ПРИЛОЖЕНИЕ №13
УТВЕРЖДЕНО
Приказом «О вводе в действие комплекта организационно-распорядительной документации по организации обработки и защиты персональных данных» МБОУ Сокольская СШ
от «30» августа 20 24 г.№ 595
(М.П.)

Инструкция
по антивирусной защите
информационных систем персональных данных

Оглавление

1. Общие положения

1.1. Муниципальное бюджетное общеобразовательное учреждение Сокольская средняя школа (далее – Организация) руководствуется настоящей Инструкцией по антивирусной защите информационных системы персональных данных (далее - Инструкция), определяющей порядок организации антивирусной защиты, порядок действий администратора безопасности и пользователей информационных систем персональных данных «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании» при обнаружении вредоносных компьютерных программ (вирусов).

1.2. Сокращения, термины и определения

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
Антивирусное ПО	Программное обеспечение средств антивирусной защиты
Вредоносное ПО	Вредоносная компьютерная программа (вирус)
АРМ	Автоматизированное рабочее место
ПДн	Персональные данные
ПО	Программное обеспечение
СВТ	Средства вычислительной техники

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности информационной системы персональных данных (администратор безопасности)	Работник, ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных	
Вредоносная программа	Программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на	ГОСТ Р 51275-2006

Термин	Определение	Источник
	информацию или ресурсы информационной системы	
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
(компьютерный) вирус	Вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы	ГОСТ Р 51275-2006
Машинный носитель информации	Материальный носитель, используемый для передачи и хранения защищаемой информации (в том числе персональных данных (далее – ПДн)) в электронном виде.	
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»,

Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.4. Пользователи информационных систем должны быть ознакомлены с настоящей Инструкцией до начала работы в информационных системах под роспись. Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн.

2. Общий порядок организации антивирусной защиты

2.1. Антивирусное ПО устанавливается на все СВТ, входящие в состав информационных систем для предотвращения заражения вредоносными

компьютерными программами (вирусами) (далее – вредоносным ПО) через съемные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сервисы) и международного информационного обмена (Интернет).

2.2. К использованию в информационных системам допускаются только лицензионные средства антивирусной защиты, прошедшие в установленном порядке процедуру сертификации средств защиты информации по требованиям безопасности информации.

2.3. На все применяемые в информационных системах средства антивирусной защиты должны быть документы, подтверждающие права Организации на их использование и действующие сертификаты ФСТЭК России.

2.4. Ответственный за организацию обработки персональных данных обеспечивает организацию антивирусной защиты информационных систем в Организации.

2.5. Администратор безопасности осуществляет установку, конфигурирование и управление средствами антивирусной защиты информационных систем в Организации в соответствии с эксплуатационной документацией на антивирусное ПО, а также надежное хранение эталонных копий антивирусного ПО.

2.6. Пользователи информационных систем являются ответственными за ежедневный контроль на своих АРМ и своевременное информирование администратора безопасности в случае обнаружения вредоносного ПО или при появлении иных предупреждающих сообщений средств антивирусной защиты (истечения срока лицензии, о неактуальности базы данных признаков вредоносных компьютерных программ (вирусов) и т.п.).

2.7. Контроль над работой пользователя информационных систем по применению на непосредственных АРМ средств антивирусной защиты осуществляет администратор безопасности.

3. Реализация антивирусной защиты

3.1. Антивирусное ПО должно запускаться автоматически при старте операционной системы СВТ информационных систем и функционировать до завершения работы операционной системы.

3.2. Пользователям информационных систем запрещается блокировать, изменять настройки и выгружать антивирусное ПО на своих АРМ.

3.3 Антивирусная проверка должна осуществляться для следующих объектов:

– файлов загрузки – при загрузке операционной системы;

– системного и прикладного программного обеспечения, исполняемых файлов – в автоматическом режиме в период сеанса работы;

– поступающей информации по каналам передачи данных – в автоматическим режиме до открытия информации (запуска исполняемых файлов);

– информации, поступающей на съемных носителях – при подключении съемного носителя к техническому средству;

– исходящей информации – непосредственно перед ее отправкой (записью на съемный носитель);

– устанавливаемого (изменяемого) программного обеспечения – непосредственно перед установкой;

– машинных носителях информации, установленных в корпус СВТ (накопители на жестких дисках) – не реже одного раза в неделю.

3.4. Любое устанавливаемое (обновляемое) программное обеспечение в информационных системах проверяется на отсутствие вредоносного ПО до момента установки. После установки или обновления программного обеспечения проводится повторная антивирусная проверка.

