|  |  |  |
| --- | --- | --- |
|  |  | УТВЕРЖДАЮДиректор МБУ ДО СШ №4 г. Туапсе МО Туапсинский район\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_С.А. Забураев"\_\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023г. |

**Инструкция**

 **по антивирусной безопасности**

**в муниципальном бюджетном учреждении**

**дополнительного образования спортивная школа №4**

**г. Туапсе МО Туапсинский район**

|  |  |  |
| --- | --- | --- |
|  |  | **Разработал**Администратор информационнойбезопасности МБУ ДО СШ №4 г.ТуапсеМО Туапсинский район \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.А. Манькова"\_\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023г. **"\_\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023г.** |

г. Туапсе

2023 год

1. **Общие положения**

Инструкция по антивирусной защите в муниципальном бюджетном учреждении дополнительного образования спортивная школа №4 г. Туапсе МО Туапсинский район определяет правила и основные требования по обеспечению антивирусной защиты информационной системы персональных данных и ответственность за их выполнение (далее – учреждение).

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

1. **Инструкция по применению средств антивирусной защиты**
	1. Защита программного обеспечения ИСПДн от вредоносного программного обеспечения (далее – ПО) осуществляется путем применения специализированных средств антивирусной защиты.
	2. К использованию допускаются только лицензионные антивирусные средства, обладающие соответствующими сертификатами, выданными
	в установленном порядке.
	3. Решение задач по установке и сопровождению средств антивирусной защиты возлагается на ответственного за систему защиты информации (далее – СЗИ) ИСПДн.
	4. Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.
	5. Все впервые вводимое в эксплуатацию ПО, должно проходить обязательный антивирусный контроль.
	6. Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места ответственного за СЗИ ИСПДн.
	7. Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах учреждения.
	8. Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов.
	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.
	10. Контроль входящей информации необходимо проводить непосредственно после ее приема.
	11. Контроль исходящей информации необходимо проводить непосредственно перед отправкой.
	12. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.
	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.
	14. При получении информации о возникновении вирусной эпидемии
	вне учреждения должно быть осуществлено информирование пользователей
	о возможной эпидемии и рекомендуемых действиях.
	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.
	16. По факту обнаружения зараженных вирусом файлов сотрудник, ответственный за СЗИ ИСПДн, должен в письменном виде проинформировать директора учреждения, указав предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.
	17. Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.
	18. Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.
	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).

**Лист ознакомления**

**с инструкцией** **по антивирусной защите**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Фамилия, имя, отчество работника** | **Дата ознакомления**  | **Подпись работника** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |