softline® 30 лет в ИТ
Мы всё сможем

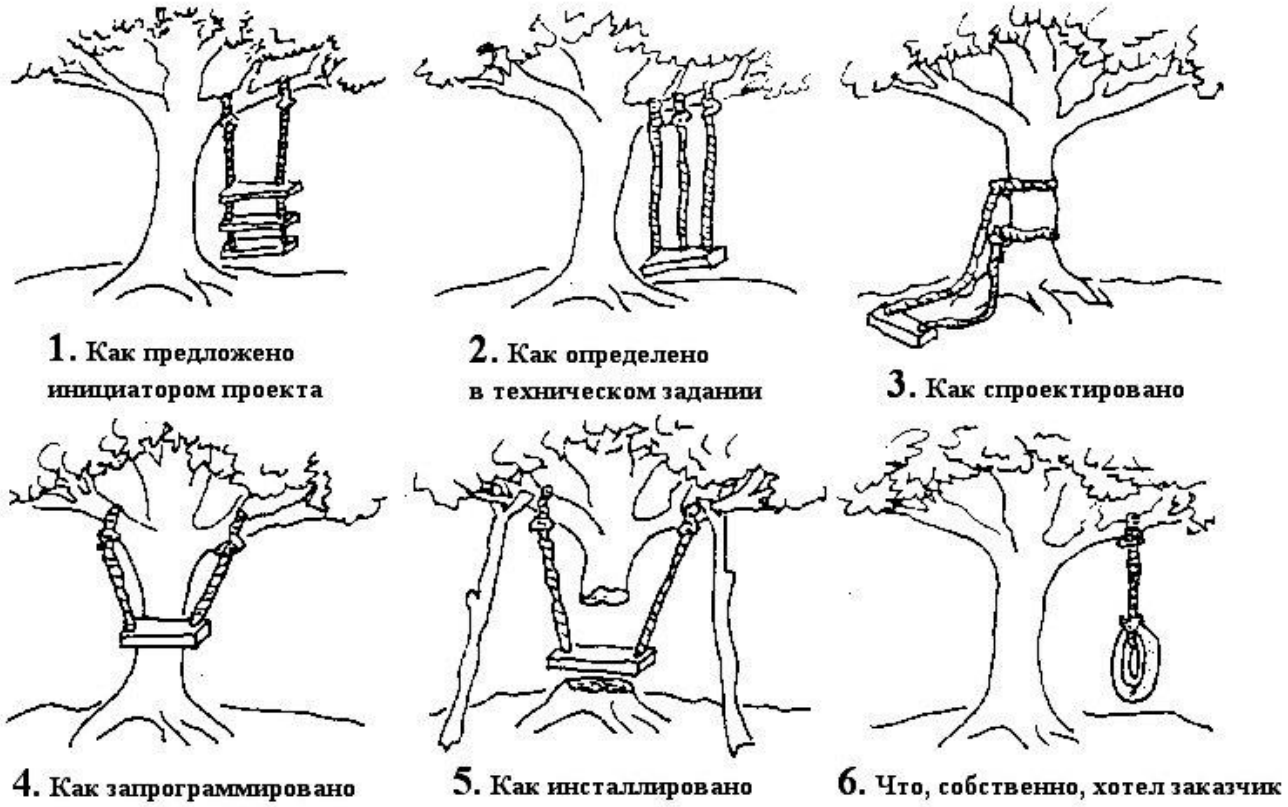
Трёхлетняя стратегия развития ИБ в банке

Смолина Юлия
Руководитель центра компетенций по консалтингу ИБ
Softline

Что хотел заказчик

На самом деле, все просто.

Предыдущая стратегия закончилась...
и надо бы сделать новую на 3 года



Анализ бизнес-стратегии

- **Сохранение устойчивой бизнес-модели Банка** - главный стратегический приоритет

Стратегические приоритеты:

