

Частное образовательное учреждение  
дополнительного профессионального образования  
«Промбезопасность»

«Утверждаю»

Директор ЧОУ ДПО «Промбезопасность»



С.М. Аленин

2017 г.

## ИНСТРУКЦИЯ по организации антивирусной защиты

г. Иваново  
2017 год

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных ЧОУ ДПО «Промбезопасность» (далее – Учебный центр).

Настоящая Инструкция предназначена для уполномоченных работников Учебного центра, а также должностного лица, выполняющего функции администратора безопасности информации (далее - администратор безопасности), и пользователей, осуществляющих обработку персональных данных в Учебном центре.

В целях обеспечения защиты от деструктивных действий компьютерных вредоносных программ производится антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники, в том числе получаемая на внешних носителях из сторонних организаций.

Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на ресурсы информационных систем.

Вредоносная программа способна выполнять ряд функций, в том числе:

- скрывать признаки своего присутствия в программной среде рабочей станции;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искашать произвольным образом, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Основными задачами системы обеспечения антивирусной защиты являются:

- исключение или существенное затруднение противоправных действий в отношении ИСПДн Учебного центра как носителей защищаемой информации;
- обеспечение условий для устойчивой бесперебойной работы объектов, сетей передачи данных.

Объектом защиты от воздействия вредоносных программ являются вычислительные структуры и транспортная среда передачи данных ИСПДн Учебного центра.

Обеспечение антивирусной защиты включает:

- регулярные профилактические работы;
- анализ ситуации проявления вредоносных программ и причины их появления;
- уничтожение вредоносных программ на автоматизированных рабочих местах (АРМ);
- принятие мер по предотвращению причин появления вредоносных программ.

Для выполнения требований по антивирусной защите ИСПДн Учебного центра используется специализированное программное обеспечение (ПО), обеспечивающее надежную ежедневную автоматическую антивирусную защиту и контроль чистоты информационных массивов данных от вредоносных программ.

Организация работ по антивирусной защите и ответственность за сопровождение системы антивирусной защиты, а также ответственность за контроль установленного порядка антивирусной защиты возлагается на администратора безопасности.

Все процессы производятся в автоматическом режиме без участия пользователей и без помех для работы основного и специального ПО.

Процесс плановой полной проверки файловой системы рабочих станций пользователей ИСПДн Учебного центра проводится во время наименьшей нагрузки оборудования пользовательскими задачами.

Администратор безопасности осуществляют следующие действия:

- проведение периодического анализа и оценки ситуации антивирусной безопасности для контроля степени защищенности ИСПДн Учебного центра и выработки предложений по изменению и улучшению состояния дел;
- проверка соблюдения порядка обновления средств и баз данных антивирусной защиты;
- осуществление контроля за состоянием средств антивирусной защиты на рабочих станциях пользователей;
- осуществление контроля за соблюдением работниками требований антивирусной защиты;
- обеспечение контроля за соблюдением требований при работе с сетью Интернет, а также за характером и объемом трафика, получаемого из сети Интернет, и его соответствия служебной необходимости;
- проведение служебных расследований по фактам обнаружения вредоносных программ, повлекших неустойчивую работу и (или) разрушение технологического оборудования, локально-вычислительной сети и информационных массивов Учебного центра;
- организацию мероприятий по улучшению антивирусной защиты Учебного центра.

Устанавливаемое (изменяемое) ПО в ИСПДн Учебного центра предварительно проверяется представителем эксплуатирующего подразделения на отсутствие вредоносных программ. Непосредственно после установки (изменения) ПО администратор безопасности выполняет антивирусную проверку на рабочих станциях ИСПДн Учебного центра.

При возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) администратор безопасности проводит внеочередной антивирусный контроль рабочих станций ИСПДн Учебного центра.

Для пользователей рабочих станций ИСПДн Учебного центра запрещена возможность изменения настроек и параметров защиты антивирусных средств на своей рабочей станции, эти действия производят администратор безопасности с помощью средств централизованного управления или вручную.

Результаты расследования причин появления и последствий воздействия вредоносных программ на рабочую станцию докладываются директору Учебного центра с предложениями по принятию мер, предотвращающих в будущем повторение подобных фактов.

## **2. ТРЕБОВАНИЯ К АНТИВИРУСНОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ**

Применение только лицензионного антивирусного ПО.

Возможность обнаружения как можно большего числа известных вредоносных программ, в том числе вирусов, деструктивного кода (макро-вирусы, объектов ActiveX, апплетов языка Java и т.п.), а также максимальная готовность быстрого реагирования на появление новых видов вирусных угроз.

Исчерпывающий список защищаемых точек (почтовые серверы, автоматизированные рабочие места и т.д.) возможного проникновения вредоносных программ.

Обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком антивирусного ПО.

Возможность автоматического распространения обновлений антивирусных баз на каждую рабочую станцию в ИСПДн Учебного центра.

