Стратегия ИБ с нуля

Ташкеев Владимир,

директор департамента консалтинга Infosecurity, ГК Softline

Я хожу на работу каждый день.

Я почти наверняка знаю, чем буду заниматься завтра.

Я довольно детально знаю, чем буду заниматься через месяц.

Я примерно знаю, чем буду заниматься через год.

Значит у меня есть какой-то план, а это и есть стратегия.

(с) Автор пожелал остаться неизвестным

Зачем разрабатывать Стратегию?

- Бизнес должен адаптироваться к изменениям (продукты и услуги, контекст, законодательство)
    - *Справедливо ли это к ИБ?*
- Масштабы бизнес выросли кратно
    - *Справедливо ли это к ИТ?*
    - *А к ИБ?*
- Бизнес ждет реструктуризация/изменение ключевого профиля деятельности
    - *ИБ в курсе?*

Основной вопрос: как развивать ИБ, что делать в первую очередь, а что может подождать?

Основной результат: портфель проектов и бюджет инвестиций

Бонус! Наличие стратегии помогает с обоснованием бюджета и штатных единиц!

Этапы разработки

Текущее состояние ИБ (AS-IS)

Оценка зрелости процессов ИБ

1 Анализ контрольной среды

- Анализ документации
- Проведение интервью

2 Оценка контрольной среды

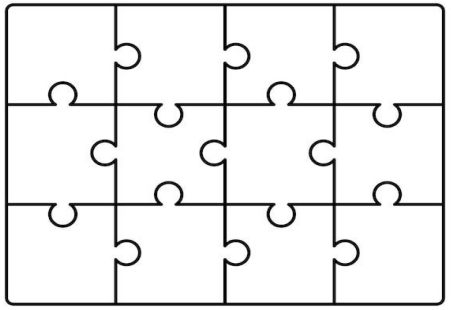
- ISO 27001/ 27002
- CIS Controls

Определение уровня зрелости ИБ

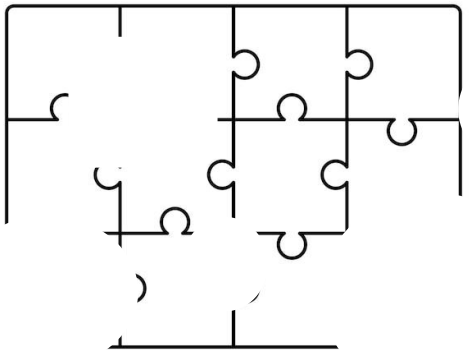
Анализ контекста (1)

Бизнес-цели и инициативы

Идеальная картина



Реальная картина



- Хорошо, если бизнес-стратегия и ИТ-стратегия существуют в документированном виде, и их можно почитать.
- В любом случае, у нас есть достаточно возможностей для сбора информации:
  - интервью менеджмента от бизнеса и ИТ;
  - анализ портфеля проектов.
- В результате мы должны получить:
  - ключевые направления бизнеса и взаимосвязи с ИТ-ландшафтом;
  - ключевые изменения в бизнесе и ИТ в ближайшие 1-3 года;
  - наиболее критичные для бизнеса рисковые сценарии в ИБ («недопустимые события»).

Анализ контекста (2)

Тренды угроз ИБ:

- развитие социальной инженерии
- шифровальщики/вымогатели
- целевые атаки
- базовые атаки на веб-ресурсы
- атаки на цепочки поставок
- ИИ в арсенале зломышленников ??

Регуляторный контекст:

- Критическая информационная инфраструктура, обработка персональных данных
- отраслевое регулирование (финансовые организации, разработка ПО, кибербез автомобилей и т.д.)

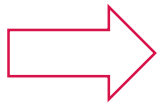
Тренды развития решений ИБ:

- zero trust architecture
- privacy by design
- от кибербезопасности – к киберустойчивости
- ИИ на страже ИБ ??

Определение сценариев реализации рисков ИБ

Контекст Компании

Специфика бизнеса
Недопустимые события
Изменения ИТ-ландшафта
Трендовые угрозы ИБ
Регуляторный контекст
Перечень ключевых активов
Бизнес-метрики
Текущий уровень зрелости ИБ



