Регламент администрирования и обновлений СКЗИ

Код документа: ИБ-02
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. Назначение и область действия

Настоящий регламент устанавливает порядок администрирования, сопровождения и обновления СКЗИ и компонентов криптографической инфраструктуры. Документ применяется при работах на серверной и клиентской части, а также при обслуживании интеграций.

2. Объекты администрирования

- СКЗИ на рабочих станциях пользователей (криптопровайдеры, средства подписи/шифрования, токены/смарт-карты).
- СКЗИ на серверах (службы подписи/шифрования, VPN-шлюзы, серверы управления, HSM - при наличии).
- Инфраструктура сертификатов (CA/RA, хранилища, списки отозванных сертификатов, политики).
- Журналы и средства мониторинга, связанные с криптографическими сервисами.

3. Требования к доступу и рабочим местам администраторов

- Администрирование выполняется с выделенных учетных записей, не используемых для повседневной работы.
- Доступ предоставляется по заявке, с ограничением по времени/задаче (при необходимости).
- Рекомендуется 2FA для административных учетных записей.
- Удаленное администрирование допускается только через защищенные каналы (VPN/SSH/TLS) и с журналированием сессий.

4. Резервное копирование конфигураций и данных

Минимальный набор резервирования:

- Конфигурации СКЗИ, политики, списки доверенных сертификатов/ЦС.
- Конфигурации серверов и сетевых устройств, влияющих на криптоконтур.
- Журналы (если требуются для расследований и отчетности).
- Критичные параметры - по правилам ключевой дисциплины (см. Политику ИБ).

Резервные копии хранятся в защищенном месте с ограниченным доступом. Периодичность, сроки хранения и ответственные лица устанавливаются организацией и фиксируются в плане резервного копирования.

5. Порядок выполнения изменений и обновлений

5.1. Инициация изменения

- Заявка на изменение (что меняем, почему, затронутые компоненты, риски).
- План работ: окно изменений, ответственные, коммуникации, критерии успеха.
- План отката: шаги возврата к предыдущей версии/конфигурации.

5.2. Подготовка и тестирование

- Сбор текущих версий и зависимостей (ОС, библиотеки, драйверы токенов, криптопровайдер).
- Проверка совместимости новой версии с инфраструктурой и приложениями.
- Тестирование на стенде/пилотной группе: основные сценарии (подпись, шифрование, VPN, выпуск/проверка сертификатов).

5.3. Внедрение обновления

- Создание резервной копии конфигураций и критичных данных перед началом работ.
- Пошаговое выполнение обновления по инструкции производителя/вендора.
- Фиксация фактических действий в журнале работ (кто, когда, что сделано).
- Проверка работоспособности по чек-листу и подтверждение владельцем системы/ответственным.

5.4. Откат

При возникновении критических ошибок выполняется откат в соответствии с планом отката. Решение об откате принимает ответственный за внедрение совместно с владельцем системы (или уполномоченным лицом).

6. Работа с уязвимостями и бюллетенями

- Ответственный за сопровождение отслеживает бюллетени безопасности вендоров и актуальность версий.
- Каждое уведомление оценивается по критичности и влиянию на объект эксплуатации.
- Для критичных уязвимостей устанавливаются приоритетные сроки устранения и временные компенсирующие меры (если требуется).

7. Журналирование работ и отчетность

Ведутся следующие записи (минимум):

- Журнал административных работ (изменения, обновления, устранение неисправностей).
- Журнал инцидентов/сбоев (классификация, время, действия, результат).
- Реестр версий и конфигураций (текущие версии СКЗИ и ключевых компонентов).

Отчетность предоставляется по запросу владельца системы и/или по условиям SLA.

8. Плановые проверки и контроль

- Ежемесячно/ежеквартально: проверка актуальности версий, сроков сертификатов, корректности времени (NTP), доступности CRL/OCSP.
- Периодически: контроль прав доступа администраторов, ревизия учетных записей и привилегий.
- Проверка резервного копирования и тестовое восстановление (не реже 1 раза в [__] месяцев).

9. Приложения

Приложение А. Чек-лист обновления СКЗИ (пример)

- 1) Получить согласование окна работ и уведомить заинтересованных.
- 2) Снять версии и зависимости, зафиксировать текущую конфигурацию.
- 3) Сделать резервную копию конфигураций/данных.
- 4) Выполнить обновление согласно инструкции вендора.
- 5) Проверить ключевые сценарии (подпись/шифрование/VPN/проверка сертификата).
- 6) Зафиксировать результаты, обновить реестр версий.

- 7) При проблемах - выполнить откат и оформить инцидент.

Приложение Б. План регламентных работ (шаблон)

Периодичность	Работа	Ответственный	Отметка/комментарий
Еженедельно	Проверка доступности криптосервисов и журналов ошибок	Администратор	
Ежемесячно	Проверка сроков сертификатов, CRL/OCSP, корректности времени	Администратор СКЗИ	
Ежеквартально	Ревизия доступов администраторов и ключевых ролей	Ответственный за ИБ	
Раз в [__] мес.	Тестовое восстановление из резервной копии	Администратор инфраструктуры	