Государственное бюджетное учреждение дополнительного образования центр детского (юношеского) технического творчества Красногвардейского района Санкт-Петербурга «Охта»

ПРИНЯТО
на Совете
ГБУ ДО ЦДЮТТ
Красногвардейского района
Санкт-Петербурга «Охта»

Протокол № 230

от « 24 » 08 2026 г.

УТВЕРЖДАЮ
Директор
ГБУ ДО ЦДЮТТ
Красногвардейского района
Санкт-Петербурга «Охта»

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Владелец Иванова Наталья Леонидовна
Действителен с17.04.2026 по 11.07.2027

Иванова Н.Л.

Приказ № 365

от « 25 » 08 2026г.

ИНСТРУКЦИЯ

по обеспечению антивирусной защиты в информационной системе

Государственного бюджетного учреждения дополнительного образования центра детского (юношеского) технического творчества Красногвардейского района Санкт-Петербурга «Охта»

Санкт-Петербург

ИНСТРУКЦИЯ
по обеспечению антивирусной защиты в информационной системе Государственного бюджетного учреждения дополнительного образования центра детского (юношеского) технического творчества Красногвардейского района Санкт-Петербурга «Охта» (ГБУ ДО ЦДЮТТ «Охта»)

1 Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты в информационной системе персональных данных (далее ИСПДн) (далее - Учреждения) и устанавливает ответственность за их выполнение.

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

2 Инструкция по применению средств антивирусной защиты

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

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

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

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

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

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

1.7 Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах Учреждения.

1.8 Ежедневно в автоматическом режиме проводится быстрая проверка оперативной памяти, системных областей и автозагрузки рабочих станций и серверов, а полное сканирование всех жестких дисков и

файлов осуществляется не реже 1 раза в месяц во внерабочее время (согласно утвержденному графику регламентных работ).

1.9 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.

1.10 Контроль входящей информации необходимо проводить непосредственно после ее приема.

1.11 Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

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

1.13 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.

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

1.15 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 работнику, ответственному за СЗИ ИСПДн;

1.16 По факту обнаружения зараженных вирусом файлов работник, 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.

1.17 Передача служебной информации, отчетов об инцидентах информационной безопасности и файлов журналов через иностранные сервисы обмена сообщениями (мессенджеры Telegram,

WhatsApp, Viber, Discord и др.) категорически запрещается (ч. 8–10 ст. 10 Федерального закона № 149-ФЗ); служебное взаимодействие осуществляется исключительно через локальную сеть, защищенную корпоративную почту или отечественную коммуникационную платформу (MAX / Сферум)

1.18 Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

1.19 Ответственный за СЗИ ИСПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.

1.20 Пользователи должны быть ознакомлены с данной инструкцией под роспись.

1.21 Проводить периодическое тестирование функций средств антивирусной защиты.

1.22 Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).

Лист ознакомления
с Инструкцией
по антивирусной защите информационной системы персональных данных
Государственного бюджетного образовательного учреждения
дополнительного образования детей центра детского (юношеского)
технического творчества Красногвардейского района Санкт-Петербурга «Охта»

№ п/п	Фамилия, имя, отчество работника	Дата ознакомления с Инструкцией	Подпись работника