

Утверждено
И.о. директора ГБОУ СОШ №1 «ОЦ»
им. В.И. Фокина с. Большая Глушица
Соколова О.А.
«01» сентября 2021 г.

ИНСТРУКЦИЯ

по организации антивирусной защиты информационных систем персональных данных ГБОУ СОШ №1 «ОЦ» им. В.И. Фокина с. большая Глушица

Настоящая инструкция определяет порядок организации антивирусной защиты на информационных системах персональных данных ГБОУ СОШ №1 «ОЦ» им. В.И. Фокина с. Большая Глушица (далее -ИСПДн).

1 Общие положения

- 1.1. Настоящая Инструкция предназначена для администратора ИБ ИСПДн, ответственного за ЗИ на объекте информатизации и пользователей, эксплуатирующих ИСПДн ГБОУ СОШ №1 «ОЦ» им. В.И. Фокина с. Большая Глушица.
- 1.2. Инструкция устанавливает требования и ответственность при организации защиты информации, в ИСПДн от программно-математических воздействий и разрушающего воздействия компьютерных вирусов.
- 1.3. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов, проводятся организуемые Администратором ИБ ИСПДн семинары и персональные инструктажи (при необходимости) пользователей ИСПДн.
- 1.4. Инструкция регулирует как вопросы организации антивирусной защиты, так и требования к порядку проведения антивирусного контроля при работе в ИСПДн.

2 Применение средств антивирусной защиты

- 2.1. Антивирусный контроль дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (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 любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).
- 2.4. Установка (обновление и изменение) системного и прикладного программного обеспечения осуществляется в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения аппаратных средств информационных систем персональных данных ГБОУ СОШ №1 «ОЦ» им. В.И. Фокина с. Большая Глушица.

2.5. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз неделю.

3 Функции Администратора ИСПДн по обеспечению антивирусной безопасности

Администратор ИБ ИСПДн обязан:

- 3.1. При необходимости 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. При необходимости производить обновление антивирусных программных средств.
- 3.5. Производить получение и рассылку (при необходимости) обновлений антивирусных баз.
- 3.6. При необходимости разрабатывать инструкции по работе пользователей программными средствами САЗ.
- 3.7. Проводить работы по обнаружению и обезвреживанию вирусов.
- 3.8. Участвовать в работе комиссии по расследованию причин заражения ПК и серверов.
- 3.9. Хранить эталонные копии антивирусных программных средств.
- 3.10. Осуществлять периодический контроль за соблюдением пользователями ПК требований настоящей Инструкции.
- 3.11. Разрабатывать инструкции по работе пользователей с системой антивирусной защиты информации.
- 3.12. Проводить периодический контроль работы программных средств системы антивирусной защиты информации на ПК (серверах).

4 Функции пользователей

Пользователи ИСПДн:

- 4.1. Получают по ЛВС или от Администратора ИБ ИСПДн носители с обновлениями антивирусных баз (в случае отсутствия механизмов централизованного распространения антивирусных баз).
- 4.2. Проводят обновления антивирусных баз на ПК (в случае отсутствия механизмов централизованного распространения антивирусных баз).
- 4.3. 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.) сотрудник подразделения самостоятельно или вместе с администратором ИБ ИСПДн должен провести внеочередной антивирусный контроль ПК. При необходимости он должен пригласить Администратора ИБ ИСПДн для определения факта наличия или отсутствия компьютерного вируса.
- 4.4. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:
 - 4.4.1. приостановить работу;
 - 4.4.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения и Администратора ИБ ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
 - 4.4.3. совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
 - 4.4.4. провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта пригласить Администратора ИБ ИСПДн);
 - 4.4.5. в случае обнаружения нового вируса, неподдающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном носителе Администратору ИБ ИСПДн для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;
 - 4.4.6. по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору ИБ ИСПДн, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

5 Ответственность при организации антивирусной защиты

5.1.1. Ответственность за организацию антивирусной защиты ИСПДн и установление порядка ее проведения, в соответствии с требованиями настоящей Инструкции, возлагается на ответственного за ЗИ в ИСПДн.

5.1.2. Ответственность за поддержание установленного порядка и соблюдение Требований настоящей Инструкции возлагается на Администратора ИБ в ИСПДн и пользователей (операторов).

5.1.3. Периодический контроль за выполнением всех требований настоящей Инструкции, и состоянием антивирусной защиты осуществляется Администратором ИБ ИСПДн.