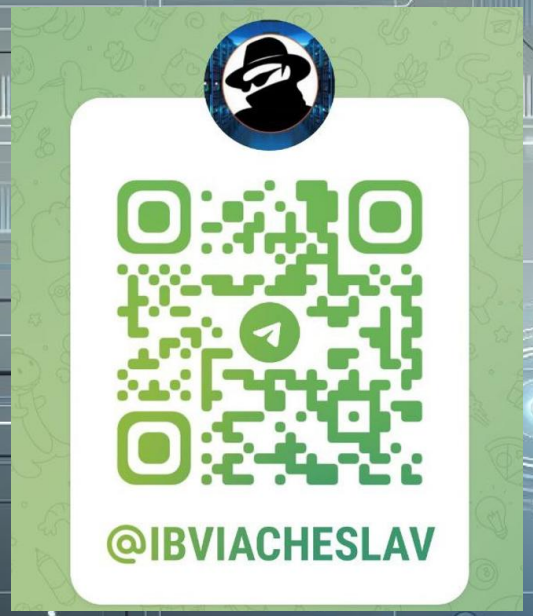
Project Management в информационной безопасности



Управление проектами в информационной безопасности

Казань 2025

Бачурин Вячеслав

Забывая об управлении проектами в ИБ, компания превращает безопасность в хаотичную реакцию — вместо стратегической защиты, теряет контроль, бюджет, время и в конечном итоге — бизнес-устойчивость.

Что происходит, когда в компании забывают про управление проектами в информационной безопасности

К Е Й С

Внедрение DLP-системы

Кредитной организации нужно повысить оценку соответствия ГОСТ Р 57580 через внедрение DLP-системы

Этап 1: Постановка задачи («Нам нужно DLP, и всё»)

Начальник отдела управления рисками направляет требование в отдел ИБ :
«Повысить оценку по ГОСТ Р 57580 — нужно закрыть риск утечки информации.
Внедрите DLP в срок не позднее 4 квартала 2025 года» .

Начальник ИБ

Да, DLP — это то, что нужно. Купим что ни будь по быстрому, чтобы успеть к аудиту».

Специалисты начинают гуглить «лучшие DLP-системы», сравнивают цены, звонят вендорам.

Специалисты ИБ

Этап 1: Постановка задачи («Нам нужно DLP, и всё»)

Никто не определяет:

→ Что именно нужно защищать?
→ Какие каналы утечки (email, USB, облачные сервисы)?
→ Какие бизнес-процессы будут затронуты?
→ Кто ответственный?
→ Как измерять успех?

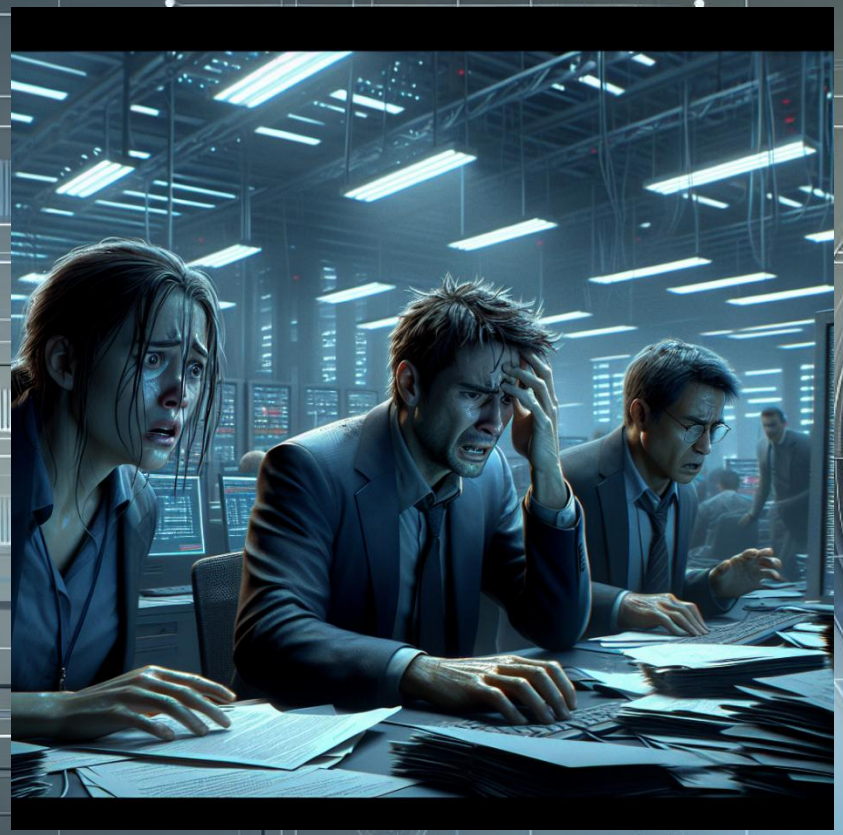
Нет чёткой цели, нет требований, нет плана.
→ Проект начинается с «надо» вместо «зачем».

