

бюджетное профессиональное
образовательное учреждение
Вологодской области
«Великоустюгский
многопрофильный колледж»

УТВЕРЖДЕНА
приказом директора
колледжа



г. № 74

ИНСТРУКЦИЯ

«19» 02 2019 г. № 29

г. Великий Устюг

по организации антивирусной защиты

1. Общие положения

1.1. Настоящая Инструкция предназначена для всех сотрудников бюджетного профессионального образовательного учреждения Вологодской области «Великоустюгский многопрофильный колледж» (далее – колледж), имеющих доступ к информационным системам колледжа (далее – ИС).

1.2. Инструкция устанавливает требования и ответственность при организации защиты информации от воздействия вредоносных компьютерных вирусов.

1.3. Инструкция регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля при работе в ИС колледжа.

2. Обеспечение антивирусной защиты

2.1. Порядок организации антивирусной защиты:

2.1.1. Для организации антивирусной защиты ИС колледжа допускаются к использованию только сертифицированные ФСТЭК (Федеральная служба по техническому и экспортному контролю) России лицензионные антивирусные средства общего применения.

2.1.2. Антивирусное средство защиты должно быть установлено на все средства вычислительной техники (СВТ) (при наличии технической возможности), входящие в ИС колледжа.

2.1.3. В ИС колледжа права по управлению (администрированию) средствами антивирусной защиты предоставлены только администратору безопасности автоматизированной системы (далее – АС).

2.1.4. Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляется ответственным за осуществление контроля за состоянием уровня защищенности информационных ресурсов и обеспечением защиты информации с привлечением (при необходимости) администратора безопасности АС и /или специалистов лицензированной организации.

2.1.5. Должностные лица не должны допускать использования в ИС

колледжа программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

2.1.6. В ИС колледжа обеспечивается централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (автоматизированных рабочих местах).

2.1.7. В ИС колледжа обеспечивается централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов).

2.1.8. Расширенный антивирусный контроль проводится администратором безопасности АС не реже одного раза в месяц и при необходимости, в случае подозрений в заражении вирусной программой.

2.1.9. При загрузке, открытии или исполнении объектов (файлов) из внешних источников средствами антивирусной защиты проводится автоматическая проверка объектов (файлов).

2.1.10. В виртуальной инфраструктуре обеспечивается реализация и управление антивирусной защитой:

- проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;

- проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

2.2. Порядок проведения антивирусного контроля:

2.2.1. Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется администратором безопасности АС на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка администратором безопасности АС.

2.2.2. При загрузке компьютера средствами антивирусной защиты проводится антивирусный контроль в автоматическом режиме.

2.2.3. 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 т.п.) пользователь ИС колледжа самостоятельно или вместе с администратором безопасности АС проводит внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.

2.2.4. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИС колледжа обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов директора колледжа и администратора безопасности АС,

владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов;

- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на съемном носителе информации администратору безопасности АС для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при наличии);

- по факту обнаружения зараженных вирусом файлов составить служебную записку администратору безопасности АС, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

2.3. Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

2.3.1. Администратор безопасности АС обеспечивает получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

2.3.2. Контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов) обеспечивается путем автоматического получения или предварительно скачиваемых обновлений из официальных источников, например, с сервера обновлений производителя антивирусного средства.

3. Ответственность при организации антивирусной защиты

3.1. Ответственность за организацию антивирусной защиты ИС колледжа в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности АС.

3.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на администратора безопасности АС и пользователей, эксплуатирующих ИС колледжа.

СОГЛАСОВАНО

Советом Учреждения

Протокол № 2

«18» 02 2019 г.

В дело № 01-14

«19» 02 2019 г.

Лист ознакомления
с инструкцией по антивирусной защите в информационных системах в
бюджетном профессиональном образовательном учреждении
Вологодской области
«Великоустюгский многопрофильный колледж»

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				