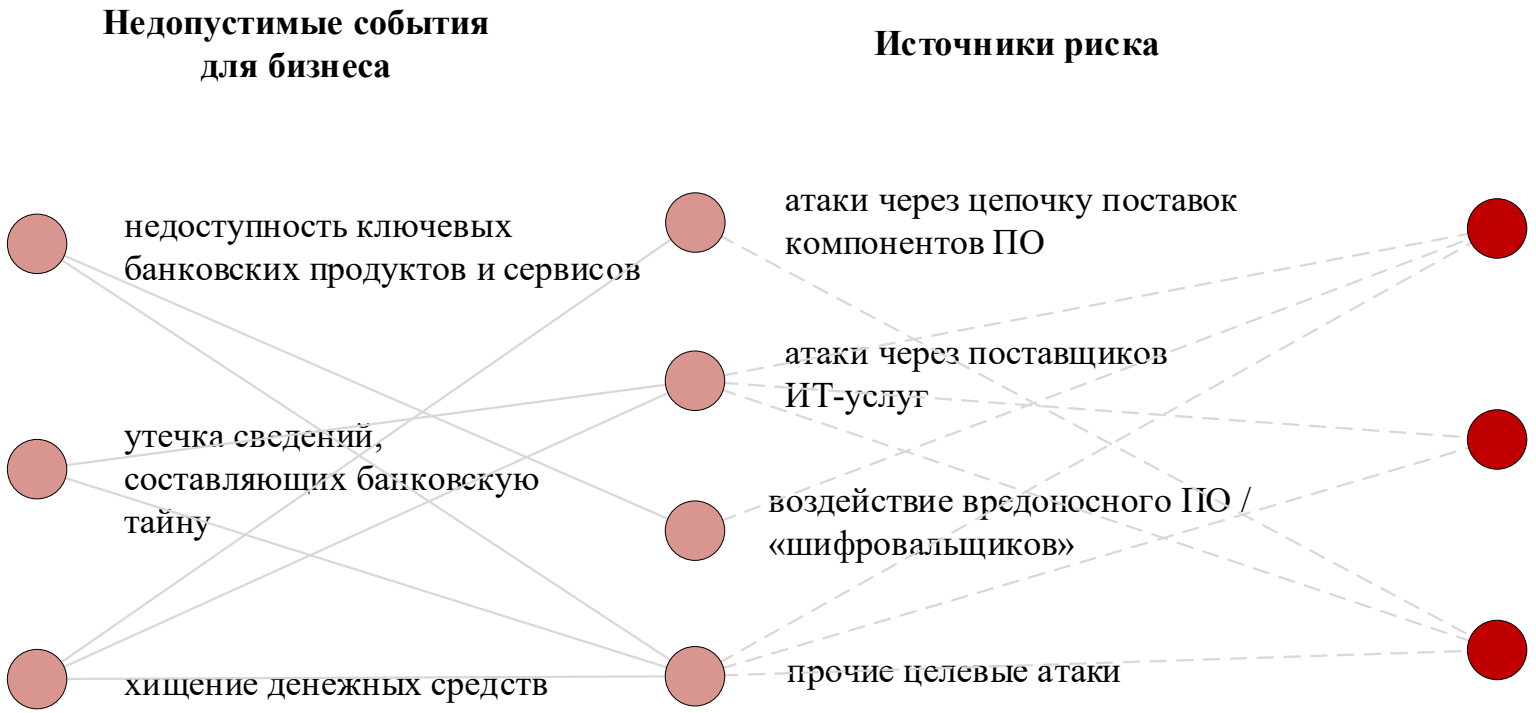
Сценарии реализации

Определение
наиболее критичных релевантных
сценариев реализации рисков ИБ

- Нарушение конфиденциальности
- Нарушение целостности
- Нарушение доступности

- Что произошло?
- Кто инициатор?
- Каков охват?
- Какие последствия?

Идентификация сценариев реализации риска (пример)



Обобщенные сценарии реализации риска ИБ

длительная остановка ключевых банковских услуг в результате целенаправленного разрушения ИТ-инфраструктуры (в результате использования вредоносного ПО или проведения целевой атаки)

утечка данных клиентов в результате целевой атаки

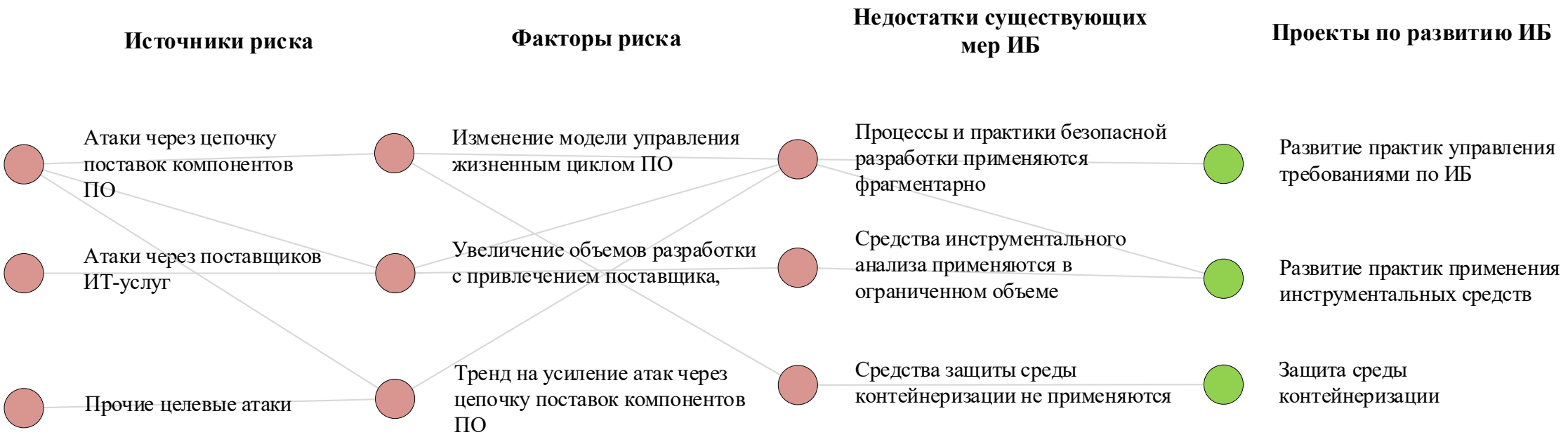
несанкционированные переводы денежных средств со счетов клиентов в результате использования уязвимостей прикладного ПО, а также через компрометацию сторонних компонентов ПО

