Приложение 2
к приказу директора
ГБПОУ КК УТМиПТ
от 27.03.2024 г. № 66

ПОЛИТИКА
антивирусной защиты информации государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

1. Общие положения

1.1. Настоящая политика антивирусной защиты информации (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация) определяет процедуры, направленные на защиту информационных систем образовательной организации от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения.

1.2. Настоящая Политика разработана в соответствии с:

1.2.1 приказом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.2.2 приказом Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

1.2.3 методическим документом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

1.3. Подсистема антивирусной защиты информации является одной из составляющих системы защиты информации образовательной организации.

1.4. Объектами защиты от воздействия вредоносных программ являются следующие компоненты информационных систем образовательной организации:

1.4.1 автоматизированные рабочие места пользователей (далее – АРМ) информационных систем;

1.4.2 сервера информационных систем (в том числе почтовые, интернет-шлюзы, прокси-сервера и другие);

1.4.3 мобильные технические средства;

1.4.4 съемные носители информации;

1.4.5 иные точки доступа в информационные системы, подверженные внедрению (заражению) вредоносными компьютерными программами (вирусами).

1.5. Защита компонентов информационных систем от компьютерных вирусов осуществляется комплексом организационных мероприятий и технических мер, включающем:

1.5.1 регулярные профилактические работы;

1.5.2 анализ ситуации проявления вредоносных программ и причины их появления;

1.5.3 уничтожение вредоносных программ на АРМ, серверах, мобильных технических средства информационных систем и на используемых съемных носителях информации;

1.5.4 принятие мер по предотвращению причин появления вредоносных программ.

1.6. Технические меры, направленные на защиту информационных систем от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения, реализуются за счет применения в составе подсистемы антивирусной защиты информации соответствующих антивирусных средств, удовлетворяющих установленным требованиям.

1.7. Реализацией комплекса мероприятий и мер по антивирусной защите занимается Администратор информационной безопасности образовательной организации.

2. Организация мероприятий по антивирусной защите информации

2.1. К использованию допускаются только лицензионные средства антивирусной защиты информации, имеющие действующие сертификаты соответствия ФСТЭК России, предъявляемые к средствам антивирусной защиты, приобретенные у разработчиков (официальных поставщиков) данных средств.

2.2. Установка средств антивирусной защиты информации на автоматизированные рабочие места и сервера должна осуществляться только с сертифицированных ФСТЭК России дистрибутивов, приобретенных у разработчиков (официальных поставщиков) данных средств.

2.3. Средства антивирусной защиты информации должны использоваться на всех автоматизированных рабочих местах и серверах информационных систем и обеспечивать выполнение следующих требований:

2.3.1 возможность обнаружения как можно большего числа известных вредоносных программ, в том числе вирусов, деструктивного кода (макровирусов, объектов ActiveX, апплетов языка Java и других), а также максимальную готовность быстрого реагирования на появление новых видов вирусных угроз;

2.3.2 своевременное уведомление о необходимости обновления антивирусных баз и их последующее обновление из доверенных источников.

Контроль целостности обновлений антивирусных баз должен обеспечиваться функционалом антивирусного средства;

2.3.3 возможность автоматического распространения обновлений антивирусных баз на каждую рабочую станцию и (или) сервер;

2.3.4 обеспечивать соответствие системных требований средства к платформам, характеристикам и комплектации применяемой вычислительной техники;

2.3.5 иметь документацию, необходимую для практического применения и освоения средства, на русском языке;

2.3.6 обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком средства.

2.4. При использовании средств антивирусной защиты информации должны выполняться следующие организационные мероприятия:

2.4.1 запрет использования посторонних (неучтенных) съемных носителей информации при работе в информационных системах;

2.4.2 запрет передачи съемных носителей информации посторонним лицам;

2.4.3 запрет запуска программ с внешних съемных носителей информации при работе в информационных системах.

2.5. При функционировании средств антивирусной защиты информации на компонентах информационных систем обязательно выполнение следующих требований:

2.5.1 антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы и другие), получаемая и передаваемая посредством каналов связи (в том числе по электронной почте), а также съемных носителей информации (CD/DVD-диски, флэш-накопители и тому подобное);

2.5.2 определение автоматической реакции средства антивирусной защиты информации при обнаружении компьютерных вирусов и другого вредоносного программного обеспечения;

2.5.3 систематическая проверка содержимого дисков АРМ, серверов;

2.5.4 проверка в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных носителей информации, сетевых подключений (в том числе к сетям общего пользования) и других внешних источников) при загрузке, открытии или исполнении таких файлов;

2.5.5 поддержание антивирусных баз в актуальном состоянии и их своевременное распространение на АРМ и сервера информационных систем;

2.5.6 запрет деактивации средств антивирусной защиты информации пользователями информационных систем;

2.5.7 деактивация средств антивирусной защиты информации на АРМ и серверах информационных систем только для проведения профилактических мероприятий и по согласованию с администратором информационной безопасности;

2.5.8 оповещение администратора информационной безопасности и в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов).

3. Ответственность за исполнение положений настоящей Политики

3.1. Ответственность за исполнение положений настоящей Политики возлагаются на всех работников образовательной организации, осуществляющих работу на средствах вычислительной техники.

3.2. Пользователи информационных систем образовательной организации:

3.2.1 не должны каким-либо образом препятствовать функционированию (в том числе обновлению) средства антивирусной защиты информации и принимать попытки его деактивации;

3.2.2 должны перед получением или передачей информации осуществить ее проверку на предмет наличия компьютерных вирусов и другого вредоносного программного обеспечения. Контроль исходящей информации необходимо проводить непосредственно перед ее отправкой и (или) записью на съемный носитель, а входящей – непосредственно после ее приема перед разархивированием;

3.2.3 при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и тому подобное) должны провести внеочередной антивирусный контроль АРМ и при необходимости привлечь Администратора информационной безопасности для определения факта наличия или отсутствия компьютерного вируса;

3.2.4 при невозможности самостоятельно устранить выявленное средствами антивирусной защиты информации вредоносное программное обеспечение – должны приостановить работу и незамедлительно уведомить Администратора информационной безопасности;

3.2.5 по факту обнаружения зараженных вирусом файлов должны составить служебную записку администратору информационной безопасности, в которой необходимо указать предположительный источник (отправителя, владельца и так далее) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные мероприятия по его нейтрализации.

3.3. Администратор информационной безопасности должен:

3.3.1 руководствоваться в своей работе настоящей Инструкцией;

3.3.2 осуществлять функции по организации антивирусного контроля в информационных системах образовательной организации;

3.3.3 содействовать пользователям информационных систем в устранении последствий вирусных заражений;

3.3.4 давать пояснения пользователям информационных систем по вопросам функционирования средств антивирусной защиты информации и при необходимости проводить персональные инструктажи;

3.3.5 осуществлять планирование и реализацию контрольных мероприятий по проверке степени выполнения положений настоящей Политики работниками образовательной организации;

3.3.6 организовывать процесс управления инцидентами информационной безопасности в части положений настоящей Политики (в соответствии с Политикой управления событиями безопасности информации).

3.4. Лица, виновные в нарушении положений настоящей Политики, могут быть привлечены к дисциплинарной, материальной, гражданской, правовой и административной ответственности.