Муниципальное бюджетное учреждение дополнительного образования Центр «Эдельвейс»

УТВЕРЖДАЮ
Директор
МБУ ДО Центра «Эдельвейс»
_____/Т.В. Марина/
(Подпись) (Ф.И.О.)
Приказ 67а «11» 09 2019 г.

ПОЛОЖЕНИЕ
об антивирусном контроле в МБУ ДО Центре «Эдельвейс»

1. Общие положения

1.1. Настоящее Положение разработано во исполнение Политики информационной безопасности **МБУ ДО Центр «Эдельвейс»** в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами и устанавливает порядок проведения антивирусного контроля в **МБУ ДО Центре «Эдельвейс»** (далее ОУ).

1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в ОУ.

1.3. Требования настоящего Положения распространяются на всех работников подразделений, использующих в работе компьютерную технику (включая работу в локальной сети ОУ) и должны применяться для всех средств компьютерной техники, эксплуатируемой в ОУ.

1.4. Организационное обеспечение мероприятий антивирусного контроля и контроль за действиями пользователей возлагается на системного администратора ОУ.

2. Основные термины, сокращения и определения

АС – автоматизированная система ОУ – система, обеспечивающая хранение, обработку, преобразование и передачу информации ОУ с использованием компьютерной и другой техники.

Компьютерный вирус программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

Зараженная программа - это программа, содержащая внедренную в нее программу-вирус.

3. Организация системы антивирусного контроля

3.1. Целью мероприятий по антивирусному контролю является предотвращение потерь информации в АС ОУ.

3.2. Задачами антивирусной защиты являются:

- определение состава и регламента запуска антивирусных диагностических средств, регламента их ревизии и обновления;
- проведение профилактических работ с применением антивирусных диагностических средств;
- непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации АС ОУ.

3.3. Для проведения мероприятий по предотвращению вирусного заражения приказом по ОУ назначается ответственный за антивирусный контроль. Ответственный за антивирусный контроль в своей работе руководствуются настоящим Положением, нормативными актами по защите информации, и другими документами.

3.4. К использованию в ОУ допускаются только лицензионные антивирусные средства, централизованно закупленные отделом информационных технологий у разработчиков (поставщиков) указанных средств, рекомендованные к применению системным администратором ОУ.
3.5. Установка средств антивирусной защиты и настройка их параметров в соответствии с руководствами по применению конкретных антивирусных средств на компьютерах в ОУ осуществляется системным администратором.
3.6. Обновление антивирусных баз должно производиться не реже 1 раза в сутки автоматически, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления обновление баз производится вручную с той же периодичностью.
3.7. Обязательному входному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация на съемных носителях и мобильных устройствах.
3.8. Файлы резервных копий, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.
3.9. Мероприятия по антивирусной защите на компьютерах в ОУ включают в себя:
- профилактика вирусного заражения;
- анализ ситуаций;
- применение средств антивирусной защиты;
- проведение расследований инцидентов связанных с вирусами.

4. Профилактика вирусного заражения

4.1. В целях исключения появления и распространения вирусов на рабочих станциях АС ОУ должны регулярно проводится профилактические мероприятия. К основным профилактическим работам и мероприятиям относятся:
- ежедневная автоматическая проверка наличия вирусов по расписанию;
- регулярная (не реже одного раза в квартал) выборочная проверка рабочих станций и серверов на наличие вирусов, даже при отсутствии внешних проявлений вирусов;
- проверка наличия вирусов на рабочих станциях, вернувшихся с ремонта (в том числе гарантийного) в сторонних организациях;
- создание резервной копии программного продукта сразу же после приобретения;
- установка защиты от записи на съемные носители информации, где это возможно;
- тщательная проверка всех поступающих и купленных программ и баз данных;
- ограничение доступа к компьютеру посторонних лиц.

4.2. Создание резервной копии программного продукта выполняется отделом информационных технологий, остальные профилактические работы и мероприятия выполняются ответственным за антивирусный контроль в ОУ.
4.3. При обнаружении вирусов на компьютере, работающем в локальной сети, проверке подлежат все компьютеры, включенные в эту сеть и работающие с общими данными и программным обеспечением.