Оценка последствий

Количественная оценка рисков ИБ (пример)

ID	Недопустимое событие	Сценарий реализации риска ИБ	Последствия для бизнеса (влияние на бизнес-метрики)	Наиболее вероятный сценарий	Вероятность реализации	Уровень риска as-is
РИБ_1	Утечка значительного объема чувствительной внутренней информации	Группа внешних злоумышленников в ходе атаки получила доступ к внутренней ИТ-инфраструктуре. В результате инцидента было скомпрометировано значительное количество чувствительной информации (например, информация о клиентах, условия сделок, ПДн).	Прямые потери: - штрафы за нарушение законодательства в области защиты ПДн (от 60 до 100 т. руб.) - компенсация клиентам за нарушение законодательства в области защиты ПДн (от 60 до 100 т. руб.) - компенсация за нарушение NDA Косвенные потери: - отток количества клиентов от 10% до 30% - снижение притока клиентов от 30% до 60% - маркетинговые затраты на обратное привлечение клиентов (от 1 млн руб. до 5 млн руб.) - затраты на расследование инцидента ИБ (от 500 т. руб. до 1 млн. руб.)	122 610 000,00 ₽	13,69%	16 780 110,34 ₽
РИБ_2	Утечка значительного объема чувствительной внутренней информации	Работник, обладающий привилегированными правами, получил несанкционированный доступ к чувствительной информации и скопировал ее с целью продажи. В результате инцидента было скомпрометировано значительное количество-чувствительной информации (например, информация о клиентах, условия сделок, ПДн).	Прямые потери: - штрафы за нарушение законодательства в области защиты ПДн (от 60 до 100 т. руб.) - компенсация клиентам за нарушение законодательства в области защиты ПДн (от 60 до 100 т. руб.) - компенсация за нарушение NDA - санкции за разглашение кредитной истории Косвенные потери: - отток количества клиентов от 10% до 30% - снижение притока клиентов от 30% до 60% - маркетинговые затраты на обратное привлечение клиентов (от 1 млн руб. до 5 млн руб.) - затраты на расследование инцидента ИБ (от 500 т. руб. до 1 млн. руб.)	131 990 000,00 ₽	36,08%	47 621 992,00 ₽
РИБ_3	Утечка значительного объема чувствительной внутренней информации	Штатный офисный работник, имея доступ к чувствительной информации, увольняясь, скопировал ее с целью выложить на публичные ресурсы, чтобы нанести вред Компании, или использовать при работе у конкурентов. В результате инцидента было скомпрометировано значительное количество чувствительной информации (например, информация о клиентах, условия сделок, ПДн).	Прямые потери: - штрафы за нарушение законодательства в области защиты ПДн (от 60 до 100 т. руб.) - компенсация клиентам за нарушение законодательства в области защиты ПДн (от 60 до 100 т. руб.) - компенсация за нарушение NDA - санкции за разглашение кредитной истории Косвенные потери: - отток количества клиентов от 20% до 40% - снижение притока клиентов от 40% до 70% - маркетинговые затраты на обратное привлечение клиентов (от 1 млн руб. до 5 млн руб.) - затраты на расследование инцидента ИБ (от 500 т. руб. до 1 млн. руб.)	175 490 000,00 ₽	20,61%	36 164 979,20 ₽
РИБ_4	Утечка значительного объема чувствительной внутренней информации	Штатный офисный работник получил несанкционированный доступ к чувствительной информации, скопировал ее с целью продажи. В результате инцидента было скомпрометировано значительное количество чувствительной информации (например, информация о клиентах, условия сделок, ПДн).	Прямые потери: - штрафы за нарушение законодательства в области защиты ПДн (от 60 до 100 т. руб.) - компенсация клиентам за нарушение законодательства в области защиты ПДн (от 60 до 100 т. руб.) - компенсация за нарушение NDA Косвенные потери: - отток количества клиентов от 10% до 30% - снижение притока клиентов от 30% до 60% - маркетинговые затраты на обратное привлечение клиентов (от 1 млн руб. до 5 млн руб.) - затраты на расследование инцидента ИБ (от 500 т. руб. до 1 млн. руб.)	122 610 000,00 ₽	20,98%	25 718 673,60 ₽