3.6. Администратор безопасности при управлении средствами антивирусной защиты информационных систем обеспечивает:

– установку, настройку, управление конфигурацией и логической структурой всего антивирусного ПО;

– установку и обновление лицензионных ключей средств антивирусной защиты;

– установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);

– ограничение доступа пользователей на АРМ к настройкам установленных средств антивирусной защиты;

– настройку рассылки сообщений об обнаружении вредоносного ПО, о сбоях в работе средств антивирусной защиты, о необходимости обновления базы данных признаков вредоносных компьютерных программ (вирусов) и т.п.;

– внеплановую проверку АРМ, съемных машинных носителей информации в случае подозрения на наличие вредоносного ПО;

– восстановление работоспособности программных средств и информационных массивов, поврежденных вредоносным ПО;

– решение проблем, возникающих в процессе использования средств антивирусной защиты.

3.7. Администратор безопасности осуществляет настройку регистрации событий информационной безопасности средств антивирусной защиты информационных систем, включая:

– отказ работоспособности средств антивирусной защиты и их компонентов;

– обнаружение вредоносного ПО;

– изменение любых текущих настроек средств антивирусной защиты;

– установка и распространение обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

Журналы регистрации событий средства антивирусной защиты информационных систем должны быть доступны для оперативного анализа в течение 1 месяца с момента регистрации события.

4. Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

4.1. Базы данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты информационных систем автоматически обновляются на ежедневной основе из доверенных источников.

4.2. Администратор безопасности не реже 1 раза в день проводит контроль обновления баз данных признаков вредоносных компьютерных программ (вирусов).

5. Порядок действий при обнаружении вредоносного программного обеспечения

5.1. При обнаружении вредоносного ПО на съемных носителях, в электронных отправлениях или при посещении ресурсов сети Интернет пользователь информационных систем обязан:

– приостановить работу с источником угрозы (съемным носителем, электронным отправлением, Интернет-ресурсом), иные работы на автоматизированном рабочем месте не запрещаются;

– сообщить администратору безопасности об обнаружении вредоносного программного обеспечения;

– принять меры по локализации и удалению вредоносного ПО, рекомендованные администратором безопасности.

5.2. При обнаружении вредоносного ПО в процессе обработки информации, за исключением пункта 3.1, пользователь обязан:

– приостановить все работы на АРМ;

– сообщить администратору безопасности об обнаружении вредоносного программного обеспечения;

– принять меры по локализации и удалению вредоносного ПО, рекомендованные администратором безопасности.

5.3. Администратор безопасности по факту событий, предусмотренных пунктами 5.1, 5.2 должен зарегистрировать вирусную атаку в журнале событий безопасности в соответствии с «Инструкцией по управлению событиями информационной безопасности информационных систем».

5.4. При обнаружении вредоносного ПО на серверном или телекоммуникационном оборудовании администратор безопасности обязан:

– немедленно сообщить ответственному за организацию обработки ПДн об обнаружении вредоносного программного обеспечения;

– принять меры по локализации и удалению вредоносного ПО, а также по выявлению источника и способа проникновения вредоносного ПО.

5.5. В случае невозможности удаления вредоносного ПО, администратору безопасности следует обратиться в организацию, осуществляющую техническую поддержку средств антивирусной защиты. При передаче образцов зараженных файлов, а также при предоставлении информации о вирусной атаке в организацию, осуществляющую техническую поддержку средств антивирусной защиты информации, должны быть соблюдены требования конфиденциальности обрабатываемых ПДн в информационных системах.

6. Обязанности пользователей информационных систем

6.1. При работе в информационных системах пользователи обязаны:

– вести ежедневный контроль над работой средств антивирусной защиты;

– проверять вложения электронной почты, съёмные машинные носители информации перед началом работы на предмет наличия вредоносного ПО;

– немедленно уведомлять администратора безопасности при подозрении на заражение АРМ вредоносным ПО (медленная работа при открытии приложений, частое зависание ПО, самопроизвольный перезапуск, сбои в работе), при обнаружении вредоносного ПО (сообщение на экране монитора о наличии вируса), а также при появлении любых предупреждающих сообщений средств антивирусной защиты (истечения срока лицензии, о неактуальности базы данных признаков вредоносных программ (вирусов) и т.п.);

6.2. Пользователям информационных систем запрещается:

– отключать, изменять настройки и выгружать антивирусное ПО на своих АРМ.

– самостоятельно осуществлять подключение (отключение) АРМ к локальной вычислительной сети, устанавливать (удалять) ПО, оборудование;

– использовать незарегистрированные в Организации машинные носители информации;

– продолжать обработку персональных данных и иные работы при обнаружении вредоносного ПО в процессе обработки информации.

