УТВЕРЖДЕНА
приказом ГПОУ «УМК»
от 28.09.2016 № 62/а

ИНСТРУКЦИЯ

по организации антивирусной защиты в информационных системах персональных данных

Оглавление

1. Общие положения

1.1. Назначение документа

1.1.1. Инструкция по организации антивирусной защиты в информационных системах персональных данных (ИСПДн) ГПОУ «УМК» (далее – Учреждение) определяет порядок установки и настройки антивирусных средств (САВЗ), проведения антивирусного контроля и обновления баз САВЗ, а также порядок действий лиц, допущенных к автоматизированной обработке персональных данных (ПДн) в ИСПДн Учреждения (далее – пользователи ИСПДн), в случае обнаружения вредоносного программного обеспечения и их ответственность.

1.1.2. Целью настоящей инструкции является превентивная защита от несанкционированных вредоносных воздействий на информационные ресурсы, программное обеспечение и файлы ИСПДн компьютерными вирусами.

1.2. Область действия документа

1.2.1. Настоящая инструкция является руководящим документом администратора ИСПДн по противодействию вредоносному программному обеспечению и компьютерным вирусам.

1.2.2. Пользователи ИСПДн должны быть ознакомлены с разделом 5 настоящей инструкции под личную и предупреждены об ответственности за его нарушение.

1.2.3. Методическое руководство по обеспечению антивирусной защиты в ИСПДн осуществляется администратором ИСПДн.

1.3. Вступление в силу документа

1.3.1. Настоящая инструкция вступает в силу с момента ее утверждения директором Учреждения.

1.3.2. Изменения в настоящую инструкцию вносятся приказом директора Учреждения.

2. Установка и настройка САВЗ

2.1. Общие положения

2.1.1. На всех АРМ ИСПДн в обязательном порядке должны быть установлены, активированы и настроены должным образом САВЗ.

2.1.2. К использованию в ИСПДн допускаются только лицензионные САВЗ.

2.1.3. В установленных законодательством РФ случаях либо по мотивированному решению постоянно действующей комиссии по защите ПДн (далее – Комиссия) к использованию в ИСПДн допускаются только сертифицированные ФСТЭК России САВЗ.

2.1.4. При установке, настройке, обновлении, удалении и администрировании САВЗ в дополнение к настоящей инструкции необходимо руководствоваться эксплуатационной и технической документацией САВЗ.

2.1.5. Правилами эксплуатации, руководством администратора либо приложением к сертификату сертифицированных САВЗ может быть установлен особый порядок установки, настройки, эксплуатации и обновления (в т. ч. запрет на обновление программных модулей), а также перечень источников обновления. Указанные в данных документах требования подлежат обязательному исполнению вне зависимости от их несоответствия требованиям настоящей инструкции.

2.2. Порядок установки и настройки САВЗ

2.1.6. Установка, настройка и администрирование САВЗ на АРМ ИСПДн осуществляется администратором ИСПДн централизованно[1], с использованием консоли (сервера) администрирования САВЗ.

2.1.7. САВЗ устанавливаются при вводе АРМ в эксплуатацию или при их замене.

2.1.8. После установки САВЗ на АРМ ИСПДн проводится проверка соответствия контрольных сумм установленных файлов, на их соответствие заявленным в технической документации САВЗ (в случае установки сертифицированных САВЗ).

2.1.9. Доступ пользователей ИСПДн к настройке САВЗ должен быть заблокирован или защищен паролем.

2.1.10. Запуск САВЗ должен осуществляться автоматически, вместе с загрузкой операционной системы.

2.1.11. При обнаружении зараженных файлов САВЗ должны проводить их лечение, а при невозможности лечения – удаление.

2.1.12. САВЗ должны обеспечивать:

- защиту АРМ и серверов ИСПДн от вирусов и вредоносных программ, в том числе:
  - автоматическое уведомление об обнаруженных инфицированных, неизлечимых или подозрительных объектах;
  - защиту от вирусов, троянских программ, червей, шпионских программ, рекламного программного обеспечения, руткитов и др.;
  - применение эвристических и сигнатурных методов детектирования угроз;
  - проактивную защиту от неизвестных угроз;
  - проверку оперативной памяти, загрузочных секторов, жестких дисков, съемных носителей, отдельных файлов;
  - непрерывный контроль вирусной активности;
  - нейтрализацию (или удаление) программного кода компьютерного вируса в зараженных объектах.
- централизованное управление (установку, настройку, удаление, обновление и т. д.);
- самозащиту от попыток выключения со стороны вирусов и вредоносных программ;
- контроль целостности передаваемой между компонентами САВЗ информации;

[1] В случае отсутствия такой возможности (САВЗ не имеет консоли (сервера) администрирования или АРМ не подключено к локальной вычислительной сети) необходимо проводить установку, настройку и администрирование индивидуально на каждом АРМ (сервере) ИСПДн

- регулярные (полные) и разовые (быстрые) антивирусные проверки (сканирования);
- возможность помещения зараженных файлов в изолированную среду (карантин);
- защиту при работе в сети, в том числе:
    - проверку файлов, веб-страниц, почтовых сообщений (передаваемых по протоколам SMTP/POP3/NNTP/IMAP4);
    - защиту от спама и фишинга в почтовых программах.
- регулярные и экстренные обновления программных модулей, эвристического ядра и сигнатурных баз;
- формирование статистических отчетов о хакерских атаках и попытках заражений.

