План реагирования на инциденты информационной безопасности

Код документа: ИБ-04
Организация: ИП MAMBETNAZAROV ATANAZAR DJOLDASBAEVICH
Основание деятельности: Регистрационный номер ИП: 7425011 • МХИК: 10305013002000000

Версия: 1.0
Статус: проект / шаблон для адаптации

Поле для утверждения:
УТВЕРЖДАЮ: _____
Должность/ФИО: _____
Подпись: _____
Дата: _____

Примечание: документ предназначен для внутреннего использования и требует адаптации под конкретные процессы, применяемые СКЗИ и требования заказчиков/регуляторов.

Содержание

1. Цель и область применения

План определяет порядок обнаружения, регистрации, классификации и обработки инцидентов информационной безопасности, включая инциденты, связанные со средствами криптографической защиты информации (СКЗИ), ключевыми носителями и сертификатами.

2. Определения и классификация инцидентов

Под инцидентом ИБ понимается событие или серия событий, приводящих или способных привести к нарушению конфиденциальности, целостности или доступности информации.

2.1. Примеры инцидентов

- Потеря или кража ключевого носителя (токен/смарт-карта).
- Компрометация PIN/пароля или ключевого материала.
- Неавторизованное изменение конфигурации СКЗИ/криптосервисов.
- Сбой криптосервиса, влияющий на бизнес-процессы (подпись/шифрование/VPN).
- Подозрение на вредоносное ПО на рабочем месте с ключевыми операциями.

2.2. Уровни критичности (пример)

Уровень	Описание	Целевое время реакции (пример)
Критический	Компрометация ключа, массовая недоступность криптосервисов, утечка конфиденциальных данных	до 1 часа
Высокий	Потеря носителя без подтвержденной компрометации, доказанное нарушение доступа	до 4 часов
Средний	Сбой отдельных операций/клиентских компонентов без потери данных	до 1 рабочего дня
Низкий	Запросы на консультации, ложные срабатывания	по плану

3. Роли, ответственность и каналы связи

Назначьте контактных лиц и каналы уведомления (заполнить):

Роль	ФИО	Телефон	Email/мессенджер
Ответственный за ИБ			
Администратор СКЗИ			
Администратор инфраструктуры			
Владелец системы/бизнес			

4. Процесс реагирования (этапы)

Процесс состоит из последовательных этапов; часть шагов может выполняться параллельно.

4.1. Обнаружение и регистрация

- Получить сообщение (пользователь, мониторинг, журнал, внешний источник).
- Зарегистрировать инцидент: время, источник, краткое описание, затронутые системы.
- Назначить ответственного и уровень критичности.

4.2. Триаж и оценка

- Подтвердить факт инцидента, исключить ложное срабатывание.
- Оценить воздействие: какие данные/системы затронуты, есть ли риск компрометации ключей.
- Определить первичные меры локализации.

4.3. Локализация (containment)

- Ограничить распространение: изоляция узла, блокировка учетной записи, ограничение сети (по необходимости).
- Остановить нежелательные процессы/доступы при сохранении доказательств.
- Обеспечить сохранность журналов и артефактов.

4.4. Устранение и восстановление

- Устранить причину: удаление вредоносного ПО, исправление конфигурации, обновление.
- Восстановить сервисы из резервных копий/эталонных конфигураций.
- Провести проверку работоспособности и контрольные тесты.

4.5. Пост-инцидентный анализ

- Сформировать отчет: что произошло, почему, последствия, принятые меры.
- Определить корректирующие действия (процессы, настройки, обучение).
- Обновить регламенты/политику при необходимости.

5. Особые случаи: инциденты с ключами и СКЗИ

5.1. Подозрение на компрометацию ключа/носителя

- Немедленно инициировать отзыв сертификата (если применимо) и блокировку доступа.
- Зафиксировать обстоятельства: где хранился носитель, кто имел доступ, какие операции выполнялись.
- Организовать выпуск нового ключа/сертификата и замену в системах.
- Обновить журналы учета ключевых носителей и выдачи/отзыва.

5.2. Нарушение целостности конфигурации СКЗИ

- Сверить конфигурацию с эталоном/резервной копией.
- Определить, кто и когда вносил изменения (по журналам).
- Восстановить корректные настройки и ограничить административный доступ до выяснения причин.

6. Сбор и сохранение доказательств

- Сохранить журналы событий, системные логи, конфигурации, дампы (по необходимости) с указанием времени и ответственного.
- Обеспечить целостность: контрольные суммы, ограничение доступа к артефактам.
- Не изменять исходные артефакты без необходимости; работать с копиями.

7. Коммуникации и отчетность

- Уведомление владельца системы/руководства - согласно уровню критичности.
- Уведомление пользователей - по утвержденному тексту, без раскрытия избыточных деталей.
- При необходимости - взаимодействие с подрядчиками/вендорами по каналам поддержки.
- Финальный отчет хранится в защищенном архиве; выводы используются для улучшения процессов.

8. Приложения

Приложение А. Карточка инцидента (шаблон)

Поле	Значение
ID инцидента	
Дата/время обнаружения	
Источник	
Затронутые системы	
Описание	
Критичность	
Ответственный	
Принятые меры (локализация)	

Поле	Значение
Устранение и восстановление	
Итог/последствия	
Корректирующие действия	

Приложение Б. Чек-лист компрометации ключа (пример)

- 1) Зафиксировать факт/подозрение, зарегистрировать инцидент.
- 2) Изъять/заблокировать носитель (если возможно), ограничить доступ пользователя.
- 3) Отозвать сертификат и распространить информацию об отзыве (CRL/OCSP).
- 4) Проверить журналы операций подписи/шифрования за период риска.
- 5) Выпустить новый ключ/сертификат, установить в системах, проверить сценарии.
- 6) Обновить журналы учета и уведомить заинтересованных.
- 7) Подготовить отчет и меры предотвращения повторения.