УТВЕРЖДАЮ
Директор ОБПОУ «КГТТС»
_____ Е.Н.Брежнев
Приказ № 453/о от 30.12.2016

# ИНСТРУКЦИЯ
## по обеспечению антивирусной защиты в информационных системах

### 1. Общие положения

1.1. Настоящая Инструкция определяет порядок обеспечения антивирусной защиты информации, обрабатываемой в информационных системах ОБПОУ КГТТС».

1.2. Настоящая Инструкция предназначена для администратора безопасности (далее - Администратор).

1.3. В настоящей Инструкции используются следующие сокращения:

– АРМ — авторизированное рабочее место;

– НСД — несанкционированный доступ;

– ПО — программное обеспечение;

– САЗ — средство антивирусной защиты;

– СЗИ — средство защиты информации.

1.4. В настоящей Инструкции используются следующие термины и их определения:

– Антивирусная защита (информации) — организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий вредоносного ПО на информацию и (или) устранение последствий этих действий;

– Антивирусные базы — список сигнатур и алгоритмов, используемые средством антивирусной защиты для идентификации и (или) противодействия вредоносному ПО;

– Вирус (компьютерный, программный) — исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению;

– Вредоносное ПО — программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на ресурсы АС[1];

– Зараженный ресурс — ресурс, подвергшийся программному воздействию;

– Лечение зараженных ресурсов — осуществляемые с использованием САЗ действия по восстановлению оригинального (до программного воздействия) содержимого зараженных ресурсов;

[1] В настоящей Инструкции, понятие «вредоносное ПО» используется для определения совокупности вирусов, троянских коней, червей, руткитов и др.

– Монитор (модуль САЗ) — модуль САЗ, постоянно находящийся в оперативной памяти и отслеживающий подозрительные действия других программ в режиме реального времени;

– Программное (программно-математическое) воздействие — несанкционированное воздействие на ресурсы информационной системы, осуществляемое с использованием вредоносного ПО;

– Ресурсы (информационные) — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах[2];

– Сканер (модуль САЗ) — модуль САЗ, предназначенный для проверки наличия вредоносного ПО в файлах, папках и дисках по требованию субъектов доступа;

– Средство антивирусной защиты (информации) — программное или программно-аппаратное средство, обеспечивающее антивирусную защиту информации.

1.5. Администратор безопасности информации, нарушивший требования настоящей Инструкции несет персональную ответственность в соответствии с законодательством РФ.

1.6. Все администраторы безопасности должны быть под подпись ознакомлены с данной Инструкцией, а также ответственностью за нарушение ее требований.

## 2. Проведение антивирусного контроля на ПЭВМ

2.1. В целях обеспечения антивирусной защиты в информационных системах вводится антивирусный контроль.

2.2. К применению в информационных системах допускается лицензионное антивирусное программное обеспечение, имеющее действующие сертификаты ФСТЭК и/или ФСБ России.

2.3. Администратор осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

2.4. Администратор проводит периодическое тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов.

2.5. При обнаружении компьютерного вируса пользователь обязан немедленно поставить в известность Администратора и прекратить какие-либо действия на ПЭВМ.

2.6. Администратор проводит в случае необходимости лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

2.7. В случае обнаружения на съемных носителях информации нового вируса, не поддающегося лечению, Администратор обязан запретить использование съемных носителей.

2.8. В случае обнаружения на жестком диске ПЭВМ вируса, не поддающегося лечению, Администратор обязан поставить в известность ответственного за

[2] В качестве ресурсов в информационной системе могут выступать файлы, области памяти машинных носителей и др.

организацию обработки персональных данных, запретить работу в информационной системе и в кротчайшие сроки, обновить пакет антивирусной программы. Если обновление антивирусных баз не дало результатов, запретить работу до устранения угрозы со стороны вредоносного ПО или принятия решения о дальнейшей работе ответственным за организацию обработки персональных данных.

## 3. Действия в случае обнаружения вредоносного ПО

3.1. При обнаружении САЗ вредоносного ПО (пользователем информационной системы, или самим администратором), должен провести мероприятия по уничтожению вредоносного ПО и лечению зараженных ресурсов АС с использованием САЗ.

3.2. Если процедура уничтожения вредоносного ПО и лечения зараженных ресурсов информационной системы завершилась успешно, администратор должен провести проверку всей информации на всех носителях, которые могли быть заражены.

3.3. При невозможности уничтожения вредоносного ПО и (или) лечения зараженных файлов на носителе информации, администратор должен запретить использование данного носителя (приостановить работу рабочей станции) и сообщить об этом лицу, ответственному за организацию обработки персональных данных для выработки решения о дальнейших действиях.