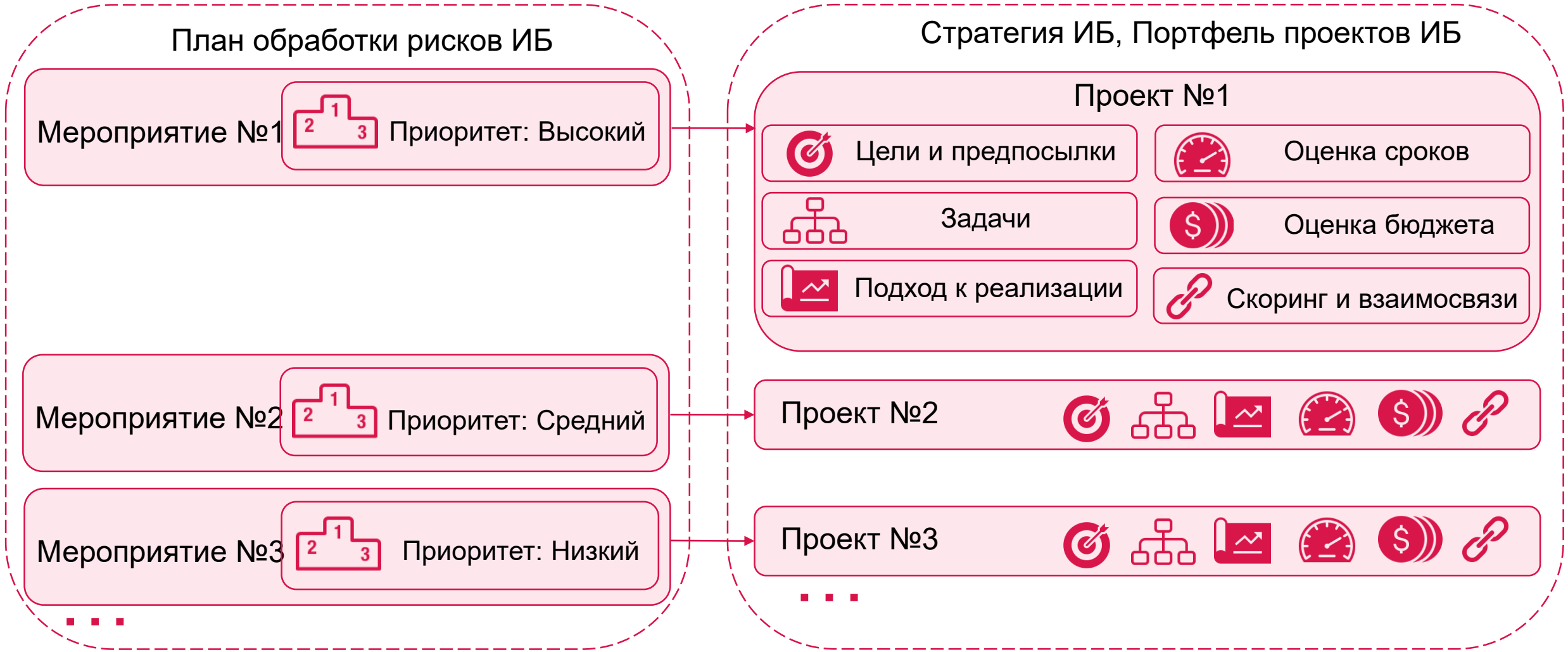
Определение направлений развития ИБ (пример логической модели)



Приоритезация мероприятий ИБ (пример)

№	Процесс (область)	Мероприятия по обработке рисков	Связанные риски *Позволит ли мероприятие снизить риск?*									Количество	Уровень влияния контроля на риск *низкий - 1 средний - 5 высокий - 10*	Стоимость реализации *низкая- 3 (до 2 млн. р.) средняя - 2 (2-5 млн. р.) высокая - 1 (свыше 5 млн. р.)*	Скорость реализации *быстрая - 3 (до 2х месяцев) средняя - 2 (до полугода) медленная - 1 (свыше 6 месяцев)*	Приоритет мероприятия
			1	2	3	4	5	6	7	8	9					
1	Организация и управление ИБ, комплаенс	Определить целевую организационную структуру ИБ в Компании. Спроектировать и формализовать процессы ИБ, распределить роли и обязанности, определить требования к инструментам автоматизации. Выстроить процессы мониторинга, анализа и оценки процессов ИБ.	Да	Да	Да	Да	Да	Да	Да	Да	Да	9	высокий (10)	средняя (2)	средняя (2)	1
2	Управление активами	1. Определить информационные потоки. 2. Выполнять контроль информационных потоков с целью обнаружения утечки конфиденциальной информации, например, с использованием системы класса DLP.	Да	Да	Да	Да	Да	Да	-	-	-	6	высокий (10)	высокая (1)	быстрая (3)	3
3	Управление активами	Внедрить систему класса MDM для централизованного управления и контроля над мобильными устройствами (ноутбуками, телефонами, планшетами).	Да	-	-	-	Да	Да	Да	Да	-	5	средний (5)	высокая (1)	медленная (1)	5
4	Управление активами	Составить и регулярно пересматривать перечни классифицированной информации. Определить требования по ИБ при обработке каждого класса информации.	Да	Да	Да	Да	Да	Да	Да	Да	-	8	низкий (1)	низкая (3)	быстрая (3)	5
5	Управление активами	Внедрить инструмент активного обнаружения подключения устройств, например, систему класса NAC.	Да	-	-	-	Да	Да	Да	Да	-	5	высокий (10)	высокая (1)	медленная (1)	5
6	Управление активами	Формализовать требования по возврату активов работниками. Включить в трудовые договора с работниками обязательство по возврату активов.	-	-	Да	-	-	-	-	-	-	1	высокий (10)	низкая (3)	быстрая (3)	5
7	Управление активами	Сформировать перечень запрещенного разрешенного или категорий запрещенного ПО. Выполнять пересмотр перечня запрещенного разрешенного ПО не реже одного раза в месяц.	Да	Да	-	Да	Да	Да	Да	Да	-	7	низкий (1)	низкая (3)	быстрая (3)	5
8	Управления доступом	Обеспечить персонализированные (не общие) учетные записи для всех систем, которые технически позволяют это сделать. Отключить предустановленные УЗ, если они не являются необходимыми в ИТ-процессах. Выполнять автоматическую блокировку учетных записей, бездействие которых составило 45 и более дней путем установки соответствующих настроек/написания скриптов.	Да	Да	-	Да	Да	Да	Да	Да	-	7	средний (5)	низкая (3)	быстрая (3)	3
9	Управления доступом	Предоставить клиентам детальные инструкции по управлению доступом в онлайн-офисе (предоставление, отзыв и пересмотр прав доступа). Предоставить клиентам детальные инструкции по работе с двухфакторной аутентификацией для доступа в онлайн-офис. Уточнять у клиента актуальность прав доступа в онлайн-офисе на регулярной основе, не реже 1 раза в год. Установить требования к сложности паролей клиентов для доступа в онлайн-офис в соответствии с требованиями Политики «Пароли». Установить минимальную длину пароля клиентов для доступа в онлайн-офис не менее 14 символов.	-	-	-	-	-	Да	-	-	Да	2	средний (5)	низкая (3)	быстрая (3)	5
10	Управления доступом	Обеспечить контроль привилегированного доступа (администраторов ИТ-активов, работников поставщиков ИТ-услуг) к ресурсам с возможностью мониторинга действий привилегированных пользователей, например, путем внедрения системы класса PAM	Да	Да	-	Да	Да	Да	Да	Да	-	7	высокий (10)	средняя (2)	быстрая (3)	1
11	Управления доступом	Использовать MFA при удаленном подключении через резервный канал.	Да	Да	-	Да	Да	Да	Да	Да	-	7	средний (5)	средняя (2)	средняя (2)	4
12	Управление конфигурациями	Формализовать требования по безопасной настройке различных компонентов ИТ-инфраструктуры: 3 потока: 1) контроллеры домена Active Directory, операционные системы серверов; 2) операционные системы АРМ, сетевое оборудование, веб-серверы; 3) системы управления базами данных, средства контейнеризации. В качестве ориентира рекомендуется использовать гайды, рекомендации по безопасной настройке оборудования/ПО (по харденингу), например CIS Benchmarks List – https://www.cisecurity.org/cis-benchmarks.	Да	Да	-	Да	Да	Да	Да	Да	-	7	высокий (10)	средняя (2)	средняя (2)	2

