Министерство образования и молодежной политики Свердловской области

государственное автономное профессиональное образовательное учреждение Свердловской области «Ирбитский мотоциклетный техникум» (ГАПОУ СО «ИМТ»)

Директор ГАПОУ СО «ИМТ»

_____ С.А. Катцина

«30» декабря 2019 г.

МП

ИНСТРУКЦИЯ

по организации антивирусной защиты в информационных системах персональных данных

государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум»

2019 год

г. Ирбит

Номер документа	СП-03-2019-№ _3.3-06__
Документ вводится	Впервые

РАССМОТРЕНО
Советом Автономного учреждения
Протокол № 10
от « 26 » декабря 2019 г.

Утверждено и введено в действие
приказом директора ГАПОУ СО «ИМТ»
№392-од от « 30 » декабря 2019 г.

Инструкция по организации антивирусной защиты в информационных системах персональных данных государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум», 2019

Инструкция по организации антивирусной защиты в информационных системах персональных данных государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум» разработана в соответствии с законодательством Российской Федерации о персональных данных и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности персональных данных, определяет требования к организации программного обеспечения, участвующего в обработке персональных данных от разрушающего воздействия компьютерных вирусов и иного вредоносного программного обеспечения, устанавливает ответственность руководителей и сотрудников, эксплуатирующих и сопровождающих информационные системы персональных данных ГАПОУ СО «ИМТ».

ИНСТРУКЦИЯ
по организации антивирусной защиты в информационных системах персональных данных государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум»

СОДЕРЖАНИЕ

ИНСТРУКЦИЯ
по организации антивирусной защиты в информационных системах персональных данных государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Инструкция по организации антивирусной защиты в информационных системах персональных данных государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум» (далее – настоящая Инструкция) является одним из локальных нормативных актов государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум» (далее – Автономного учреждение), регламентирующих деятельность Автономного учреждения по обеспечению безопасности персональных данных работников организации, участников образовательного процесса.

2. Настоящая инструкция разработана в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «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», другими нормативными правовыми актами по обеспечению безопасности персональных данных и определяет требования к организации программного обеспечения (ПО), участвующего в обработке персональных данных от разрушающего воздействия компьютерных вирусов и иного вредоносного ПО, и устанавливает ответственность руководителей и сотрудников, эксплуатирующих и сопровождающих информационные системы персональных данных Автономного учреждения

3. Организационное и техническое обеспечение процессов антивирусной защиты информационных систем персональных данных (далее – ИСПДн) Автономного учреждения и контроль за действиями исполнителей и обслуживающего персонала возлагается на Администратора информационных систем персональных данных Автономного учреждения (далее – Администратора ИСПДн).

2. УСТАНОВКА И ОБНОВЛЕНИЕ АНТИВИРУСНЫХ СРЕДСТВ

4. На рабочих местах ИСПДн может использоваться программное и аппаратное обеспечение, необходимое для выполнения служебной деятельности и согласованное с Администратором ИСПДн.

5. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, имеющие соответствующий сертификат ФСТЭК по защите персональных данных.

6. Установка средств антивирусного контроля на автоматизированное рабочее место (АРМ) и серверах ИСПДн осуществляется Администратором ИСПДн в соответствии с Инструкцией по установке и эксплуатации производителя соответствующего средства антивирусного контроля.

7. Регулярное обновление антивирусных средств осуществляется автоматически и контролируется Администратором ИСПДн, ответственным за организацию антивирусной защиты. В случае получения пользователем на рабочем месте сообщения о невозможности (сбое) автоматического обновления, необходимо оповестить об этом Администратора ИСПДн.

3. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

8. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль системной памяти, объектов автозапуска и загрузочных секторов всех дисков компьютера.

9. Полная антивирусная проверка компьютера должна включать проверку всех жестких дисков, всех сменных дисков и устройств, почтовых ящиков, резервного хранилища системы. Она должна проводиться регулярно, не реже одного раза в месяц и может регламентироваться и контролироваться сервером администрирования антивирусной защиты ИСПДн.

10. Обязательному постоянному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, запоминающих устройств USB, CD-ROM и т.п.).

11. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо «чистой» (не зараженной вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере.

12. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

14. Установка (изменение) системного и прикладного ПО осуществляется на основании инструкции по установке и эксплуатации ПО и аппаратных средств ИСПДн данного производителя.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) ПО АРМ и/или серверах ИСПДн, должна быть выполнена антивирусная проверка:

1) на защищаемых серверах и на АРМ – Администратором ИСПДн,
2) на других серверах и рабочих станциях, не требующих защиты, - лицом, установившим (изменившим) ПО, в присутствии и под контролем Администратора ИСПДн.

15. Факт выполнения полной антивирусной проверки после установки (изменения) ПО должен регистрироваться в специальном журнале (Приложение № 1).

16. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник самостоятельно или вместе с ответственным за обеспечение безопасности информации должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь Администратора ИСПДн, для определения им факта наличия или отсутствия компьютерного вируса.

4. ДЕЙСТВИЯ СОТРУДНИКОВ ПРИ ОБНАРУЖЕНИИ КОМПЬЮТЕРНОГО ВИРУСА

17. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

1) приостановить работу;

2) немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

3) совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

4) провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора);

18. В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, Администратор ИСПДн должен передать его в организацию, с которой заключен договор на антивирусную поддержку (разработчику антивирусного ПО).

19. По факту обнаружения зараженных вирусом файлов составить служебную записку Администратору ИСПДн,, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

5. ОТВЕТСТВЕННОСТЬ ПРИ ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

20. Ответственность за организационное и техническое обеспечение процессов антивирусной защиты информационных систем персональных данных Автономного учреждения и контроль за действиями исполнителей и обслуживающего персонала возлагается на Администратора ИСПДн.

21. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей инструкции возлагается на Администратора ИСПДн.

22. Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей инструкции сотрудниками Автономного учреждения осуществляется Администратора ИСПДн,, ответственным за организацию антивирусной защиты ИСПДн» Автономного учреждения.

6. ПРОЦЕДУРА ВНЕДРЕНИЯ И ОБЕСПЕЧЕНИЯ НАСТОЯЩЕЙ ИНСТРУКЦИИ

23. Настоящая Инструкция вводится в действие приказом директора автономного учреждения.

24. Настоящая Инструкция принимается к действию лицами, осуществляющими деятельность в информационных систем персональных данных Автономного учреждения, под подпись с даты введения инструкции.

29. Настоящая Инструкция принимается на неопределенный срок. Изменения и дополнения в настоящую Инструкцию вносятся и рассматриваются в составе новой редакции на Совете Автономного учреждения и утверждаются приказом директора Автономного учреждения.

Приложение № 1

ЖУРНАЛ
результатов полной антивирусной проверки

№ п\п	Лица, осуществляющие контроль за антивирусной защитой		Дата полной проверки	Результат проверки
	Должность	ФИО		