также внутренних инструкций, по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

3.1.2. Контролировать выполнение требований действующих нормативных и локальных документов по защите персональных данных, при проведении работ на ПК.

3.1.3. Работать с учетными записями пользователей ИСПДн (удаление, регистрация новых пользователей), их правильная настройка и разграничение прав доступа пользователей к защищаемым ресурсам ИСПДн согласно разрешительной системе доступа.

3.1.4. Контролировать доступ пользователей к работе на ПК и соблюдение пользователями требований нормативных и руководящих документов.

3.1.5. Настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе на ПК.

3.1.6. Сопровождать подсистемы обеспечения целостности информации на ПК:

- периодический контроль за отсутствием на жестком диске ПК остаточной информации по окончании работы пользователей;
- поддержание установленного порядка и правил антивирусной защиты информации, обрабатываемой на ПК;
- контроль за соблюдением пользователями инструкции по антивирусному контролю. Программирование, выдача пользователям паролей.

3.1.7. Контроль за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусе ПК и устройств.

3.1.8. Обеспечивать устойчивую работоспособность элементов ИСПДн, средств ее защиты при обработке персональных данных на ПК.

3.1.9. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения и серверов (операционные системы, прикладное и специальное ПО);
- аппаратных средств;
- аппаратных и программных средств защиты.

3.1.10. Обеспечивать работоспособность элементов ПК, ИСПДн, локальной сети, сети Интернет.

3.1.11. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

3.1.12. 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.

3.1.13. Проводить периодический контроль принятых мер защиты, впределах возложенных на него функций.

3.1.14. Осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля пользователем ИСПДн.

3.1.15. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

3.1.16. Информировать директора Учреждения о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

3.1.17. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

3.1.18. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3.2. Ответственный за администрирование ПК, ПО, ИСПДн имеет право:

3.2.1. Обеспечивать правильное функционирование и поддерживать работоспособность ПК и средств защиты информации от несанкционированного доступа в пределах возложенных на него функций.

3.2.2. В случае отказа работоспособности ПК и средств защиты информации от несанкционированного доступа принимать меры по их восстановлению.

3.2.3. Проводить инструктаж пользователей по правилам работы на ПК.

3.2.4. Немедленно докладывать директору Учреждения или лицу, исполняющему его обязанности, о фактах и попытках несанкционированного доступа к персональным данным, о неправомерных действиях пользователей или иных лиц, приводящих к нарушению требований по защите информации, а также об иных нарушениях требований информационной безопасности ИСПДн.

3.2.5. Проводить работу по выявлению возможных каналов утечки персональных данных, вести их учёт и принимать меры к их устранению.

3.2.6. Осуществлять не реже одного раза в неделю обновление антивирусных баз на ПК в ИСПДн.

3.2.7. Контролировать целостность (неизменность, сохранность) программного обеспечения, разрешительной системы доступа, а при обнаружении фактов изменения проверяемых параметров немедленно докладывать директору Учреждения.

3.2.8. Требовать от сотрудников Учреждения соблюдения установленного комплекса мероприятий по обеспечению безопасности информации.

3.2.9. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и расследованиях фактов (попыток) несанкционированного доступа.

3.2.10. 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.

4. Организация парольной защиты

4.1. Личные пароли доступа к персональным данным, содержащимся на ПК или в ИСПДн, выдаются ответственным за администрирование ПК, ПО, ИСПДн.

4.2. 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:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) 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 так же 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.

4.3. 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.

4.4. Правила хранение 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.

4.5. Лица, использующие паролирование, обязаны:

- Четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.

- Своевременно сообщать об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

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

5.1. Работа в локальных сетях или сети Интернет на элементах ИСПДн, должна проводиться при служебной необходимости.

5.2. При работе в Сети запрещается:

- Осуществлять работу при отключенных средствах защиты (антивирус и других).

- Передавать по Сети защищаемую информацию.

- Запрещается скачивать из Сети программное обеспечение и другие файлы.

- Запрещается посещение сайтов сомнительной репутации (сайты, содержащие нелегально распространяемое ПО и другие).

- Запрещается нецелевое использование подключения к Сети.