Рассмотрено
на заседании Совета
ГАПОУ СО «ЕТХМ»
Протокол № 5,
от « 20 » мая 2020 г.

УТВЕРЖДЕНО
Приказом директора
ГАПОУ СО «ЕТХМ»
№ 140 - о/д от « 20 » мая 2020 г.

ИНСТРУКЦИЯ
по проверке электронного журнала обращений к информационной системе персональных данных ГАПОУ СО «ЕТХМ»

Екатеринбург
2020 г.

Введено в действие с 20.05.2020 г.

1. Задачи проверки

Под проверкой понимается отслеживание событий, происходивших на автоматизированных рабочих местах (далее – АРМ) в течение определенного времени.

Общими задачами проверки являются:

- Контролирование состояния защищенности системы;
- Выявление причин произошедших изменений;
- Определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к НСД;
- Установление времени изменений.

Проверку средств защиты осуществляет администратор информационной безопасности.

2. Журналы записей о событиях

События, происходящие на АРМ, входящем в состав ИСПДн, регистрируются в журналах.

Каждому событию соответствует отдельная запись в журнале, содержащая подробную информацию для анализа события.

В состав используемых в ИСПДн средств защиты информации может входить специальное программное средство для аудита журналов событий, предназначенное для загрузки и просмотра журналов (далее - программа просмотра журналов). В программу просмотра журналов могут быть загружены записи следующих журналов:

- Штатные журналы операционной системы Windows;
- Журналы событий средств защиты информации.

3. Штатные журналы операционной систем

В штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе. События используемых средств защиты информации в них не регистрируются.

Информация о событиях, происходящих на АРМ под управлением ОС Windows, сохраняется в следующих штатных журналах:

- Журнал приложений - содержит сведения об ошибках, предупреждениях и других событиях, возникающих при исполнении приложений;
- Системный журнал - содержит сведения об ошибках, предупреждениях и других событиях, возникающих в операционной системе;
- Журнал безопасности - хранит информацию о попытках регистрации, а также о событиях, связанных с использованием ресурсов.

Подробное описание содержимого штатных журналов ОС Windows отражено в документации к операционной системе.

Загрузка и просмотр записей штатных журналов может осуществляться как в программе просмотра журналов средств защиты, так и с помощью стандартных средств работы с журналами ОС Windows - в оснастке «Просмотр событий» («Eventviewer»).

4. Журнал событий средств защиты информации

Журналы средств защиты информации (далее - СЗИ) хранят информацию о событиях, отслеживаемых средствами самих СЗИ, в этом журнале регистрируются события, заданные параметрами СЗИ для локальной политики безопасности.

5. Аудит

Сведения, содержащиеся в журнале, позволяют отслеживать использование механизмов защиты, которые предоставляют средства защиты информации АРМ (шифрование файлов, полномочное управление, замкнутая программная среда и др.) подробное описание регистрируемых событий указано в соответствующих руководствах к используемым СЗИ.

6. Просмотр событий электронных журналов

Администратор информационной безопасности в ИСПДн производит проверку электронных журналов.

В случае обнаружения нарушений администратор информационной безопасности докладывает о данном факте ответственному за организацию обработки персональных данных.

Разработал:
Секретарь Титова Н.А.