Политика информационной безопасности и ключевая дисциплина

Код документа: ИБ-01
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

Настоящая Политика определяет базовые требования к обеспечению информационной безопасности и ключевой дисциплины при проектировании, внедрении, эксплуатации и обслуживании средств криптографической защиты информации (СКЗИ) и связанной инфраструктуры.

- Политика обязательна для владельца системы, администраторов, пользователей и подрядчиков, допущенных к работам.
- Требования применяются ко всем системам, где используются криптографические ключи, сертификаты, контейнеры ключей и средства подписи/шифрования.
- Документ является шаблоном и должен быть адаптирован под конкретный объект и применяемые СКЗИ.

2. Основные принципы

- Минимально необходимый доступ (least privilege) и разделение ролей.
- Непрерывность защиты: требования учитываются на всех этапах жизненного цикла (проектирование, внедрение, эксплуатация, вывод из эксплуатации).
- Контроль изменений и воспроизводимость конфигураций.
- Трассируемость: действия администрирования и ключевые операции фиксируются в журналах.
- Приоритет обеспечения целостности и конфиденциальности ключевого материала.

3. Роли и ответственность

Рекомендуемый набор ролей (может быть расширен):

Роль	Ответственность (кратко)
Владелец системы	Утверждает требования ИБ, назначает ответственных, принимает риски.
Администратор СКЗИ	Настройка СКЗИ, выпуск/установка сертификатов, обслуживание, обновления, ведение журналов.
Администратор инфраструктуры	ОС/серверы/сеть, резервное копирование, управление учетными записями инфраструктуры.
Пользователь	Соблюдает правила хранения ключевых носителей, использует СКЗИ по инструкции, сообщает об инцидентах.
Ответственный за ИБ	Контроль соблюдения, анализ инцидентов, аудит настроек, обучение.

4. Классификация информации и требования к защите

Информация и активы классифицируются для определения требуемых мер защиты.

- Открытая: допускается распространение без ограничений.
- Для служебного пользования: доступ ограничен сотрудникам/подрядчикам по необходимости.
- Конфиденциальная: коммерческая/персональные данные/служебная тайна; требуется контроль доступа, шифрование при хранении/передаче.

- Ключевая: криптографические ключи, PIN/PUK, seed-значения, ключевые контейнеры ключей; максимальные требования защиты.

Ключевой материал не должен передаваться в открытом виде, копироваться или храниться в местах, не предназначенных для этого, если иное не предусмотрено утвержденными процедурами.

5. Криптографическая защита и применение СКЗИ

СКЗИ применяются для обеспечения конфиденциальности, целостности и аутентичности данных.

- Выбор СКЗИ и режимов работы выполняется на этапе проектирования и фиксируется в технической документации.
- Используются только разрешенные организацией алгоритмы/криптопровайдеры и поддерживаемые версии.
- Ключевые операции выполняются в доверенной среде (выделенные рабочие места/серверы, при необходимости - аппаратные модули).
- Секретные параметры (PIN/пароли) не передаются по незащищенным каналам; допускается передача по принципу разделенного знания.

6. Ключевая дисциплина

Ключевая дисциплина - совокупность правил генерации, учета, хранения, использования, смены и уничтожения ключей.

6.1. Генерация и выпуск

- Ключи генерируются на доверенном устройстве/в СКЗИ с использованием штатных механизмов.
- Назначается ответственное лицо за выпуск ключей/сертификатов; обеспечивается разделение ролей при критичных операциях.
- Параметры ключей и срок действия фиксируются в журнале учета.

6.2. Хранение и использование

- Ключевые носители (токены/смарт-карты) хранятся у владельца либо в сейфе/контейнере с учетом выдачи и возврата.
- PIN/PUK хранится отдельно от носителя; запрещено хранить PIN вместе с носителем.
- Запрещена передача ключевых носителей третьим лицам без оформленной процедуры.
- При отсутствии пользователя носитель извлекается из устройства (если применимо).

6.3. Смена, отзыв и уничтожение

- Плановая смена ключей выполняется согласно установленному графику либо по истечении срока действия.
- При подозрении на компрометацию выполняется немедленный отзыв сертификата и выпуск нового ключевого материала.
- Уничтожение/утилизация носителей и контейнеров производится документально с отметкой в журнале.

6.4. Резервное копирование ключей (если допускается)

Резервирование ключевого материала допускается только при наличии утвержденной процедуры и при условии, что это не противоречит требованиям применяемого СКЗИ и модели угроз. Копии хранятся в защищенном виде, с ограниченным доступом и учетом операций.

7. Управление доступом и учетными записями

- Доступ предоставляется на основании заявки/распоряжения и утверждается владельцем системы или ответственным за ИБ.
- Учетные записи администраторов являются персональными; совместное использование учетных данных запрещено.
- Критичные операции выполняются под повышенным контролем (двухфакторная аутентификация, разделение ролей).
- При увольнении/смене роли доступы отзываются незамедлительно.

8. Журналирование и мониторинг

- Фиксируются: входы в систему, операции администрирования, выпуск/отзыв сертификатов, изменения конфигураций, ошибки и аварии.
- Журналы защищаются от изменения и хранятся не менее [__] месяцев (значение задать организацией).
- Подозрительные события анализируются ответственным за ИБ; при необходимости инициируется реагирование на инцидент.

9. Управление изменениями

Изменения конфигурации, обновления и модернизация выполняются по заявке на изменение, с оценкой рисков и планом отката. Рекомендуется выделенный тестовый контур и подтверждение работоспособности до ввода в промышленную эксплуатацию.

10. Обучение и контроль соблюдения

- Пользователи и администраторы проходят вводный и периодический инструктаж по ИБ и правилам обращения с ключевыми носителями.
- Проводится выборочный контроль соблюдения требований (аудит журналов, проверка актуальности доступов).
- Нарушения фиксируются; корректирующие меры назначаются ответственным лицом.

11. Пересмотр документа

Политика пересматривается не реже 1 раза в год или при существенных изменениях инфраструктуры, внедрении новых СКЗИ, изменении требований заказчика/регулятора или по итогам инцидента.

12. Приложения

Приложение А. Пример матрицы ролей и операций

Операция	Владелец системы	Администратор СКЗИ	Пользователь	Ответственный за ИБ
Выпуск ключей/сертификатов	Утверждает	Выполняет	Получает	Контролирует
Отзыв сертификата	Утверждает/инициирует	Выполняет	Сообщает	Контролирует
Изменение настроек СКЗИ	Утверждает	Выполняет	-	Контролирует
Доступ к журналам	Читает	Пишет/читает	-	Читает/анализирует

Приложение Б. Поля для адаптации

- Перечень применяемых СКЗИ и систем (приложить список).
- Сроки хранения журналов, правила резервного копирования.
- Контактные лица и порядок согласования доступов/изменений.
- Требования заказчиков/регуляторов, применимые к конкретным проектам.