Приложение № 16
к приказу ГАУ ДПО ИРО
от 12.02.2025 № 23

Правила
контроля и мониторинга за обеспечением уровня защищенности информации, содержащейся в информационных системах государственного автономного учреждения дополнительного профессионального образования Иркутской области «Институт развития образования Иркутской области»

1. Контроль состояния информационной безопасности является неотъемлемой составной частью работ по поддержанию требуемого режима защиты информационных систем государственного автономного учреждения дополнительного профессионального образования Иркутской области «Институт развития образования Иркутской области» (далее соответственно – ГАУ ДПО ИРО, ИС).

2. Контроль состояния информационной безопасности в ходе эксплуатации объектов информатизации проводится с периодичностью не реже, чем один раз в три года с целью подтверждения сохранения защитных функций ИС и проверки выполнения пользователями объектов информатизации и ответственными работниками структурного подразделения ГАУ ДПО ИРО, ответственное за обеспечение безопасности ПДн при их обработке в ИС.

3. Контроль проводится также в случаях нарушения информационной безопасности с целью определения причин произошедших нарушений и выработке мер по противодействию повторным нарушениям информационной безопасности.

4. Основными задачами контроля являются:

1) проверка соответствия системы обеспечения информационной безопасности требованиям действующего законодательства, стандартов, положениям локальных нормативных актов;

2) проверка соответствия организации работ по обеспечению информационной безопасности требованиям установленного режима защиты ИС;

3) оценка обоснованности принимаемых мер защиты информации и соответствия их установленным требованиям информационной безопасности;

4) проверка своевременности и полноты выполнения работниками ГАУ ДПО ИРО требований законодательства и локальных нормативных актов по обеспечению информационной безопасности.

5. Для реагирования на события безопасности в ИС работником, ответственным за обеспечение безопасности ПДн, должны осуществляться централизованный сбор, запись, хранение, мониторинг и корреляция информации о событиях безопасности.

6. События безопасности, подлежащие регистрации в ИС, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС.

7. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в ИС.

8. Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется администратором информационной системы, исходя из возможностей реализации угроз безопасности информации, и фиксируется в журнале учета мероприятий по контролю режима защиты конфиденциальной информации и выполнения обязательных процедур.

9. Сбор, запись и хранение информации о событиях безопасности должны предусматривать:

1) возможность выбора администратором безопасности информации событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий

безопасности;

2) генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту);

3) хранение информации о событиях безопасности.

10. Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учётом типов событий безопасности, подлежащих регистрации, состава и содержания информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

11. Реагирование на сбои при регистрации событий безопасности должно предусматривать:

1) предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (ёмкости) памяти) при регистрации событий безопасности;

2) реагирование на сбои при регистрации событий безопасности путём изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

12. Администратор безопасности информации осуществляет мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирует на них. Мониторинг (просмотр и анализ) записей регистрации (аудита) проводиться для всех событий, подлежащих регистрации, и с периодичностью, обеспечивающей своевременное выявление признаков инцидентов безопасности в ИС. В случае выявления признаков событий безопасности в ИС осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

13. Информация о событиях безопасности подлежит защите и обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

14. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только администратору безопасности.