СОГЛАСОВАНО
Протокол заседания ПК
от 01.09.2022г. № б/н
Председатель ПК

_____ Раздьяконов С.Ю.

Финагина О. В.
Подписано цифровой подписью: Финагина О. В.
Дата: 2022.11.22 14:41:23 +03'00'

УТВЕРЖДАЮ
Директор
Государственного бюджетного общеобразовательного учреждения средней общеобразовательной школы №174 Центрального района Санкт-Петербурга
_____О.В. Финагина
Введено в действие с 01.09.2019 г.
приказом от 01.09.2022 г.№____

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 174 ИМЕНИ И. К. БЕЛЕЦКОГО ЦЕНТРАЛЬНОГО РАЙОНА САНКТ-ПЕТЕРББУРГА

ИНСТРУКЦИЯ
по организации антивирусной защиты информационных систем персональных данных в ГБОУ школа №174 Центрального района Санкт-Петербурга

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных ГБОУ школа №174 Центрального района Санкт-Петербурга (далее- ОУ).

1.3. Действие настоящей Инструкции распространяется на всех сотрудников ОУ, имеющих доступ к информационным системам, сетям и персональным данным.

1.4. 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.

1.5. 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 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);
- 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 ОУ как носителей защищаемой информации;

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

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

1.8. Обеспечение антивирусной защиты включает:

- регулярные профилактические работы;

- анализ ситуации проявления вредоносных программ и причины их появления;

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

- принятие мер по предотвращению причин появления вредоносных программ.

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

1.10. Организация работ по антивирусной защите и ответственность за сопровождение системы антивирусной защиты возлагается на сотрудника ОУ выбранного директором.

1.11. Ответственность за контроль установленного порядка антивирусной защиты возлагается на заместителя директора по УВР.

1.12. Периодический контроль состояния антивирусной защиты ИСПДн ОУ возлагается на заместителя директора по УВР.

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

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

1.15. Работник, отвечающий за регулярное 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 антивирусной безопасности для контроля степени защищенности ИСПДн ОУ 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 сервере, 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 администрации;

- организацию мероприятий по улучшению антивирусной защиты.

1.16. 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.) проводится внеочередной антивирусный контроль рабочих станций (серверов) ИСПДн ОУ.

1.18. Для пользователей ИСПДн ОУ запрещена возможность изменения настроек и параметров защиты антивирусных средств.

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 администрации, проводится служебное расследование.

1.20. Результаты расследования причин появления и последствий воздействия вредоносных программ докладываются руководителю ОУ.

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, а также максимальная готовность быстрого реагирования на появление новых видов вирусных угроз.

2.3. Исчерпывающий список защищаемых точек возможного проникновения вредоносных программ.

2.4. Возможность автоматического распространения обновлений антивирусных баз в ИСПДн ОУ.

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

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

3. МЕРОПРИЯТИЯ ПО ШТАТНОМУ УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ

3.1. В штатном режиме работы системы антивирусной безопасности выполняется:

- установка средств антивирусной защиты на все объекты антивирусной защиты в ОУ;

- необходимые обновления версий средств антивирусной защиты на объектах антивирусной защиты;

- контроль над выполнением задач постоянной защиты;

- контроль актуальности версий антивирусных баз;

4. МЕРОПРИЯТИЯ ПО НЕШТАТНОМУ УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ

4.1. В случае заражения рабочих станций (серверов) вредоносными программами заместитель директора по УВР 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;

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

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

5. УНИЧТОЖЕНИЕ ВРЕДОНОСНЫХ ПРОГРАММ

5.1. Уничтожение вредоносных программ выполняется заместителем директора по УВР.

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.

6. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ

6.1. Организация мероприятий по централизованной антивирусной защите ИСПДн ОУ возлагается на заместителя директора по УВР.