Портфель проектов ИБ



Пример проекта ИБ (может включать несколько мероприятий)

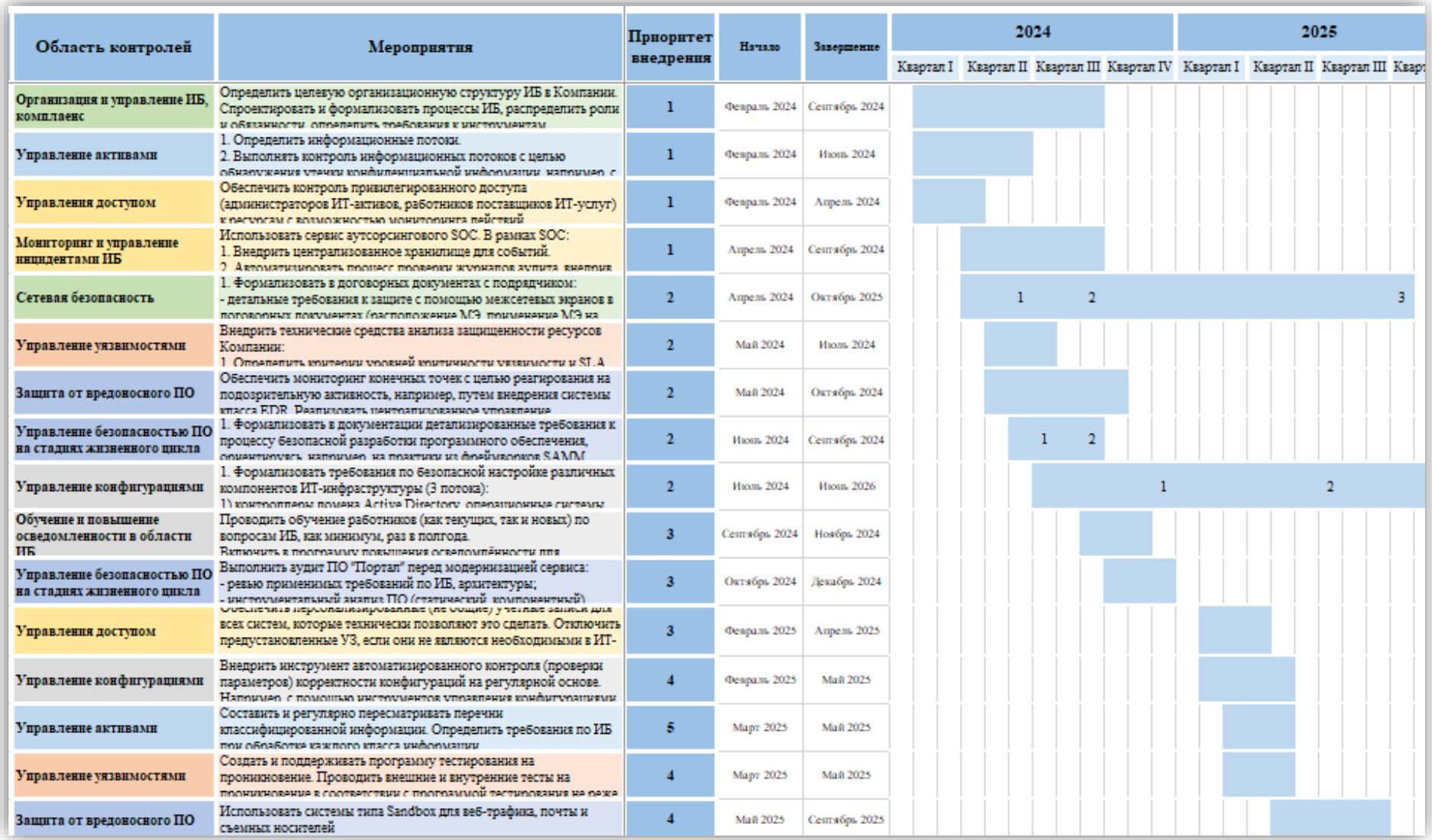
Мероприятие:

