Приложение № 12
к Приказу от 06.02.2018 г. № 19

Инструкция по регистрации событий безопасности в типовом сегменте «Информационной системы, содержащей сведения о возможностях дополнительного образования на территории Московской области»

1. Общие положения

1.1 Настоящая инструкция по регистрации событий безопасности в иповом сегменте «Информационной системе, содержащей сведения о озможностях дополнительного образования на территории Московской бласти» (далее по тексту – информационная система) определяет события зопасности, их состав, содержание, сроки хранения, порядок анализа и меры щиты информации о событиях безопасности, подлежащих регистрации в нформационной системе.

1.2 Администратор информационной безопасности в своей работе уководствуется настоящей инструкцией.

1.3 Настоящая инструкция является дополнением к действующим ормативным документам по вопросам защиты информации, и не исключает бязательного выполнения их требований.

2. Определение событий безопасности, подлежащих регистрации, и роков их хранения

2.1 События безопасности, подлежащие регистрации в информационной истеме, должны определяться с учетом способов реализации угроз езопасности для информационной системы. К событиям безопасности, длежащим регистрации в информационной системе должны быть отнесены ые проявления состояния информационной системы и ее системы защиты нформации, указывающие на возможность нарушения конфиденциальности, остности или доступности информации, доступности компонентов нформационной системы, нарушения процедур, установленных рганизационно-распорядительными документами по защите информации ратора, а также на нарушение штатного функционирования средств защиты нформации.

2.2 События безопасности, подлежащие регистрации в информационной истеме, и сроки их хранения соответствующих записей регистрационных урналов, должны обеспечивать возможность обнаружения, идентификации и нализа инцидентов, возникших в информационной системе.

2.3 В информационной системе подлежат регистрации следующие ытия:

- вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;
- подключение машинных носителей информации и вывод информации на носители информации;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;
- попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

3. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

3.1 Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

3.2 При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы, состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

3.3 При регистрации подключения машинных носителей информации и вывода информации на носители информации, состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

3.4 При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации, состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

3.5 При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам, состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

3.6 При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей), состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер)).

3.7 При регистрации попыток удаленного доступа к информационной системе, состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

4. Сбор, запись и хранение информации о событиях безопасности

4.1 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения, должен предусматривать:

- возможность выбора ответственным за защиту информации в информационной системе и (или) администратором информационной системы событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности определенных в пункте 2.3 настоящей инструкции;
- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, определенными в соответствии с пунктами 3.2 – 3.7 настоящей инструкции;
- хранение информации о событиях безопасности в течение времени, установленного в соответствии с пунктом 2.2 настоящей инструкции.

4.2 Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с пунктами 3.2 – 3.7 настоящей инструкции, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

5. Реагирование на сбои при регистрации событий безопасности

5.1 В информационной системе должно осуществляться реагирование на ои при регистрации событий безопасности, в том числе аппаратные и ограммные ошибки, сбои в механизмах сбора информации и достижение едела или переполнения объема (емкости) памяти.

5.2 Реагирование на сбои при регистрации событий безопасности должно едусматривать:

- предупреждение (сигнализация, индикация) о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
- реагирование на сбои при регистрации событий безопасности, путем изменения ответственным за защиту информации в информационной системе и (или) администратором информационной системы 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.

6. Мониторинг (просмотр, анализ) результатов регистрации событий пасности и реагирование на них

6.1 Мониторинг (просмотр и анализ) записей регистрации (аудита) должен одиться для всех событий, подлежащих регистрации в соответствии и с одичностью, установленной оператором, и обеспечивающей еременное выявление признаков инцидентов безопасности в рмационной системе.

6.2 В случае выявления признаков инцидентов безопасности в рмационной системе, осуществляется планирование и проведение ероприятий по реагированию на выявленные инциденты безопасности в ветствии с Порядком проведения разбирательств по фактам возникновения идентов в информационной системе.

7. Генерирование временных меток и (или) синхронизация системного ени в информационной системе

7.1 Получение меток времени, включающих дату и время, используемых генерации записей регистрации (аудита) событий безопасности в рмационной системе достигается посредством применения внутренних ных часов информационной системы.

8. Защита информации о событиях безопасности

8.1 Защита информации о событиях безопасности (записях регистрации) обеспечивается применением мер защиты информации от мерного доступа, уничтожения или модифицирования и в том числе ет защиту средств ведения регистрации (аудита) и настроек механизмов ции событий.

8.2 Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только администратору информационной безопасности.