Этап 2: Выбор и закупка («Купили, потому что дешевле и быстрее»)

Что делают:
Выбирают DLP-систему, потому что:
→ у вендора хороший презентационный ролик.
→ скидка 20% при закупке до конца месяца.
→ «у конкурентов внедрено — значит, нормально».
Никто не тестирует на реальных данных, не оценивает интеграцию с Active Directory, почтовыми серверами, облачными хранилищами.

Результат этапа:
Выбрана система, которая не подходит под бизнес-процессы банка.
→ Пользователи не могут работать — DLP блокирует легитимные операции.
→ Начинаются жалобы, «обходные пути», отключение системы.

Этап 3: Внедрение («Пусть IT установит — мы потом настроим»)



Что делают:
Проект передаётся IT-отделу: «Установите, настройте, как получится».
Нет плана внедрения, нет этапов: пилот → тест → полное внедрение.
Нет коммуникации с бизнес-подразделениями:
→ Юристы не знают, какие документы будут блокироваться.
→ Операционный отдел не понимает, почему не отправляются платежки.
Нет обучения пользователей — «сами разберутся».

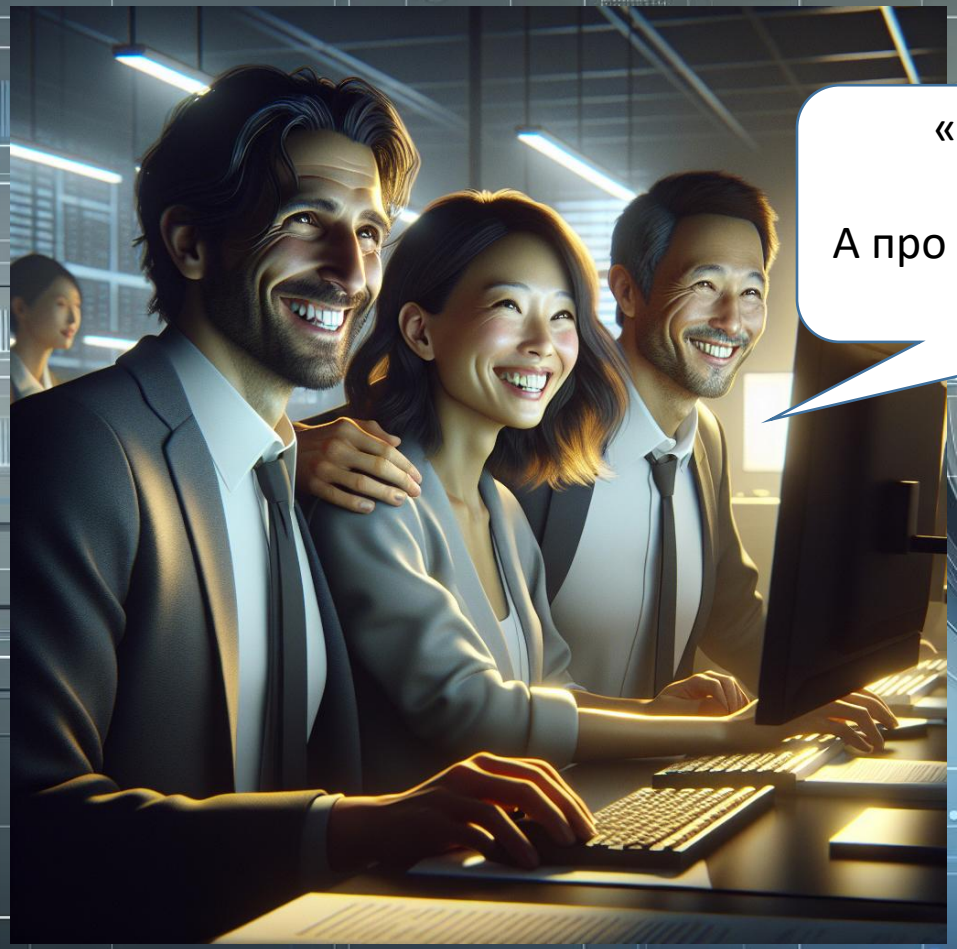
Результат этапа:
Система работает, но мешает бизнесу.
→ Работа замедляется.
→ Пользователи обходят DLP через личные почты, мессенджеры, USB.
→ Проблему утечек не решили — просто утечки стали «незаметнее».