Обеспечить мониторинг конечных точек с целью реагирования на подозрительную активность, например, путем внедрения системы класса EDR. Реализовать централизованное управление антивирусным ПО для всех устройств.

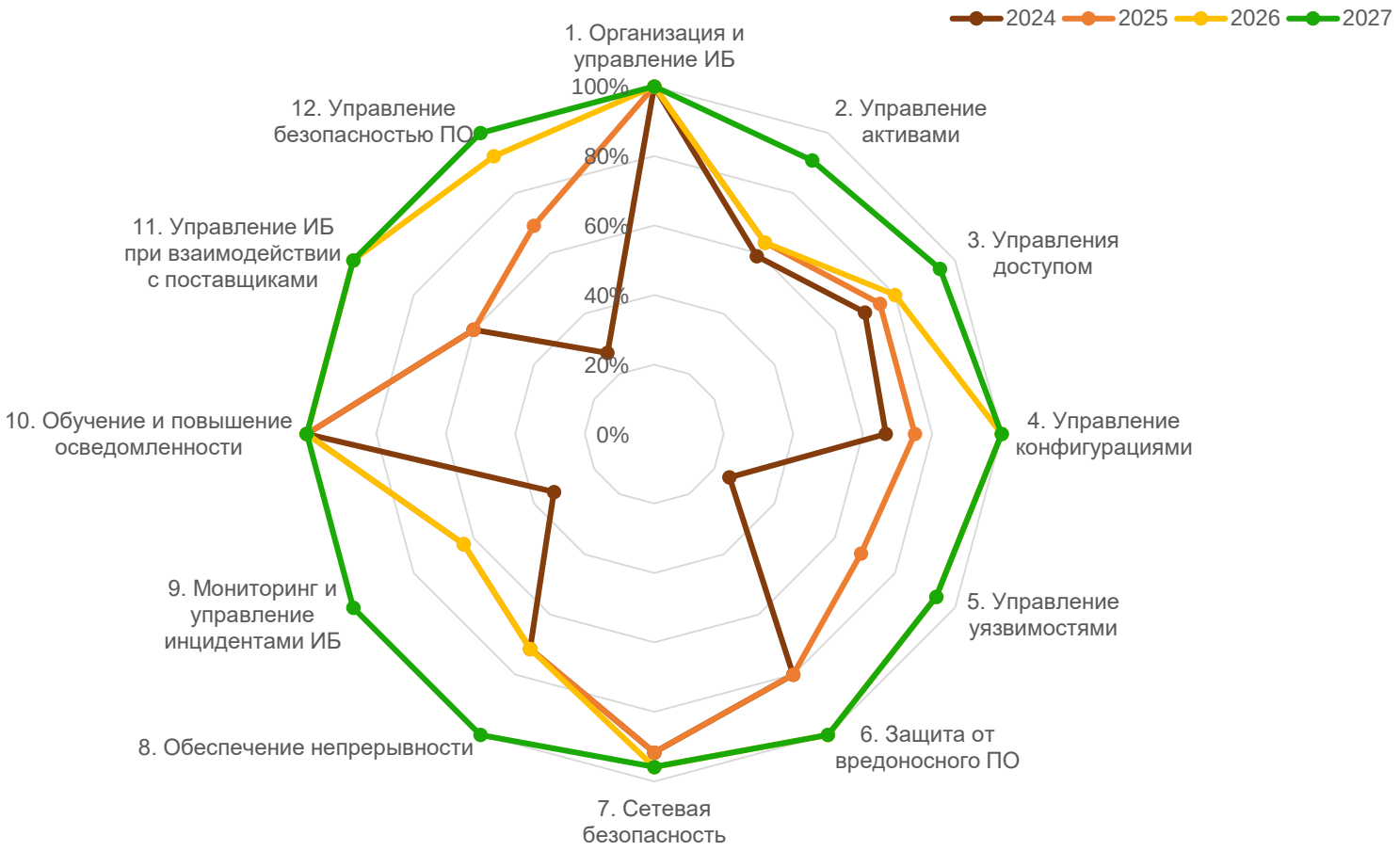
Цели и предпосылки	Цель – обеспечение мониторинга и реагирования на подозрительную активность на конечных точках. Предпосылки для реализации инициативы: • распределенная сеть офисов, существенное количество персонала; • используемые решения не унифицированы, централизованное управление отсутствует; • механизмы поведенческого анализа пользователей для обнаружения угроз не применяются; • согласно мировой статистике более половины успешных атак выполняются с использованием вредоносного ПО.
Задачи	• обеспечить сбор данных с конечных точек в режиме реального времени; • сохранять информацию о действиях пользователей, сетевой активности и запущенных программах для последующего анализа; • выявлять и классифицировать подозрительную активность, а также уведомлять блок ИБ о ней; • блокировать атаки — изолировать подозрительные файлы, останавливать вредоносные процессы, разрывать сетевые соединения; • интегрировать с защитными решениями для конечных точек, SIEM-системами и другими средствами защиты.
Подход к реализации	Установка агентов решения на конечные точки и серверы. Настройка централизованной консоли для управления агентами. Мониторинг запущенных процессов, действий пользователя и сетевых коммуникаций с использованием агента и передача информации на локальный сервер или в облако. Анализ системой полученных данных при помощи технологий машинного обучения, сопоставление их с базами индикаторов компрометации (IoC) и другой доступной информацией о сложных угрозах. В случае обнаружения события с признаками киберинцидента оповещение об этом работников ИБ. Настройка способов автоматического реагирования на различные события с признаками киберинцидента.
Оценка сроков и бюджета	Стоимость: Срок:
Скоринг и взаимосвязи	Влияние на величину связанных рисков: *высокий* Сумма связанных рисков: *~150 млн* Стоимость реализации: *средняя* Скорость реализации: *средняя*