3. Антивирусный контроль

3.1. Общие положения

3.1.1. Администратор ИСПДн осуществляет повседневный контроль над функционированием САВЗ в ИСПДн.

3.1.2. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, сообщения электронной почты и т.д.), получаемая или передаваемая по телекоммуникационным каналам, а также данные на машинных носителях информации (МНИ).

3.2. Порядок проведения антивирусного контроля

3.2.1. Все программное обеспечение, устанавливаемое на АРМ ИСПДн, предварительно проверяется на наличие вредоносных программ.

3.2.2. Ежемесячно на всех АРМ ИСПДн проводится полная антивирусная проверка САВЗ (загрузочные сектора, локальные жесткие диски, резервные хранилища файлов, помещенных на карантин и др.).

3.2.3. Все МНИ при подключении к ИСПДн проверяются САВЗ на наличие вредоносных программ (быстрая проверка).

3.2.4. При возникновении подозрения в заражении АРМ ИСПДн компьютерным вирусом (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИСПДн самостоятельно (при необходимости совместно с администратором ИСПДн) проводит внеочередную полную антивирусную проверку АРМ ИСПДн.

3.2.5. В некоторых случаях для определения факта наличия вредоносных программ пользователь ИСПДн может обратиться к администратору ИСПДн.

4. Обновление баз САВЗ

4.1. Обновление баз САВЗ на АРМ ИСПДн, не подключенных к ЛВС

4.1.1. Обновление баз САВЗ на АРМ ИСПДн, не имеющих подключения к локальной вычислительной сети (ЛВС) Учреждения и сетям связи общего пользования, осуществляется администратором ИСПДн вручную с использованием учтенных МНИ, в обязательном

порядке проверяемых САВЗ перед их использованием или подключением к АРМ ИСПДн, еженедельно.

4.1.2. Обновление баз САВЗ на АРМ ИСПДн, не имеющих подключения к ЛВС Учреждения, но подключенных к сетям связи общего пользования, осуществляется ежедневно в установленное время с официального сервера обновлений производителя САВЗ.

4.2. Обновление баз САВЗ на АРМ ИСПДн, подключенных к ЛВС

4.2.1. При централизованном управлении антивирусной защитой консоль (сервер) администрирования ежедневно в установленное время обновляет базы САВЗ с официального сервера обновлений производителя САВЗ и размещает их в общедоступное для АРМ ИСПДн хранилище.

4.2.2. Обновление баз САВЗ на АРМ ИСПДн, подключенных к ЛВС Учреждения, осуществляется ежедневно в установленное время из общедоступного хранилища консоли (сервера) администрирования.

4.2.3. При локальном управлении антивирусной защитой роль консоли (сервера) администрирования по обновлению баз САВЗ и их размещению в общедоступное хранилище выполняет САВЗ, установленное на одном из АРМ ИСПДн. В этом случае, обновление баз САВЗ на остальных АРМ ИСПДн происходит в аналогичном п. 4.2.2 порядке.

5. Действия при обнаружении вредоносных программ

5.1. Общие положения

5.1.1. Пользователям ИСПДн запрещается отключать САВЗ, а также самостоятельно вносить изменения в их настройки.

5.1.2. В случае возникновения ошибок обновления или функционирования САВЗ, пользователь ИСПДн обязан обратиться к администратору ИСПДн.

5.2. Порядок действий при обнаружении вредоносных программ

5.2.1. В случае обнаружения при проведении антивирусной проверки (или антивирусного контроля) вредоносных программ и (или) компьютерного вируса пользователь ИСПДн обязан:

1) приостановить все операции, связанные с обработкой информации на АРМ;
2) немедленно поставить в известность о факте обнаружения вредоносных программ и (или) компьютерного вируса администратора ИСПДн, владельцев зараженных или поврежденных вредоносными программами и (или) компьютерными вирусами файлов, а также смежные структурные подразделения Учреждения, использующие эти файлы в работе;
3) выполнить лечение зараженных файлов, а при невозможности лечения совместно с их владельцами и администратором ИСПДн принять решение об их удалении (помещении на карантин).

6. Сводный перечень регулярных мероприятий

6.1. Сводный перечень регулярных мероприятий, вводимых настоящим документом, представлен в таблице 1, в которой для каждого мероприятия указаны:

- наименование;
- периодичность выполнения;
- номер пункта настоящего документа, вводящего мероприятие;
- ответственное за выполнение мероприятия лицо.

Таблица 1 - Сводный перечень регулярных мероприятий

Наименование мероприятия	Периодичность	Пункт	Ответственный
Полная антивирусная проверка всех АРМ ИСПДн (в автоматическом режиме)	Ежемесячно	3.2.2	Администратор ИСПДн
Обновление баз САВЗ на АРМ ИСПДн не имеющих подключения к ЛВС Учреждения и к сетям связи общего пользования	Еженедельно	4.1.1	Администратор ИСПДн

7. Ответственность

7.1. Ответственность за поддержание установленного настоящей инструкцией порядка проведения антивирусного контроля, обновления баз САВЗ, а также за получение новых лицензионных ключей при истечении срока действия текущих лицензий и ознакомление пользователей ИСПДн с настоящей инструкцией несет администратор ИСПДн.

7.2. Пользователи ИСПДн и Администратор ИСПДн несут персональную ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей инструкцией.