Этап 4: Последствия («Мы всё испортили, но никто не виноват»)

Что делают:
DLP отключают или оставляют в «тестовом режиме» — без реальной защиты.

Результат этапа:
Потеря денег, времени, доверия, безопасности.
→ Банк не соответствует стандартам.
→ Риск утечки данных остаётся.
→ Управление проектами в ИБ — так и остаётся «не нужным».

Этап 5: Аудит и оценка («Мы же поставили DLP — значит, соответствуем требованиям»)



«У нас DLP стоит — вот лицензия».
А про остальное — не знали, что нужно».

→ Какие политики настроены?
→ Какие инциденты зафиксированы?
→ Какова эффективность блокировки?
→ Есть ли отчёты по нарушениям?

Аудит провален.
→ Не соответствует ГОСТ 57580 — нет доказательств эффективности.→ Штрафы, предписания, репутационные риски.
→ Руководство Банка в шоке: «Мы же потратили огромную сумму денег»

Вывод по кейсу:

Забывая об управлении проектами, компания превращает внедрение защиты информации, в дорогостоящую и бесполезную процедуру — вместо инструмента защиты, проект становится источником хаоса, сопротивления и рисков.

Что нужно было сделать

Фаза: ИНИЦИАЦИЯ (Прежде чем что-то делать)

Цель: Не просто "повысить оценку по ГОСТу", а "внедрить работающую систему защиты от утечек данных, которая соответствует требованиям ГОСТ Р 57580 и снижает реальные риски".

Просто сказать "внедрить DLP" — это **не цель**, это задача. Цель должна быть **конкретной, измеримой, достижимой, релевантной и ограниченной во времени (SMART)**.

Цель 1: Повысить оценку соответствия требованиям ГОСТ Р 57580 на 5 пунктов к 31 декабря 2025 года."

Цель 2: Снизить количество инцидентов утечки информации на 20% в течение 6 месяцев после внедрения DLP.
Можно посчитать количество инцидентов до и после внедрения DLP.

Результат: Уже на этом этапе стало бы ясно, что **главная цель** — не купить софт, а получить работающую защиту. Это меняет весь фокус.

Что нужно было сделать

Фаза: ПЛАНИРОВАНИЕ

Сбор требований: Вместо одного человека, принимающего решение, нужно создать список того, что нужно от DLP всем. Появиться **список условий**, при которых DLP будет *принята* работниками и будет *работать*, а не висеть мертвым грузом.

Составить "дорожную карту" (План проекта). В этом плане есть четкие **этапы и сроки:** Неделя 1: Выбор поставщика; Неделя 2-3: Юридическая подготовка; Неделя 4: Разрабатываем «Инструкцию для сотрудников»; Месяц 2: Пилотирование. Установка. Постепенное подключение агентов и настройка; Месяц 3: После того, как все привыкли, и система настроена под бизнес-процессы, переводим ее в рабочий режим с блокировкой.

