Муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа №8»

ПРИКАЗ

30.12.2020 г. № 104

Об утверждении инструкций по информационной безопасности

В соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию администратора информационной безопасности информационных систем персональных данных в МБОУ «Средняя общеобразовательная школа № 8».
2. Утвердить Инструкцию по организации парольной защиты в МБОУ «Средняя общеобразовательная школа № 8».
3. Утвердить Инструкцию по проведению антивирусного контроля в МБОУ «Средняя общеобразовательная школа № 8».
4. Утвердить инструкцию по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств в МБОУ «Средняя общеобразовательная школа № 8».
5. Утвердить инструкцию пользователей и технология обработки защищаемой информации в информационных системах персональных данных в МБОУ «Средняя общеобразовательная школа № 8».
6. Утвердить инструкцию пользователей ИСПДн по обеспечению безопасности при возникновении внештатных ситуаций.
7. Утвердить инструкцию по защите машинных носителей информации.
8. Утвердить инструкцию по защите технических средств в учреждении.
9. Утвердить инструкцию ответственного за защиту информации.
10. Утвердить инструкцию по управлению доступом пользователей к информации.

11. Утвердить инструкцию по управлению программным обеспечением.

12. Утвердить инструкцию по управлению событиями информационной безопасности.

13. Всем сотрудникам учреждения строго соблюдать требования утвержденных инструкций.

14. Контроль исполнения настоящего приказ оставляю за собой.

Директор школы  И.В. Абрамова

УТВЕРЖДАЮ

Директор школы _____ И.В. Абрамова

Приказ № 104 от 30.12. 2020 г.

ИНСТРУКЦИЯ

пользователей и технология обработки защищаемой информации в информационных системах персональных данных в МБОУ «Средняя общеобразовательная школа № 8»

1. Объекты вычислительной техники (ОВТ) разрешается использовать для обработки защищаемой информации при соблюдении следующих условий:

1.1. Право работы на ОВТ предоставляется Администратору информационной безопасности информации и пользователям.

1.2. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ОВТ, несет персональную ответственность за свои действия.

2. Обязанности пользователя ОВТ.

2.1. Выполнять на ОВТ только те процедуры, которые определены для него в должностной инструкции и других документах, регламентирующих рабочий процесс.

2.2. Знать и соблюдать установленные требования по защите информации, учету, хранению и пересылке машинных носителей информации, а также руководящих и организационно-распорядительных документов на данный ОВТ.

2.3. Пользователи перед началом обработки на ОВТ файлов, хранящихся на съемных носителях информации, должны осуществить проверку файлов на наличие компьютерных вирусов. Антивирусный контроль ОВТ должен осуществляться пользователем не реже одного раза в неделю.

2.4. Экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.5. Соблюдать установленный режим разграничения доступа к информационным ресурсам: получать у Администратора информационной безопасности (АИБ) временный пароль, самостоятельно изменять его, надежно запоминать и хранить в тайне.

2.6. Немедленно докладывать АИБ обо всех фактах и попытках НСД к обрабатываемой на ОВТ информации или об ее исчезновении (искажении).

2.7. Пользователям ОВТ запрещается:

- записывать и хранить информацию на неучтенных носителях информации (НИ);
- оставлять во время работы съемные носители информации (НИ) без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации;
- отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на данный ОВТ;
- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;
- самостоятельно устанавливать, тиражировать, или модифицировать

программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

- обрабатывать на ОВТ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам обработки информации;

- сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ОВТ;

- производить копирование дискет, отдельных файлов с учтенных НИ на неучтенные НИ, в том числе для временного хранения информации;

- работать на ОВТ при обнаружении каких-либо неисправностей;

- хранить НИ вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;

- хранить на учтенных НИ программы и данные, не относящиеся к рабочей информации;

- привлекать посторонних лиц для производства ремонта ОВТ.

3. Организация парольной защиты при работе на объектах информатизации.

3.1 Личные пароли доступа к объекту информатизации, системе защиты от НСД, выдаются пользователям Администратором информационной безопасности, и при этом необходимо руководствоваться следующими требованиями:

- длина пароля должна быть не менее 6-ти буквенно-цифровых символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об ответственном исполнителе;

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

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

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 2 позициях;

- в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

- не использовать ранее использованные пароли.