7. Ответственность

7.1. Пользователи информационных систем должны быть предупреждены об ответственности за невыполнение требований настоящей Инструкции.

7.2. Работники Организации несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

Приложение

Рекомендации по защите компьютера от программ-шифровальщиков

1. Общие рекомендации

1.1. Не открывайте почтовые вложения от неизвестных отправителей.

В большинстве случаев программы-шифровальщики распространяются через почтовые вложения. Задача злоумышленника – убедить пользователя открыть вложение из письма, поэтому темы писем содержат угрозы: уведомление от арбитражного суда об иске; исполнительное производство о взыскании задолженности; возбуждение уголовного дела и тому подобное.

При этом вредоносными могут оказаться не только файлы формата EXE. Так же были случаи заражения компьютеров при открытии специально сформированных злоумышленниками файлов форматов DOC и PDF.

1.2. Своевременно обновляйте антивирусные базы, операционную систему и другие программы.

Регулярно обновляйте ваш антивирус. Вместе с антивирусными базами обновляются программные компоненты, улучшаются существующие функции и добавляются новые. А также устанавливайте обновления для операционной системы и других программ, которыми вы пользуетесь.

1.3. Регулярно создавайте резервные копий файлов и храните их вне компьютера.

Храните резервные копии вне компьютера (например, на съёмных носителях или в «облачных» хранилищах) и в зашифрованном виде. Таким образом, файлы будут защищены не только от программ-шифровальщиков, но и от отказов компьютерной техники.

1.4. Настройте доступ к общим сетевым папкам.

Если вы используете общие сетевые папки, рекомендуется создать отдельную сетевую папку для каждого пользователя. При этом права на запись должны быть только у владельца папки. Таким образом, при заражении одного компьютера файлы будут зашифрованы только в одной сетевой папке. В противном случае, заражение одного компьютера может привести к шифрованию всех документов на всех сетевых папках.

2. Рекомендации по настройке параметров компьютера

2.1. В состав операционных систем Windows входит служба защиты системы на всех дисках, которая создаёт резервные копии файлов и папок во время архивации или создания точки восстановления системы. По умолчанию эта служба включена только для системного раздела. Рекомендуется включить службу для всех разделов.

3. Что делать, если файлы зашифрованы

3.1. Если у вас установлен какой-либо антивирусный продукт, то в настройках параметров этого продукта выполните следующее:

- Отключите автоматическое удаление обнаруженных вредоносных объектов;
- Установите действие **Поместить файл на карантин**.

Примечание: рекомендуется не удалять объекты из карантина, так как в некоторых случаях вредоносные файлы могут содержать ключи, которые могут помочь при расшифровке.

3.2. Удалите вирус.

Если у вас не установлен какой-либо антивирусный продукт, то проведите полную проверку при помощи бесплатных программ.

3.3. Создайте копии зашифрованных файлов.

3.4. Попытайтесь восстановить файлы:

- Для пользователей Windows 8;
- Для пользователей Windows 10.

3.5. Воспользуйтесь утилитами для автоматической расшифровки файлов:

- Утилита RectorDecryptor;
- Утилита XoristDecryptor;
- Утилита RakhniDecryptor.

ВНИМАНИЕ! Перед запуском утилит создайте копии файлов.

4. Список мест, где могут находиться файлы программ-шифровальщиков.

4.1. APPDATA:

- ОС Windows:
  - Диск:\Documents and Settings\%UserName%\Application Data\
  - %USERPROFILE%\Local Settings\Application Data

4.2. TEMP (временный каталог):

- %TEMP%\???????.tmp\ (пример: temp\vum35a5.tmp)
- %TEMP%\???????.tmp\??\ (пример: temp\7ze5418.tmp\mp)
- %TEMP%\???????\ (пример: temp\pcrdd27)
- %WINDIR%\Temp

4.3. Временный каталог Internet Explorer:

- ОС Windows: %USERPROFILE%\Local Settings\Temporary Internet Files\

4.4. Рабочий стол: %UserProfile%\Desktop\

4.5. Корзина:

- Диск:\Recycler\
- Диск:\$Recycle.Bin\
- Диск:\$Recycle.Bin\s-1-5-21-??????????-??????????-??????????-1000 (? --0-9)

4.6. Системный каталог

- %WinDir%
- %SystemRoot%\system32\

4.7. Каталог документов пользователя

- %USERPROFILE%\Мои документы\
- %USERPROFILE%\Мои документы\Downloads

4.8. Каталог для скачивания файлов в веб-браузере: %USERPROFILE%\Downloads

4.9. Каталог автозагрузки: %USERPROFILE%\Главное меню\Программы\Автозагрузка