Назначить "команду мечты" (Управление людьми)
Начальник отдела ИБ понимает: если он один тянет эту телегу, ничего не выйдет. Он заранее **договаривается с ключевыми работниками**: С Юристом: "Ты отвечаешь за то, чтобы все документы были в порядке". Начальником отдела кадров: "Ты помогаешь донести эту информацию до всех сотрудников и собрать с них подписи". С Начальниками отделов: "Вы — мои главные союзники. Объясните своим ребятам, зачем это нужно, и сообщайте мне, если система где-то "глючит" и мешает работе".

Что нужно было сделать

Управление качеством: Систему настраивать не "как получится", а в строгом соответствии с теми требованиями, что собрали на этапе планирования.

Фаза: ИСПОЛНЕНИЕ

Начальнику ИБ как мост между "железкой" DLP и живыми людьми. Процесс внедрения должен проходит гладко, прозрачно и с минимальным дискомфортом для бизнеса.

Именно эти действия не дали бы системе уйти в "вечный тестовый режим". Потому что люди бы ее не саботировали, а приняли как полезный, хоть и немного строгий, инструмент.

Развитие команды и управление коммуникациями: На фазе "Исполнение" начальник отдела ИБ должен был превратиться из "технаря и руководителя " в **активного лидера и переговорщика.**

Что нужно было сделать

Фаза: МОНИТОРИНГ И КОНТРОЛЬ (Постоянный процесс)

Вместо того чтобы просто смотреть, "работает ли сервер DLP", нужно отслеживать ключевые показатели, которые были определены на этапе планирования:

Процент охвата рабочих мест: Не "охвачено 100%", а "95% агентов в активном режиме, 5% требуют вмешательства".

Количество инцидентов: "Система регистрирует в среднем 10 попыток некритичного нарушения в день и 1 серьезную блокировку в неделю". Если инцидентов ноль — это не повод для радости, а красный флаг. Это значит, что система либо не настроена, либо не работает.

Процент ложных срабатываний: "Настроены ли политики так, чтобы не мешать работе? Если бухгалтерия не может отправить отчет из-за DLP — это не их проблема, а проблема проекта, которую нужно срочно решить".

Проводить совещания по проекту :

Раз в неделю/месяц собирать всех заинтересованных лиц и задавать три простых вопроса:

1. Что сделано по плану? (По плану мы должны были настроить политики для бухгалтерии. Готово?)
2. Что пошло не так? (Отдел продаж жалуется, что система блокирует легальные рассылки. Почему?)
3. Что делаем, чтобы исправить? (Кто, к какому сроку и как настроит политики для отдела продаж?)

Что нужно было сделать

Фаза: ЗАВЕРШЕНИЕ

Главная цель фазы завершения — формально подтвердить, что проект выполнил все поставленные цели, и передать результат. Это не просто "все, деньги потрачены", а "вот, пожалуйста, работающий продукт, документы и закрытые требования".

Вывод: Завершение проекта — это не вздох облегчения "слава богу, всё позади", а финишный рывок, который превращает вложения в реальную ценность. Это тот самый момент, когда "купленная деталь" начинает работать на бизнес.

Итог: Завершение проекта характеризуется успешным развертыванием работоспособной системы предотвращения утечек данных, удовлетворяющей положениям ГОСТ Р 57580 и направленной на минимизацию реальных рисков.

Что нужно было сделать

- Инициация
- Составление плана
- Реализация плана
- Отслеживание прогресса
- Закрытие проекта

Project Management
это не просто набор правил, а структурированный подход к управлению проектами. Если бы Банк следовал этим принципам, он бы сэкономил деньги, время и нервы, и добился реального повышения безопасности.

Информационная безопасность

Agile

PMBOK

PMI

Project Management в информационной безопасности

@IBVIACHESLAV

Управление проектами в информационной безопасности

Казань 2025

Бачурин Вячеслав