Как быстро навести порядок в ИБ-процессах: первые 90 дней руководителя ИБ

Без процессной основы любое внедренное СЗИ — это просто красивый аксессуар

Насущные вызовы эксплуатации СЗИ в информационной безопасности

В ряде организаций процессы эксплуатации СЗИ остаются на начальной стадии развития: требуются уточнение ролей, формализация регламентов и единый подход к мониторингу и поддержке СЗИ.

«Без процесса эксплуатация СЗИ это имитация безопасности»

Фокус первых 90 дней: управляемость, а не технологии СЗИ

01

Для начала необходимо провести глубокий аудит текущих процессов, владельцев и выявить уязвимые места в ИБ-системе организации и процессы взаимодействия.

02

Следующим шагом — устранение критических пробелов и уязвимостей, которые могут привести к серьезным инцидентам, чтобы стабилизировать состояние безопасности.

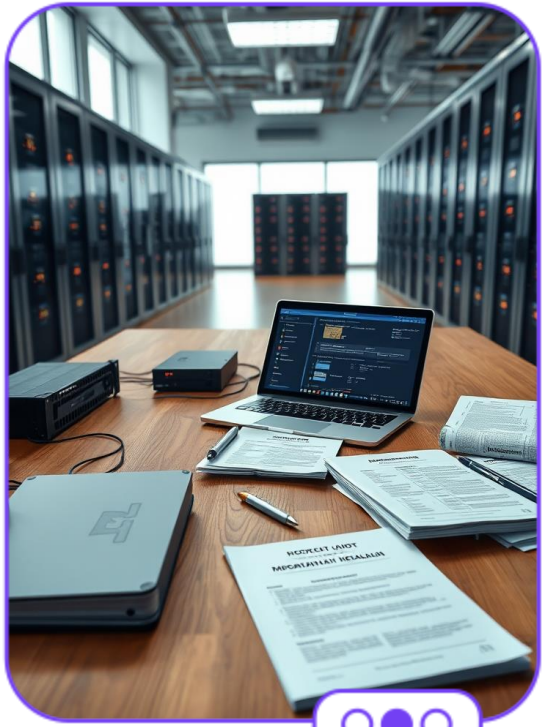
03

Важнейшая задача — создание процессной основы с четким распределением ролей и контролем, поскольку без этого любые технологии СЗИ теряют эффективность.

Аудит и легализация реального состояния ИБ за первые 30 дней

01

Проводится полный инвентаризационный аудит парка СЗИ, проверяется актуальность используемых решений и распределение ролей между сотрудниками по их эксплуатации.



02

Выявляются разрывы между ИТ и ИБ, собирается подробная информация о лицензиях, обновлениях и соответствии требований ФСТЭК и ФСБ, чтобы построить реалистичную картину.

Период 30–60 дней: разработка управляющей системы эксплуатации СЗИ

01

Формируется RACI-матрица, которая распределяет роли и ответственности между ИТ и ИБ для эффективного взаимодействия и контроля операций.

02

Создается краткая процессная модель, охватывающая основные операции: управление доступом, инцидентами, изменениями и вводом в эксплуатацию.

03

Разрабатываются минимальные регламенты для ключевых систем СЗИ: NGFW, EDR, DLP, SIEM, обеспечивающие единые стандарты эксплуатации и сопровождения.

04

Начинается внедрение SOC-light — упрощенного центра мониторинга с логированием, корреляциями и каналами оповещений для быстрой реакции.

Распределение ролей и ключевые процессы эксплуатации СЗИ

Таблица сопоставляет ключевые роли с основными процессами эксплуатации СЗИ для повышения прозрачности и управления.

Роль	Инцидент-менеджмент	Обновления	Мониторинг	Интегратор
Владелец	Контроль и утверждение	Назначение ответственных	Проверка метрик	Утверждение требований
Исполнитель	Обработка и эскалация	Выполнение обновлений	Сбор и анализ логов	Взаимодействие и отчеты
Ответственный за обновления	Согласование сроков	Планирование и выполнение	Отчетность	Контроль SLA
Ответственный за мониторинг	Мониторинг событий	Проверка статуса обновлений	Анализ тревог	Сопровождение процессов
Ответственный за лицензии	Отслеживание сроков	Обновление контрактов	Поддержка системы	Коммуникация с подрядчиками

Четкое распределение ответственности по процессам обеспечивает прозрачное и эффективное управление эксплуатацией СЗИ.

Пример наведения порядка: от хаоса к управляемости за 90 дней

Исходная точка: СЗИ без владельцев, процессов и регламентов

В организации существовал разрозненный парк СЗИ со множеством решений разных поставщиков, но без ясных владельцев и регламентов. Лицензии истекали незаметно, инциденты не расследовались, SIEM не использовалась по прямому назначению.

Назначение ролей и создание регламентов

Руководитель ИБ внедрил RACI-матрицу с ясным распределением ролей и создал короткие, практичные регламенты по эксплуатации каждого СЗИ-компонента для обеспечения управляемости и ответственности.

Внедрение централизованного управления и мониторинга

Был запущен единственный ServiceDesk для учета задач, введено регулярное обновление и актуализация корреляций в SIEM, реализован SOC-light с четкой схемой реагирования и SLA по ключевым процессам.

Итог первых 90 дней: устойчивая основа для зрелого ИБ

День 30: Аудит и инвентаризация

Завершен комплексный аудит парка СЗИ, выявлены разрывы и состояние лицензий для точной оценки текущего положения.

День 45: Разработка RACI и процессов

Созданы матрица ответственности и краткие регламенты для ключевых компонентов, формируются первые управляющие модели.

День 75: Внедрение SOC-light и мониторинга

Запущена минимальная аналитическая платформа для отслеживания и реагирования на инциденты в режиме реального времени.

День 90: Старт полноценного процесса эксплуатации

Установлены SLA, сформирован реестр ИС и карта рисков, обеспечена прозрачность и контроль исполнения задач.

Заключение: построение управляемой системы ИБ за 90 дней

Выстроенная эксплуатация СЗИ формирует основу эффективной системы ИБ, обеспечивая контроль инцидентов, лицензий и ответственности для дальнейшего развития и защиты бизнеса.