

Муниципальное общеобразовательное бюджетное учреждение  
«Табагинская средняя общеобразовательная школа»  
Городского округа «Город Якутск»

677911, с. Табага, улица Пеледуйская, 4, телефон 408-398, 408-344, факс 408-398



"Утверждаю"

Директор МОБУ Табагинская СОШ

/Н.А. Шилова/

« 5 » сентября 2019 г.

**Инструкция по антивирусной защите Муниципального общеобразовательного учреждения «Табагинская средняя общеобразовательная школа» городского округа «город Якутск»**

**Введение.**

1.1. Настоящая инструкция определяет порядок организации антивирусной защиты и порядок действий администратора безопасности и пользователей информационной(-ых) системы(-ем) персональных данных (далее - ИСПДн) МОБУ ТСОШ при обнаружении вредоносного программного обеспечения (далее – ПО).

**2. Порядок организации антивирусной защиты.**

2.1. Программное обеспечение антивирусной защиты (далее – антивирусное ПО) устанавливаются на все средства вычислительной техники, входящие в составы ИСПДн. Антивирусное ПО обеспечивает защиту от внедрения вредоносного программного обеспечения со съемных носителей, через электронные отправления, из информационно-вычислительной сети, из сетей связи общего пользования и международного информационного обмена (Интернет).

2.2. Антивирусная защита каждой ИСПДн строится как единая система, которая обеспечивает:

2.2.1. управление конфигурацией и логической структурой всего программного обеспечения системы антивирусной защиты;

2.2.2. управление установкой и обновлением лицензионных ключей средств антивирусной защиты;

2.2.3. управление рассылкой и установкой обновлений баз средств антивирусной защиты;

2.2.4. ограничение доступа пользователей на рабочих местах к настройкам установленных средств антивирусной защиты;

2.2.5. настройку рассылки сообщений об обнаружении вирусов, о сбоях в работе средств антивирусной защиты и т.п.;

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

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

2.4. При осуществлении антивирусной защиты ИСПДн выполняются следующие обязательные мероприятия:

2.4.1. контроль съемных носителей информации на предмет наличия на них вредоносного программного обеспечения до начала работы с ними;

2.4.2. проверка всех электронных отправок на предмет наличия вредоносного программного обеспечения;

2.4.3. периодическая проверка на предмет наличия вредоносного программного

- обеспечения жестких магнитных дисков (не реже одного раза в неделю);
- 2.4.4. внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие вредоносного программного обеспечения;
- 2.4.5. восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.
- 2.5. Обновления баз данных средств антивирусной защиты в ИСПДн осуществляется в автоматическом режиме (не реже одного раза в сутки).
- 2.6. Установку и настройку антивирусного ПО осуществляет администратор безопасности в соответствии с эксплуатационной документацией на данное ПО.

### **3. Порядок действий при обнаружении вредоносного ПО.**

- 3.1. При обнаружении вредоносного программного обеспечения на съемных носителях, в электронных отправлениях или при посещении ресурсов сети Интернет пользователь каждой ИСПДн обязан:
  - 3.1.1. приостановить работу с источником угрозы (съемным носителем, электронным отправлением, Интернет-ресурсом), иные работы на автоматизированном рабочем месте не запрещаются;
  - 3.1.2. сообщить администратору безопасности об обнаружении вредоносного программного обеспечения;
  - 3.1.3. принять меры по локализации и удалению вредоносного программного обеспечения, рекомендованные администратором безопасности.
- 3.2. При обнаружении вредоносного программного обеспечения в процессе обработки информации, за исключением пункта 3.1, пользователь обязан:
  - 3.2.1. приостановить все работы на автоматизированном рабочем месте;
  - 3.2.2. сообщить администратору безопасности об обнаружении вредоносного программного обеспечения;
  - 3.2.3. принять меры по локализации и удалению вредоносного программного обеспечения, рекомендованные администратором безопасности.
- 3.3. Администратор безопасности по факту событий предусмотренных пунктами 3.1, 3.2 должен зарегистрировать вирусную атаку в журнале событий безопасности в соответствии с «Инструкцией по управлению событиями информационной безопасности».
- 3.4. При обнаружении вредоносного программного обеспечения на серверном или телекоммуникационном оборудовании, администратор безопасности обязан:
  - 3.4.1. немедленно сообщить ответственному за организацию обработки ПДн об обнаружении вредоносного программного обеспечения;
  - 3.4.2. принять меры по локализации и удалению вредоносного программного обеспечения, а также по выявлению источника и способа проникновения вредоносного программного обеспечения.
- 3.5. В случае невозможности удаления вредоносного программного обеспечения, 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 в ИСПДн ПДн.

### **4. Заключительные положения.**

- 4.1. Пользователи ИСПДн должны быть предупреждены об ответственности за невыполнение требований настоящей инструкции.
- 4.2. Пользователи ИСПДн должны быть ознакомлены с настоящей инструкцией до начала работы с ИСПДн под роспись. Обязанность ознакомления сотрудников с настоящей инструкцией лежит на ответственном за организацию обработки ПДн.
- 4.3. Сотрудники Организации несут ответственность за ненадлежащее исполнение или

неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

#### **5. Нормативно-правовые акты.**

- 5.1. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».
- 5.2. Постановление Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- 5.3. Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

### **Приложение №1**

#### **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. Начиная с Windows Vista, 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 (например: Kaspersky Virus Removal Tool или Kaspersky Rescue Disk).

### 3.3. Создайте копии зашифрованных файлов.

### 3.4. Попытайтесь восстановить файлы:

- Для пользователей [Windows 7](#);
- 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 NT/2000/XP:
  - Диск:\Documents and Settings\%UserName%\Application Data\
  - %USERPROFILE%\Local Settings\Application Data
- ОС Windows Vista/7/8:
  - Диск:\Users\%UserName%\AppData\Roaming\
  - %USERPROFILE%\AppData\Local

### 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 NT/2000/XP: %USERPROFILE%\Local Settings\Temporary Internet Files\
- ОС Windows Vista/7/8:
  - %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\
  - ..\temporary internet files\content.ie5\
  - ..\temporary internet files\content.ie5\???????\ (? -- a-z, 0-9)

### 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