Соответствие системных требований антивирусного ПО платформам, характеристикам и комплектации применяемой вычислительной техники.

Надежность и работоспособность антивирусного ПО в любом из предусмотренных режимов работы, по возможности, в русскоязычной среде.

Наличие документации, необходимой для практического применения и освоения антивирусного ПО, на русском языке.

## **3. МЕРОПРИЯТИЯ ПО ШТАТНОМУ УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ**

В штатном режиме работы системы антивирусной администратор безопасности выполняет:

- установку средств антивирусной защиты на все объекты антивирусной защиты, добавляемые в средства защиты ИСПДн Учебного центра, в порядке, описанном в эксплуатационной документации;
- необходимые обновления версий средств антивирусной защиты на объектах антивирусной защиты;
- контроль над выполнением задач постоянной защиты;
- настройку автоматических проверок объектов антивирусной защиты не реже одного раза в неделю с целью профилактики;
- непрерывный мониторинг информационного обмена в средствах защиты ИСПДн Учебного центра с целью выявления проявлений программно-математических воздействий;
- обработку сведений, поступающих от средств антивирусной защиты;
- формирование сводных отчетов о работе средств антивирусной защиты, инцидентах и проч.;
- обработку отчетов о состоянии логических сетей;
- формирование отчетов о работе средств антивирусной защиты логической сети.

Процесс управления системой антивирусной защиты включает в себя следующие действия администратора безопасности:

- внесение изменений в политику антивирусной защиты;
- управление средствами антивирусной защиты, входящими в состав системы антивирусной защиты;
- мониторинг событий, информация о которых поступает от средств антивирусной защиты с объектов защиты.

В обязанности администратора безопасности входит проведение мероприятий, обеспечивающих возможность анализа результатов работы средств системы антивирусной защиты:

- разработка отчетов о работе средств антивирусной защиты;
- разработка сводных отчетов о работе средств антивирусной защиты, инцидентах и пр. за месяц.

В отчетах о состоянии системы антивирусной защиты отражается следующая информация:

- количество обнаруженных вредоносных программ за данный период;
- наиболее активные обнаруженные вредоносные программы;
- объекты, где наблюдается наибольшая частота обнаружения вредоносных программ;
- список зараженных объектов.

#### **4. МЕРОПРИЯТИЯ ПО НЕШТАТНОМУ УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ**

В случае заражения рабочих станций вредоносными программами администратор безопасности выполняет следующие действия:

- централизованно обновляет антивирусные базы всех объектов антивирусной защиты;
- проверяет состояние всех объектов антивирусной защиты, наличие зараженных рабочих станций в случае обнаружения пораженных узлов;
- оперативно принимает меры по предотвращению распространения заражения вредоносными программами и при необходимости отключает от сети зараженную рабочую станцию;
- проводит действия, направленные на устранение вредоносной программы на всех пораженных узлах ИСПДн Учебного центра;
- по завершении мероприятий по устраниению последствий заражения восстанавливает работоспособность рабочей станции и передает ее ответственному пользователю.

## **5. УНИЧТОЖЕНИЕ ВРЕДОНОСНЫХ ПРОГРАММ**

Уничтожение вредоносных программ выполняется администратором безопасности.

Если вредоносная программа поразила какие-либо программы, то уничтожение вредоносной программы выполняется путем уничтожения программы на жестком диске либо на ином магнитном носителе. После уничтожения зараженной программы восстанавливают программу, используя резервную копию.

Если вредоносная программа поразила файлы, то вредоносная программа уничтожается либо путем стирания этих файлов, либо путем использования специального "лечащего" режима антивирусного ПО. Использование "лечащего" режима не дает полной гарантии восстановления файла, поэтому после "лечения" необходима проверка восстановления данного файла. "Лечащие" программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы или файла с данными либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

В любом случае после уничтожения вредоносных программ и восстановления зараженных программ и файлов с данными еще раз выполняется проверка наличия вредоносных программ, используя антивирусную программу с установленными последними обновлениями. Перед повторной проверкой производится перезагрузка рабочей станции через выключение и последующее их включение. Если повторная проверка не выявила вредоносных программ, то можно быть уверенным в их отсутствии.

## **6. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ**

Организация мероприятий по централизованной антивирусной защите ИСПДн Учебного центра возлагается на администратора безопасности.

Администратор безопасности несет ответственность за формирование политики антивирусной защиты, организацию своевременной инсталляции средств антивирусной защиты информации и централизованное обновление баз данных вирусных описаний на комплексе программно-технических средств ИСПДн Учебного центра.

Выполнение технических мероприятий по централизованной антивирусной защите в ИСПДн Учебного центра производится непосредственно администратором безопасности.

Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации и требований настоящей Инструкции в части защиты ИСПДн Учебного центра несут пользователи, за которыми закреплены соответствующие рабочие станции ИСПДн Учебного центра.