Приложение № 3
УТВЕРЖДЕНО
приказом МБУ «КЦСОН» ТГО
от 16.01.2020г. № 9-А

ИНСТРУКЦИЯ

По проведению антивирусного контроля в информационной системе персональных данных Муниципального бюджетного учреждения «Комплексный центр социального обслуживания населения» Тайгинского городского округа

1. Общие положения.

1.1. Настоящая Инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных МБУ «КЦСОН» ТГО (далее - Учреждение).

1.2. Настоящая Инструкция предназначена для должностного лица, выполняющего функции уполномоченного лица безопасности информации, и пользователей, осуществляющих обработку персональных данных в Учреждении.

1.3. В целях обеспечения защиты от деструктивных воздействий 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.

1.4. 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 (сервера);

- обладать способностью к само дублированию, 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);

- искажать 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.

1.6. Основными задачами системы обеспечения антивирусной защиты являются:

- исключение или существенное затруднение противоправных действий в отношении ИСПДн Учреждения как носителей защищаемой информации;

- обеспечение условий для устойчивой бесперебойной работы объектов, сетей передачи данных.

1.7. Обеспечение антивирусной защиты включает:

- регулярные профилактические работы;

- анализ ситуации проявления вредоносных программ и причины их появления;

- уничтожение вредоносных программ на автоматизированных рабочих местах (АРМ) (серверах);

- принятие мер по предотвращению причин появления вредоносных программ.

1.8. Организация работ по антивирусной защите и ответственность за сопровождение системы антивирусной защиты возлагается на техника-программиста

1.9. Работники, на которых возлагается ответственность по антивирусной защите, имеют полноправный доступ ко всем АРМ, серверам и другому оборудованию ИСПДн Учреждения.

1.10. 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 и серверов ИСПДн Учреждения проводится во время наименьшей нагрузки оборудования пользовательскими задачами.

1.11. Работник, отвечающий за ежедневное сопровождение антивирусной защиты, обладает необходимыми практическими навыками и теоретическими знаниями по данному вопросу. В основные обязанности по антивирусной защите входит:

- проведение периодического анализа и оценки ситуации по обеспечению антивирусной безопасности для контроля степени защищенности ИСПДн 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 серверах, рабочих ПК;

- осуществление контроля за соблюдением работниками требований по обеспечению 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;

Ответственный работник осуществляют следующие действия:

- контроль и анализ еженедельных отчетов по состоянию антивирусной защиты;

- проведение служебных расследований по фактам обнаружения вредоносных программ, повлекших неустойчивую работу и (или) разрушение технологического оборудования, локально-вычислительной сети и информационных систем

- организацию мероприятий по улучшению антивирусной защиты Учреждения

1.12. Устанавливаемое (изменяемое) ПО в ИСПДн Учреждения предварительно проверяется представителем эксплуатирующего подразделения на отсутствие вредоносных программ. Непосредственно после установки (изменения) ПО, администратор безопасности либо уполномоченный работник подразделения ИТ выполняет антивирусную проверку на рабочих станциях и серверах ИСПДн Учреждения

1.13. 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, либо уполномоченный работник подразделения ИТ проводит внеочередной антивирусный контроль рабочих станций (серверов) ИСПДн Учреждения

1.18. Для пользователей рабочих станций ИСПДн Учреждения запрещена возможность изменения настроек и параметров защиты антивирусных средств на своей рабочей станции, эти действия производит администратор безопасности или уполномоченный работник подразделения ИТ с помощью средств централизованного управления или вручную.

1.19. По факту появления и проникновения вредоносных программ, повлекших неустойчивую работу и (или) вывод из строя технологического оборудования, локально-вычислительной сети и информационных массивов

Учреждения, проводится служебное расследование Группой реагирования на инциденты информационной безопасности.

1.20. Результаты расследования причин появления и последствий воздействия вредоносных программ на рабочую станцию (сервер) докладываются руководителю Отдела информационной безопасности территориального органа Учреждения с предложениями по принятию мер, предотвращающих в будущем повторение подобных фактов.

2. Требования к антивирусному программному обеспечению.

2.1. Применение только лицензионного антивирусного ПО.

2.2. 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.

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

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

2.5. Возможность автоматического распространения обновлений антивирусных баз на каждую рабочую станцию (сервер) в ИСПДн Учреждения

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

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

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

3. Мероприятия по штатному управлению средствами антивирусного контроля.

3.1. В штатном режиме работы системы антивирусной уполномоченный работник подразделения ИТ выполняет:

- установку средств антивирусной защиты на все объекты антивирусной защиты, добавляемые в средства защиты ИСПДн Учреждения в порядке, описанном в эксплуатационной документации;

- контроль наличия связи между сервером администрирования и защищаемыми объектами;

- 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;

- контроль актуальности версий антивирусных баз и модулей сканирования ПО сервера администрирования;

- непрерывный мониторинг информационного обмена в средствах защиты ИСПДн Учреждения 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.

3.2. Процесс управления системой антивирусной защиты включает в себя следующие действия администратора безопасности либо уполномоченного работника подразделения ИТ:

- 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.

3.3. В обязанности администратора безопасности либо уполномоченного работника подразделения ИТ 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.

4.1. В случае заражения рабочих станций (серверов) вредоносными программами администратор безопасности выполняет следующие действия:

- централизованно обновляет антивирусные базы сервера администрирования и 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 зараженный ПК

- проводит действия, направленные на устранение вредоносной программы на всех пораженных узлах ИСПДн Учреждения;

- по завершении мероприятий по устранению последствий заражения восстанавливает работоспособность рабочей станции и передает ее ответственному пользователю.

4.2. Все или часть вышеперечисленных мероприятий может быть делегирована уполномоченному работнику подразделения ИТ.

5. Уничтожение вредоносных программ.

5.1. Уничтожение вредоносных программ выполняется уполномоченным работником подразделения ИТ.

5.2. 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 ее резервную копию.

5.3. 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.

5.4. 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 сервера или 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.

6.1. Организация мероприятий по централизованной антивирусной защите ИСПДн Учреждения возлагается на техника -программиста

6.2. Техник -программист 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 Учреждения

6.3. Выполнение технических мероприятий по централизованной антивирусной защите в ИСПДн Учреждения производится непосредственно администратором безопасности либо делегируется уполномоченному работнику подразделения ИТ.

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