ПРИЛОЖЕНИЕ № 11
к приказу
от 6 августа 2024 г.
№ 65-ос

ПРАВИЛА
регистрации событий безопасности в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва

1. Общие положения

1.1. Настоящие Правила регламентируют состав и содержание информации о событиях безопасности, подлежащих регистрации, правила и процедуры сбора, записи, хранения и защиты информации о событиях безопасности в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва (далее – ИС Госкомохотнадзора РТ).

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

2.1. В ИС Госкомохотнадзора РТ подлежат регистрации в текущий момент времени события безопасности, утвержденные Перечнем событий безопасности в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва, подлежащих регистрации.

2.2. Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются в соответствии с пунктом 3 настоящих Правил.

2.3. Сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС Госкомохотнадзора РТ, в течение 3 месяцев.

2.4. Срок хранения информации о зарегистрированных событиях безопасности составляет не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации.

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. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, приведены в Перечне событий безопасности в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва, подлежащих регистрации.

4. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

4.1. Процедуры сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения предусматривают:

– возможность выбора администратором информационной безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в соответствии с Перечнем событий безопасности в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва, подлежащих регистрации;

– генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с Перечнем событий безопасности в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва, подлежащих регистрации, с составом и содержанием информации, установленными для соответствующего типа события;

– хранение информации о событиях безопасности в течение времени, установленного в соответствии с пунктом 2 настоящих правил.

4.2. Объем памяти для хранения информации о событиях безопасности рассчитывается и выделяется администратором информационной безопасности ИС Госкомохотнадзора РТ с учетом типов событий безопасности, подлежащих регистрации в соответствии с «Перечнем событий безопасности в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва, подлежащих регистрации», составом и содержанием информации о событиях безопасности, подлежащих регистрации, 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 ИС Госкомохотнадзора РТ реагирование на сбои при регистрации событий безопасности (в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти) должно предусматривать:

– предупреждение (сигнализация, индикация) администратора информационной безопасности 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 администратором информационной безопасности параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИС Госкомохотнадзора РТ, запись поверх устаревших хранимых записей событий безопасности.

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

6.1. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться администратором информационной безопасности не реже одного раза в неделю для всех событий, подлежащих регистрации в соответствии с Перечнем событий безопасности в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва, подлежащих регистрации, и обеспечивать своевременное выявление признаков инцидентов безопасности в ИС.

6.2. В случае выявления признаков инцидентов безопасности в ИС Госкомохотнадзора РТ администратор информационной безопасности осуществляет планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

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

7.1. В ИС Госкомохотнадзора РТ осуществляется генерирование надежных меток времени и синхронизация системного времени.

7.1.1. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИС Госкомохотнадзора РТ достигается посредством применения внутренних системных часов информационной системы или путем синхронизации системного времени.

8. Защита информации о событиях безопасности

8.1. Защита информации о событиях безопасности (записях регистрации (аудита) в ИС Госкомохотнадзора РТ должна обеспечиваться применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в проектной и организационно-распорядительной документации по защите информации, и в том числе

включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

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

Лист ознакомления
с Правилами регистрации событий безопасности в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				