ПРИЛОЖЕНИЕ № 18
к приказу
от 6 августа 2024 г.
№ 65-ос

ИНСТРУКЦИЯ
по выявлению инцидентов безопасности и реагированию на них

1. Общие положения и цели

Настоящая инструкция рассматривает вопросы обнаружения и реагирования на инциденты информационной безопасности (далее – ИБ) в Государственном комитете по охране объектов животного мира Республики Тыва (далее – Госкомохотнадзор РТ).

Под инцидентом информационной безопасности понимается любое неблагоприятное событие, в результате которого один из аспектов безопасности может подвергнуться угрозе, слабое место или неисправность системы безопасности.

Реагирование на инциденты безопасности осуществляется в целях:

1) гарантирования целостности информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – Информация);
2) сохранения и восстановления Информации;
3) выяснения причин того, почему инцидент стал возможен;
4) предотвращения развития вторжения и будущих инцидентов;
5) нахождения и наказания нарушителей.

2. Этапы реагирования на инциденты безопасности

Жизненный цикл реагирования на инциденты ИБ состоит из четырех стадий, которые следуют одна за другой и все вместе образуют непрерывный цикл:

1) обнаружение и регистрация инцидента;
2) устранение причин и последствий инцидента;
3) расследование инцидента;
4) реализация корректирующих мероприятий.

Настоящая инструкция должна пересматриваться после каждого инцидента ИБ и по необходимости.

3. Обнаружение инцидентов информационной безопасности

Информация об инцидентах ИБ может поступать по следующим каналам:

1) журналы регистрации событий операционной системы или средств защиты информации;
2) оповещения подсистемы антивирусной защиты или подсистемы обнаружения (предотвращения) вторжений;

3) информация, получаемая от работников Госкомохотнадзора РТ по любым каналам связи (телефон, электронная почта, речевой канал и т.д.).

Все процессы обнаружения инцидентов ИБ подлежат обязательному документированию.

4. Информирование об инцидентах

Администратор ИБ Госкомохотнадзора РТ совместно с администратором ИС Госкомохотнадзора РТ (далее – группа реагирования) несут ответственность за все процессы по обнаружению и реагированию на инциденты ИБ. Группа реагирования получает информацию о случившихся инцидентах и принимает меры по их устранению.

Работники, имеющие доступ к системе, в том числе те, кто осуществляет техническое сопровождение данной системы, обязаны при получении информации обо всех нетипичных событиях ИБ, незамедлительно сообщить группе реагирования.

Для оперативного получения информации об инцидентах ИБ группа реагирования имеет следующие каналы связи:

Телефон для обращения в рабочие часы с 9.30 до 18.00 в будние дни:	8-(394)-22-5-61-60
Телефон для обращений в нерабочее время:	89233841030
Адрес электронной почты:	Ohota-tuva@yandex.ru

К нетипичным событиям ИБ, о которых следует сообщать группе реагирования, относятся:

- крахи системы, перезагрузки системы;
- появление новых учетных записей;
- появление новых файлов;
- изменения в размерах и датах файлов;
- попытки записи в системные файлы;
- модификация или удаление данных (например, начали исчезать файлы);
- отказ в обслуживании;
- необъяснимо низкая производительность системы (например, необычно плохое время отклика системы);
- аномалии (например, появление сообщений на экране, частые и необъяснимые звуковые сигналы);
- подозрительные пробы (например, многочисленные неудачные попытки входа с другого узла сети);
- ошибки оператора;
- несоблюдение политик и руководств по ИБ другими работниками;
- нарушение физических мер обеспечения безопасности;
- неконтролируемое внесение изменений в систему;

– неправильное срабатывание программного или аппаратного обеспечения;

– нарушения доступа.

Неправильное срабатывание или другое аномальное поведение системы может стать индикатором атаки на безопасность или нарушения безопасности, и о них надо всегда докладывать, как о случае нарушения информационной безопасности.

Все работники, подрядчики и пользователи третьей стороны должны быть ознакомлены с процедурой информирования об инцидентах нарушения ИБ, а также проинформированы о необходимости незамедлительного сообщения об инцидентах и событиях ИБ.

Группа реагирования проводит сбор информации, связанной с событием, о котором поступило сообщение для того, чтобы убедиться, что инцидент ИБ действительно имеет место быть и локализовать область, задействованную в инциденте.

5. Реагирование на инциденты ИБ

Для реагирования на инциденты ИБ группа реагирования может привлекать по необходимости работников Госкомохотнадзора РТ и внешних экспертов. Необходимость привлечения тех или иных специалистов определяется в зависимости от вида инцидента.

Работники Госкомохотнадзора РТ могут привлекаться к реагированию на инциденты ИБ по согласованию с и. о. руководителя (председателя) Госкомохотнадзора РТ. Внешние эксперты привлекаются по согласованию с и. о. руководителя (председателя) Госкомохотнадзора РТ, при этом в обязательном порядке должно быть заключено письменное соглашение о конфиденциальности между Государственном комитете по охране объектов животного мира Республики Тыва и внешней стороной.

Все процессы реагирования на инциденты должны обязательно документироваться.

Первостепенной задачей группы реагирования является сдерживание инцидента ИБ, то есть принятие всех необходимых мер для локализации инцидента ИБ, препятствующих его распространению (при этом необходимо ограничить доступ к объектам, задействованным в инциденте ИБ). После сдерживания инцидента группа реагирования должна приступить в ликвидации последствий и восстановлению системы, то есть к приведению системы в нормальное состояние (при этом необходимо протоколировать все действия, которые осуществляются в ходе реагирования на инцидент). Далее группа реагирования проводит расследование инцидента и анализ случившегося.

Целью расследования инцидента ИБ является раскрытие всех причинно-следственных связей и получение следующей информации:

– источники инцидента ИБ (нарушители);

– цели инцидента ИБ;

– причины возникновения и способы осуществления инцидента ИБ;
– последствия инцидента ИБ.

6. Анализ причин и оценка результата

После проведения расследования инцидента ИБ группа реагирования проводит:

– принятие мер по устранению последствий произошедшего инцидента ИБ, в том числе по восстановлению ИС;
– переоценку рисков, повлекших возникновение инцидента ИБ;
– анализ перечня защитных мер для минимизации выявленных рисков в случае повторения инцидента ИБ;
– анализ инструкций и правил ИБ, включая настоящий документ;
– планирование и принятие мер по устранению инцидентов;
– планирование и принятие мер по предотвращению повторного возникновения инцидентов;
– по необходимости обучение (информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации) персонала Госкомохотнадзора РТ для повышения их осведомленности в части ИБ.

Раз в три месяца, а также по необходимости, группа реагирования готовит и предоставляет и.о. руководителя (председателя) Госкомохотнадзора РТ отчеты по проведенной работе по расследованию инцидента ИБ с указанием предлагаемых мероприятий, направленных на снижение ущерба от подобных инцидентов ИБ.

Лист ознакомления

с Инструкцией по выявлению инцидентов безопасности и реагированию на них

№ 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.				