Целевое состояние (пример дорожной карты)

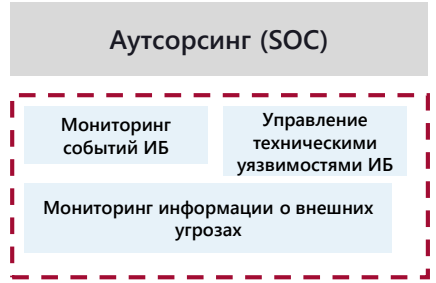
Область контролей	Мероприятия	Приоритет внедрения	Начало	Завершение
Организация и управление ИБ, комплаенс	Определить целевую организационную структуру ИБ в Компании. Спроектировать и формализовать процессы ИБ, распределить роли и обязанности, определить требования к инструментам	1	Февраль 2024	Сентябрь 2024
Управление активами	1. Определить информационные потоки. 2. Выполнять контроль информационных потоков с целью обнаружения утечки конфиденциальной информации, например, с	1	Февраль 2024	Июнь 2024
Управления доступом	Обеспечить контроль привилегированного доступа (администраторов ИТ-активов, работников поставщиков ИТ-услуг) к ресурсам с возможностью мониторинга действий	1	Февраль 2024	Апрель 2024
Мониторинг и управление инцидентами ИБ	Использовать сервис аутсорсингового SOC. В рамках SOC: 1. Внедрить централизованное хранилище для событий. 2. Автоматизировать процесс проверки журналов аудита, внедрив	1	Апрель 2024	Сентябрь 2024
Сетевая безопасность	1. Формализовать в договорных документах с подрядчиком: - детальные требования к защите с помощью межсетевых экранов в договорных документах (расположение МЭ, применение МЭ на	2	Апрель 2024	Октябрь 2025
Управление уязвимостями	Внедрить технические средства анализа защищенности ресурсов Компании: 1. Определить критерии уровней критичности уязвимости и SLA	2	Май 2024	Июль 2024
Защита от вредоносного ПО	Обеспечить мониторинг конечных точек с целью реагирования на подозрительную активность, например, путем внедрения системы класса EDR. Реализовать централизованное управление	2	Май 2024	Октябрь 2024
Управление безопасностью ПО на стадиях жизненного цикла	1. Формализовать в документации детализированные требования к процессу безопасной разработки программного обеспечения, ориентируясь, например, на практики их фреймворков SAMM	2	Июнь 2024	Сентябрь 2024
Управление конфигурациями	1. Формализовать требования по безопасной настройке различных компонентов ИТ-инфраструктуры (3 потока): 1) контроллеры домена Active Directory, операционные системы	2	Июль 2024	Июнь 2026
Обучение и повышение осведомленности в области ИБ	Проводить обучение работников (как текущих, так и новых) по вопросам ИБ, как минимум, раз в полгода. Включить в программу повышения осведомлённости для	3	Сентябрь 2024	Ноябрь 2024
Управление безопасностью ПО на стадиях жизненного цикла	Выполнить аудит ПО "Портал" перед модернизацией сервиса: - ревью применимых требований по ИБ, архитектуры; - инструментальный анализ ПО (статический, компонентный)	3	Октябрь 2024	Декабрь 2024
Управления доступом	Обеспечить персонализированные (не общие) учетные записи для всех систем, которые технически позволяют это сделать. Отключить предустановленные УЗ, если они не являются необходимыми в ИТ-	3	Февраль 2025	Апрель 2025
Управление конфигурациями	Внедрить инструмент автоматизированного контроля (проверки параметров) корректности конфигураций на регулярной основе. Например, с помощью инструментов управления конфигурациями	4	Февраль 2025	Май 2025
Управление активами	Составить и регулярно пересматривать перечни классифицированной информации. Определить требования по ИБ при обработке каждого класса информации	5	Март 2025	Май 2025
Управление уязвимостями	Создать и поддерживать программу тестирования на проникновение. Проводить внешние и внутренние тесты на проникновение в соответствии с программой тестирования не реже	4	Март 2025	Май 2025
Защита от вредоносного ПО	Использовать системы типа Sandbox для веб-трафика, почты и съемных носителей	4	Май 2025	Сентябрь 2025