5. Анализ ситуаций

5.1. При сообщении антивирусных программы о подозрении на наличие вирусов на рабочей станции, необходимо приостановить работу и немедленно известить об этом системного администратора ОУ, а также других пользователей и подразделения, использующие эти файлы в работе, если зараженные файлы являются совместно используемыми.
5.2. Анализ ситуации наличия вирусов выполняется ответственным за антивирусный контроль в ОУ. При анализе могут дополнительно использоваться специальное программное обеспечение для обнаружения вирусов.
5.3. В ходе анализа ситуации обязательно требуется определить источник заражения. Если источником заражения является съемный носитель либо другая рабочая станция ОУ, то необходимо проверить на наличие вирусов рабочую станцию - источник заражения. В случае

заражения через глобальную сеть Интернет или по электронной почте следует немедленно заблокировать ресурс или адрес электронной почты – источник заражения.
5.4. В случае обнаружения вирусного заражения расследование допущенных нарушений производится системным администратором на основании Регламента реагирования на инциденты информационной безопасности, утвержденного в Организации.

6. Применение средств антивирусной защиты

6.1. Уничтожение вирусов выполняется системным администратором ОУ.
6.2. После уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы.
6.3. В случае обнаружения, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусный контроль должен направить зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку.

7. Ответственность

7.1. Ответственность за выполнение мероприятий по антивирусной защите информации на ПК, эксплуатируемых подчиненными лицами в подразделении в соответствии с требованиями настоящего Положения, возлагается на руководителя подразделения.
7.2. Ответственность за выполнение мероприятий по антивирусной защите информации на ПК на рабочем месте в соответствии с требованиями настоящего Положения, возлагается на пользователя ПК.
7.3. Ответственность за проведение профилактических мероприятий по обеспечению антивирусной защиты в АС ОУ, а также уничтожение выявленных вирусов возлагается на системного администратора ОУ.
7.4. Периодический контроль за состоянием антивирусной защиты в АС ОУ, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящего Положения сотрудниками подразделений ОУ системный администратор ОУ.
7.5. Сотрудники ОУ, нарушившие требования настоящего документа, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации.

Инструкция пользователя по антивирусной защите МБУ ДО Центр «Эдельвейс»

Характерные проявления вирусов

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Основные источники вирусов:

- съемный носитель (дискета, флеш-карта, CD-ROM, DVD-ROM, мобильное дисковое устройство) на котором находятся зараженные вирусом файлы;
- компьютерная сеть, в том числе система электронной почты и Интернет;
- жесткий диск, на который попал вирус в результате работы с зараженными программами.

Пользователь обязан:

- ежедневно при начальной загрузке рабочей станции убедиться в загрузке антивирусного программного обеспечения и в случае его отсутствия уведомить ответственного за антивирусный контроль;
- Сотрудник обязан проводить антивирусный контроль всех внешних носителей информации (дискет, компакт-дисков, магнитооптических дисков и т.п.), поступающих со стороны (из внешних организаций, других подразделений Организации и т.п.) или полученных по компьютерным сетям (скопированных на общедоступный ресурс локального компьютера другими пользователями). Если антивирусная программа не работает в фоновом режиме, самому проводить проверку всех этих файлов или обращаться для этого в отдел информационных технологий;
- Во всех случаях возможного проявления действия вирусов, обнаружения файлов, пораженных вирусом или подозрении на наличие вируса сотрудник должен:
    - без попытки какого-либо лечения незамедлительно сообщить об этом ответственному за антивирусный контроль и оценить с ним возможные пути заражения и распространения данного вируса;
    - совместно с ним провести лечебно-восстановительные мероприятия.
- Сотрудник обязан делать резервные копии файлов, содержащих ценную служебную информацию, если эти файлы не размещены в сетевых папках на серверах Организации;
- Сотрудник не должен самостоятельно устанавливать программное обеспечение, если это не входит в его обязанности. Запрещается устанавливать и запускать нелицензионное или не относящееся к выполнению им своих должностных обязанностей программное обеспечение;
- КАТЕГОРИЧЕСКИ ЗАПРЕЩЕНО использование съёмных носителей, принадлежащих лицам, временно допущенным к работе на компьютере в Организации (студенты-практиканты, временно замещающие, сотрудники сторонних организаций и т.п.).

Пользователю запрещается:

- изменять настройки и конфигурацию средств антивирусной защиты;
- удалять или добавлять в систему какие-либо другие средства антивирусной защиты.