



Инструкция по антивирусной защите

1. Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты ИСПДн (информационная система ГБОУ гимназии № 664 (далее - Учреждения) и устанавливает ответственность за их выполнение.

Действие настоящей инструкции распространяется в полном объеме на Учреждение и обязательна для выполнения всеми сотрудниками.

2. Инструкция по применению средств антивирусной защиты

2.1 Защита программного обеспечения ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

2.2 К использованию допускаются только лицензионные антивирусные средства, обладающие сертификатами регулирующих органов РФ.

2.3 Решение задач по установке и сопровождению средств антивирусной защиты возлагается на ответственного за СЗИ (средства защиты информации) ИСПДн.

2.4 Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.

2.5 Все впервые вводимое в эксплуатацию программное обеспечение должно проходить обязательный антивирусный контроль.

2.6 Средства антивирусной защиты устанавливаются на всех серверах Учреждения.

2.7 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.

2.8 Контроль входящей информации необходимо проводить непосредственно после ее приема.

2.9 Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

2.10 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

2.11 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, обнаруживший проблему, должен провести внеочередной антивирусный контроль либо обратиться к ответственному за СЗИ ИСПДн.

2.14 При получении информации о возникновении вирусной эпидемии вне Учреждения должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.

2.15 В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
 - немедленно поставить в известность о факте обнаружения вируса ответственного за СЗИ ИСПДн;
 - провести лечение зараженных файлов;
 - в случае невозможности лечения обратиться к сотруднику, ответственному за СЗИ ИСПДн;
- 2.16 По факту обнаружения зараженных вирусом файлов сотрудник, ответственный за СЗИ ИСПДн, должен составить служебную записку, 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.
- 2.17 Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях (рабочая станция - компьютер, который включен в состав локальной сети).
- 2.18 Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.
- 2.19 Ответственный за СЗИ ИСПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.
- 2.20 Пользователи должны быть ознакомлены с данной инструкцией под роспись.
- 2.21 Проводить периодическое тестирование функций средств антивирусной защиты.
- 2.22 Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).