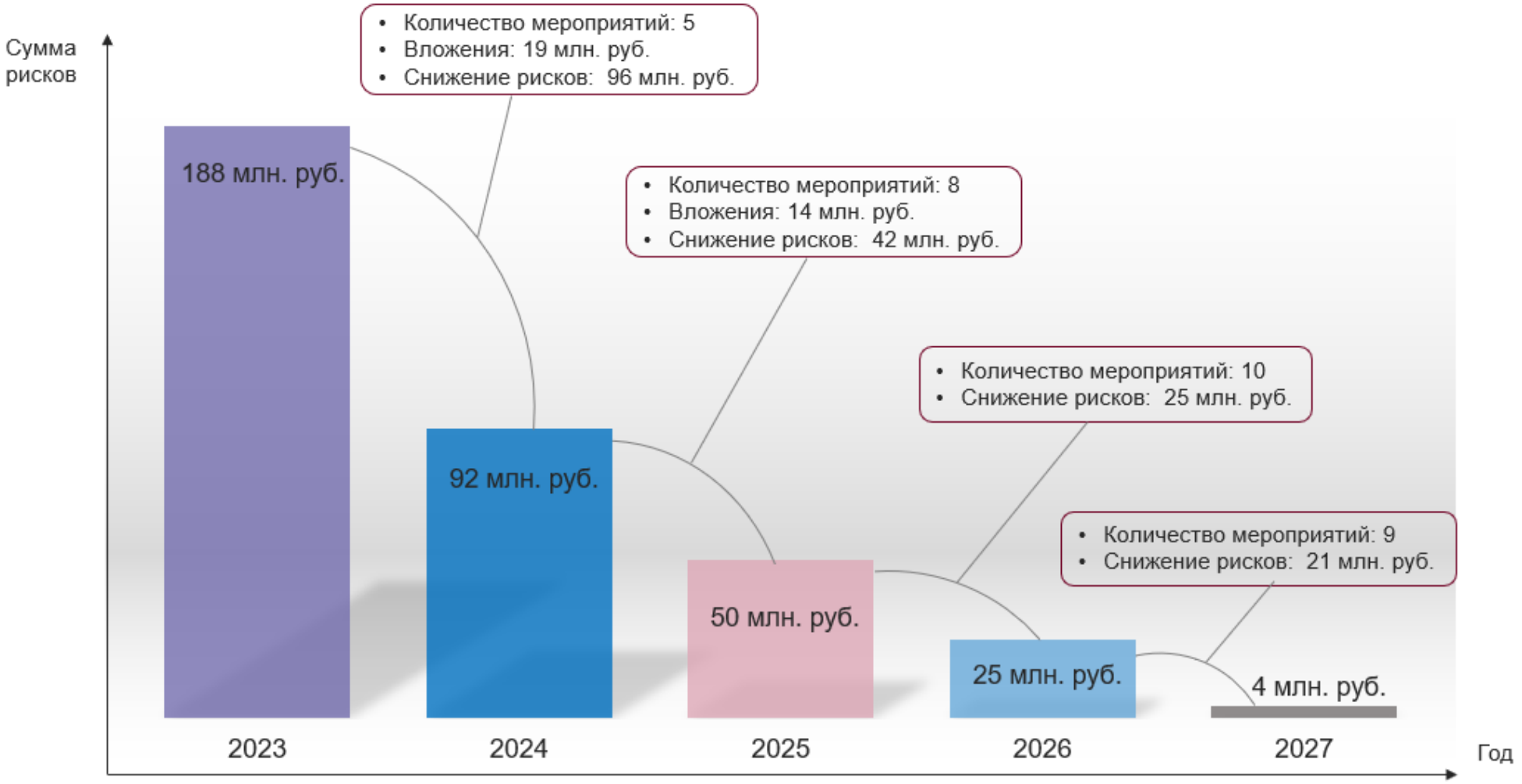
Изменение уровня зрелости ИБ по ходу реализации стратегии



Что насчет организационной структуры ИБ?



Как реализация стратегии влияет на величину рисков? (пример)



На этом все?

Жизнь стратегии только начинается после разработки!

- Регулярные ревью целей и задач (1-2 раза в год)
- Мониторинг рисков и контекста (на постоянной основе)
- Внесение изменений и анализ их влияния на портфель проектов (по мере необходимости)
- Мониторинг исполнения дорожной карты (на контрольных точках)

softline®

Цифровая Трансформация.
Успешная. Эффективная.