3.2. Лица, использующие паролирование, обязаны:

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

- своевременно сообщать Администратору безопасности о всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

3.3. При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

- хранить пароли в записанном виде на отдельных листах бумаги;

- сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

4. Порядок применения парольной защиты.

4.1. Полная плановая смена паролей на ОВТ проводится не реже одного раза в год.

4.2. Удаление (в т.ч. внеплановая смена) личного пароля любого пользователя ОВТ должна производиться в следующих случаях:

- в случае подозрения на дискредитацию пароля;
- по окончании срока действия;
- в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) пользователя после окончания последнего сеанса работы данного с системой;
- по указанию Администратора информационной безопасности.

4.3. Смена пароля осуществляется Администратором информационной безопасности.

4.4. Для предотвращения доступа к защищаемой информации, находящейся в ПЭВМ, минуя ввод пароля, пользователь во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации Win + L или кнопки «Блокировать».

Порядок применения (смены) паролей при работе на ПЭВМ, оборудованных системой защиты от НСД, приведен в эксплуатационной документации на СЗИ.

5. Технология обработки защищаемой информации.

5.1. При первичном допуске к работе на ОВТ Пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, изучает инструкцию пользователя средств защиты информации, получает персональный идентификатор или личный текущий пароль у Администратора информационной безопасности.

5.2. В процессе работы пользователь производит обработку защищаемой информации на ОВТ под управлением операционной системы Windows.

5.3. При необходимости вывод защищаемой информации из ИСПДн осуществляется следующим образом:

- копированием информации на учтенные носители;
- печать на принтере;
- передача информации по каналам связи с обязательным применением криптографической защиты.

Подготовил:

Администратор безопасности информации _____ М.О. Черкашин

УТВЕРЖДАЮ
Директор школы _____ И.В. Абрамова
Приказ № 104 от 30.12. 2020 г.

ИНСТРУКЦИЯ
по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств в МБОУ «Средняя общеобразовательная школа № 8»

Настоящей инструкцией регламентируются действия при проведении модификаций программного обеспечения, технического обслуживания средств вычислительной техники в МБОУ СОШ № 8, а так же при возникновении нештатных ситуаций.

Модификация программного обеспечения (ПО) и аппаратных средств в МБОУ СОШ № 8, аттестованной по требованиям безопасности информации, производится при обязательном согласовании с организацией, проводившей аттестацию данной ИСПДн.

1. Для аварийного восстановления общесистемного программного обеспечения в МБОУ СОШ № 8 должны храниться копии дистрибутивов, с которых устанавливалось данное ПО.

2. Установка и обновление ПО производится с оригинальных лицензионных дистрибутивных носителей.

3. Модификация программного обеспечения (ПО) в защищаемой в МБОУ СОШ № 8 согласуется с администратором информационной безопасности.

4. После установки (обновления) ПО в защищаемых ИСПДн администратор информационной безопасности должен произвести настройку средств управления доступом к компонентам ПО, проверить работоспособность ПО и правильность настройки средств защиты.

5. Обновление баз антивирусной программы в ИСПДн осуществляется ежедневно под контролем администратора информационной безопасности.

6. Для аварийного восстановления программных средств защиты информации в МБОУ СОШ № 8 должны храниться копии дистрибутивов, с которых устанавливалось данное ПО.

7. Все изменения в программном обеспечении ИСПДн вносятся в соответствующие разделы технических паспортов государственных информационных систем.

8. После завершения работ по внесению изменений в состав программного обеспечения аттестованной ИСПДн, проводится переаттестация.

9. При передаче ПЭВМ из состава ИСПДн на техническое обслуживание с ПЭВМ снимаются аппаратные средства защиты информации (при наличии) и жесткий диск с информацией.

10. Техническое обслуживание и ремонтные работы ПЭВМ из состава ИСПДн должны осуществляться только уполномоченными сотрудниками, назначенными ответственными за их обслуживание (сопровождение). Их вызов осуществляется сотрудниками подразделения, эксплуатирующего ИСПДн, при возникновении нештатных ситуаций (выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств ПЭВМ).

13. Ответственность за соблюдение требований по обеспечению безопасности информации при проведении технического обслуживания и ремонтных работ на защищаемых ПЭВМ в составе ИСПДн возлагается на администратора информационной безопасности.

Подготовил:

Администратор безопасности информации _____ М.О. Черкашин