

УТВЕРЖДАЮ

Директор МБУ ДО «СШ «Виктория»
МО Усть-Лабинский район

Гнехачев М.А.



подпись

расшифровка подписи

М.А. Гнехачев
"24" декабря 2023 г.

Инструкция

по антивирусной защите в

МБУ ДО «СШ «Виктория» МО Усть-Лабинский район

РАЗРАБОТАЛ

Администратор информационной
безопасности Гунькина О.И.

О.И. Гунькина
подпись
расшифровка подписи
"24" декабря 2023 г.

г. Усть-Лабинск
2023

1. Общие положения

Инструкция по антивирусной защите в организации МБУ ДО «СШ «Виктория» МО Усть-Лабинский район определяет правила и основные требования по обеспечению антивирусной защиты информационной системы персональных данных и ответственность за их выполнение (далее – организация)

Действие настоящей инструкции распространяется в полном объеме на организацию и обязательно для выполнения всеми сотрудниками.

2. Инструкция по применению средств антивирусной защиты

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

2.2. К использованию допускаются только лицензионные антивирусные средства, обладающие соответствующими сертификатами, выданными в установленном порядке.

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

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

2.5. Все впервые вводимое в эксплуатацию ПО, должно проходить обязательный антивирусный контроль.

2.6. Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места ответственного за СЗИ ИСПДн.

2.7. Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах организации.

2.8. Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов.

2.9. 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.

2.10. Контроль входящей информации необходимо проводить непосредственно после ее приема.

2.11. Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

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

2.13. 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 рабочей станции либо обратиться к ответственному за СЗИ ИСПДн.

2.14. При получении информации о возникновении вирусной эпидемии вне организации 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 в письменном виде проинформировать руководителя организации, указав 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.

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;

- проводить периодическое тестирование функций средств антивирусной защиты;

- проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе);

- ознакомить пользователей с настоящей инструкцией под роспись (лист ознакомления прилагается).