Государственное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа № 459
Пушкинского района Санкт-Петербурга

ОБСУЖДЕНО И ПРИНЯТО
Общим собранием работников
ГБОУ школы № 459
Пушкинского района Санкт-Петербурга
Протокол № 2 от 04.03.2025

РАЗРАБОТАН И ПРИНЯТ
педагогическим Советом
ГБОУ школы № 459
Пушкинского района Санкт-Петербурга
Протокол № 2 от 04.03.2025

УТВЕРЖДЕН
Директор ГБОУ школы № 459
Пушкинского района Санкт-Петербурга

А.В. Суенкова

Приказ № 35-од от 27.03.2025

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 459 ПУШКИНСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

Подписано цифровой подписью: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 459 ПУШКИНСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

ИНСТРУКЦИЯ

по организации антивирусной защиты информационных систем персональных данных государственного бюджетного общеобразовательного учреждения средней общеобразовательной школы № 459 Пушкинского района Санкт Петербурга

Санкт-Петербург

2025

1. Общие положения

1.1. Настоящая Инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее — ИСПДн) Государственного бюджетного общеобразовательного учреждения средней общеобразовательной школы № 459 Пушкинского района Санкт-Петербурга (далее — Школа) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (ПО).

1.2. Требования настоящей Инструкции распространяются на всех сотрудников Школы, использующих в работе ИСПДн, включая административный, педагогический и технический персонал.

1.3. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, Администратор безопасности ИСПДн проводит семинары и персональные инструктажи для пользователей ИСПДн.

1.4. Доведение Инструкции до сотрудников Школы осуществляется Администратором безопасности ИСПДн под роспись в журнале ознакомления.

1.5. В случае невозможности исполнения требований настоящей Инструкции в полном объеме (например, в нештатных ситуациях, связанных с отказами оборудования, сбоями или злоумышленными действиями), практическая реализация мер защиты определяется Администратором безопасности ИСПДн по согласованию с ответственным за обеспечение безопасности персональных данных.

---

2. Применение средств антивирусной защиты

2.1. Антивирусный контроль дисков и файлов ИСПДн должен проводиться в автоматическом режиме после загрузки компьютера (периодическое сканирование или мониторинг).

2.2. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн (сканирование).

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация на съемных носителях (флеш-накопители, CD/DVD и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации — непосредственно перед отправкой.

2.4. Установка, обновление и изменение системного и прикладного программного обеспечения осуществляется в соответствии с внутренними регламентами Школы.

2.5. Обновление антивирусных баз должно проводиться регулярно, но не реже одного раза в неделю.

---

3. Функции Администратора безопасности ИСПДн по обеспечению антивирусной безопасности

Администратор безопасности ИСПДн обязан:

3.1. Проводить инструктажи пользователей ИСПДн по вопросам применения средств антивирусной защиты.

3.2. Настраивать параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.

3.3. Предварительно проверять устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусов.

3.4. Производить обновление антивирусных программных средств и баз данных.

3.5. Получать и распространять обновления антивирусных баз среди пользователей ИСПДн.

3.6. Разрабатывать инструкции по работе пользователей с программными средствами антивирусной защиты.

3.7. Проводить работы по обнаружению и обезвреживанию вирусов.

3.8. Участвовать в расследовании причин заражения компьютеров и серверов.

3.9. Хранить эталонные копии антивирусных программных средств.

3.10. Осуществлять периодический контроль за соблюдением пользователями требований настоящей Инструкции.

3.11. Проводить периодический контроль работы программных средств антивирусной защиты на компьютерах и серверах.

---

4. Функции пользователей

Пользователи ИСПДн обязаны:

4.1. Получать обновления антивирусных баз от Администратора безопасности ИСПДн (в случае отсутствия централизованного механизма обновления).

4.2. Проводить обновление антивирусных баз на своих компьютерах (в случае отсутствия централизованного механизма обновления).

4.3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частые системные ошибки и т.п.) немедленно провести внеочередной антивирусный контроль компьютера и уведомить Администратора безопасности ИСПДн.

4.4. В случае обнаружения зараженных файлов:

- Приостановить работу с зараженными файлами.
- Немедленно уведомить руководителя структурного подразделения и Администратора безопасности ИСПДн.
- Провести анализ необходимости дальнейшего использования зараженных файлов.
- Провести лечение или уничтожение зараженных файлов (при необходимости с привлечением Администратора безопасности).
- В случае обнаружения нового вируса, не поддающегося лечению, передать зараженный файл Администратору безопасности для дальнейшего анализа.

---

5. Порядок пересмотра Инструкции

5.1. Инструкция подлежит полному пересмотру в случае внедрения новых средств антивирусной защиты, существенно изменяющих порядок работы с ними.

5.2. В остальных случаях Инструкция подлежит частичному пересмотру.

5.3. Изменения в Инструкции фиксируются в листе регистрации изменений (Приложение 1).

---

6. Ответственность за организацию и контроль выполнения Инструкции

6.1. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников Школы.

6.2. Ответственность за организацию и контроль выполнения антивирусной защиты возлагается на Администратора безопасности ИСПДн.

6.3. Общий контроль за информационной безопасностью возлагается на ответственного за обеспечение безопасности персональных данных Школы.