

Рассмотрена и принята
на заседании педагогического
совета (протокол от 24.05.2017 г. №5)

Утверждена
приказом директора от 24.05.2017 г. № 99/11
И.о. директора Тарасова Н.Ю.



Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных

1. Общие положения

Данная Инструкция устанавливает порядок планирования и проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации школы.

2. Виды мониторинга информационной безопасности

2.1. Мониторинг работоспособности аппаратных компонент автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование) должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

2.2. Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

- установление сроков действия паролей (не более 3 месяцев);
- периодическую (не реже 1 раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

2.3. Мониторинг целостности программного обеспечения включает следующие действия:

- проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
- обнаружение дубликатов идентификаторов пользователей;
- восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

2.4. Мониторинг попыток несанкционированного доступа

Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств, и предусматривает:

- фиксацию неудачных попыток входа в систему в системном журнале;
- протоколирование работы сетевых сервисов;
- выявление фактов сканирования определенного диапазона сетевых портов, в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

2.5. Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, производится по обращениям пользователей, в ходе администрирования систем и проведения профилактических работ для выявления