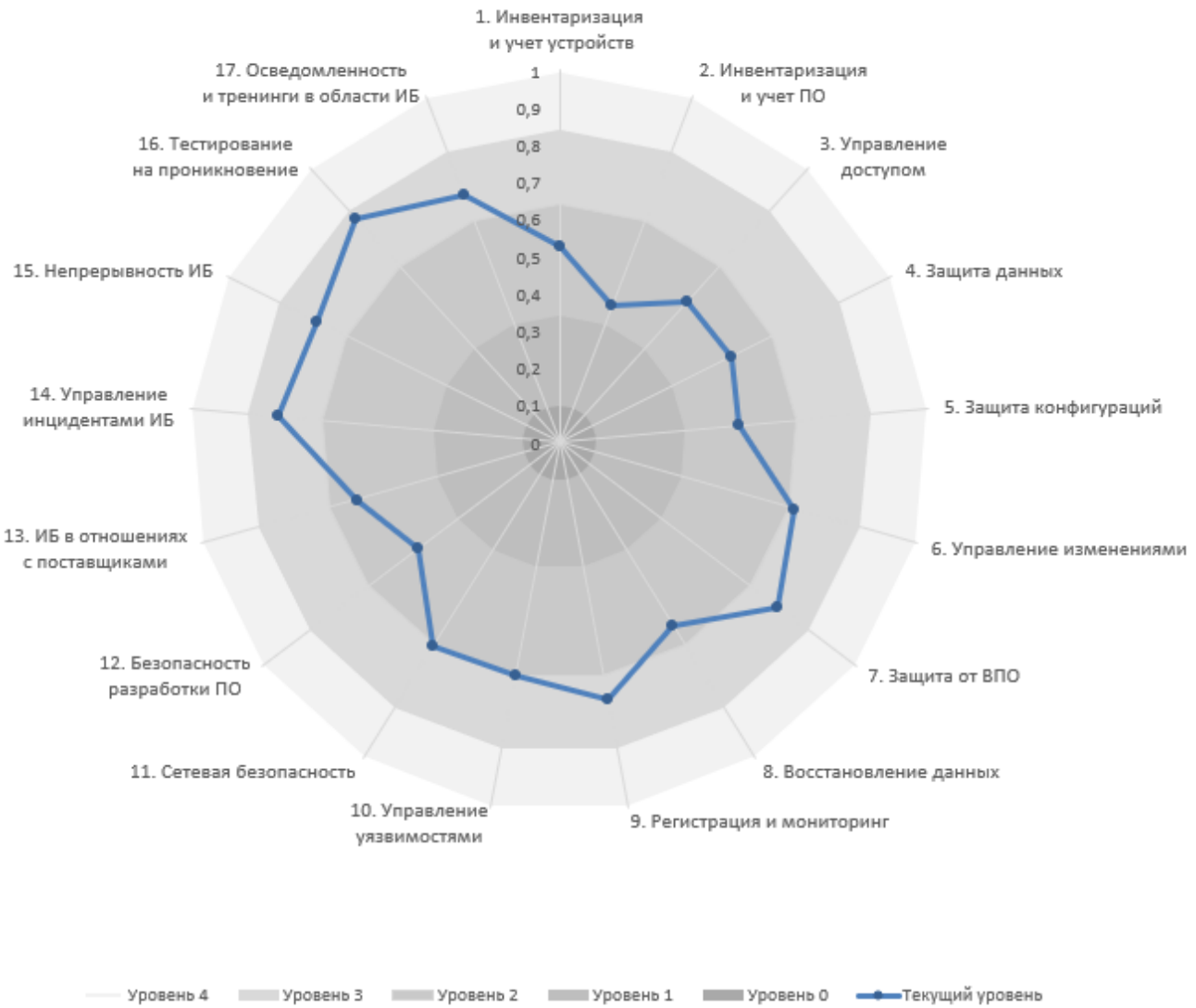
- Трансформация каналов взаимодействия с клиентами
- Трансформация ИТ
- Трансформация международного бизнеса

Основные недопустимые события*:

- Недоступность / деградация ключевых клиентских сервисов
- Утечка данных клиентов
- Несанкционированные переводы денежных средств
- Зависимость от ключевых поставщиков/разработчиков

*потенциальные события и/или сценарии реализации риска, оказывающие значительное негативное влияние на деятельность Банка (на основе интервью со структурными подразделениями)

Оценка текущего уровня зрелости ИБ



Основные области, требующие внимания:

- Практики безопасной разработки ПО
- Контроль и защита средств контейнеризации
- Обнаружение и контроль подключения к сети Банка несанкционированных устройств
- Контроль сетевого трафика
- Контроль безопасных конфигураций оборудования и ПО
- Процессы и практики SOC
- Повышение осведомленности

Содержание документа

Развитие практик безопасной разработки ПО

Развитие практик управления требованиями по ИБ

- Детализация требований к разрабатываемому ПО
- Детализация процесса моделирования угроз
- Анализ бизнес-требований и архитектуры
- Требования к внешним разработчикам

Развитие практик применения инструментальных средств

- Встраивание инструментов в конвейер CI/CD
- Контроль использования сторонних компонентов
- Управление секретами
- Оркестрация инструментов

Защита среды контейнеризации

Внедрение средств контроля безопасности среды контейнеризации, включая инфраструктуру частного облака

Усиление защиты конвейера CI/CD

Харденинг конвейера CI/CD (разграничение прав доступа, критерии успешности тестирования и т.д.)

Программа Bug Bounty

Запуск программы поиска уязвимостей на российской платформе

Усиление безопасности ИТ-инфраструктуры

Управление безопасностью (харденинг) конфигураций

- Разработка стандартов безопасных конфигураций
- Регулярный автоматизированный контроль корректности конфигураций

Микросегментация серверных сегментов сети

- Микросегментация сети и изоляция сегментов с учетом принципов «нулевого доверия»

Контроль доступа к сети

- Внедрение средств контроля доступа к сети (NAC)

Развитие технических решений для выявления сетевых аномалий

- Пилот выбор и внедрение системы поведенческого анализа сетевого трафика (NTA / NDR)
- Развитие практик управления IPS/IDS

Комплексное усиление безопасности ПУД

Детализированная оценка рисков, связанных с утечками клиентских данных. Выбор и планирование мероприятий для снижения рисков.

Развитие функции SOC

Обеспечение необходимого уровня покрытия

- Анализ и приоритезация источников
- Расширение уровня покрытия SOC внутренней сети и облака
- Глубокое профилирование правил корреляции

Развитие практики проведения киберучений

Проведение киберучений с участием ДИБ, ИТ, прочих подразделений на основе детализированных сценариев кризисных ситуаций.

Развитие процессов и практик SOC

- Формализация внутренних процессов SOC
- Внедрение практик проактивного поиска угроз (threat hunting)
- Программа по развитию и удержанию персонала SOC

Развитие инструментов и процессов обнаружения ИТ-активов

Комплекс требований и мероприятий по автоматизации обнаружения новых ИТ-активов в сети Банка

Внешний аудит SOC

Оценка зрелости SOC, анализ покрытия, качества правил и т.д.

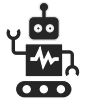
Развитие практик управления рисками ИБ

Развитие методологической основы

- Детализация подхода к управлению рисками ИБ
- Развитие количественного подхода к оценке рисков ИБ

Развитие инструментов

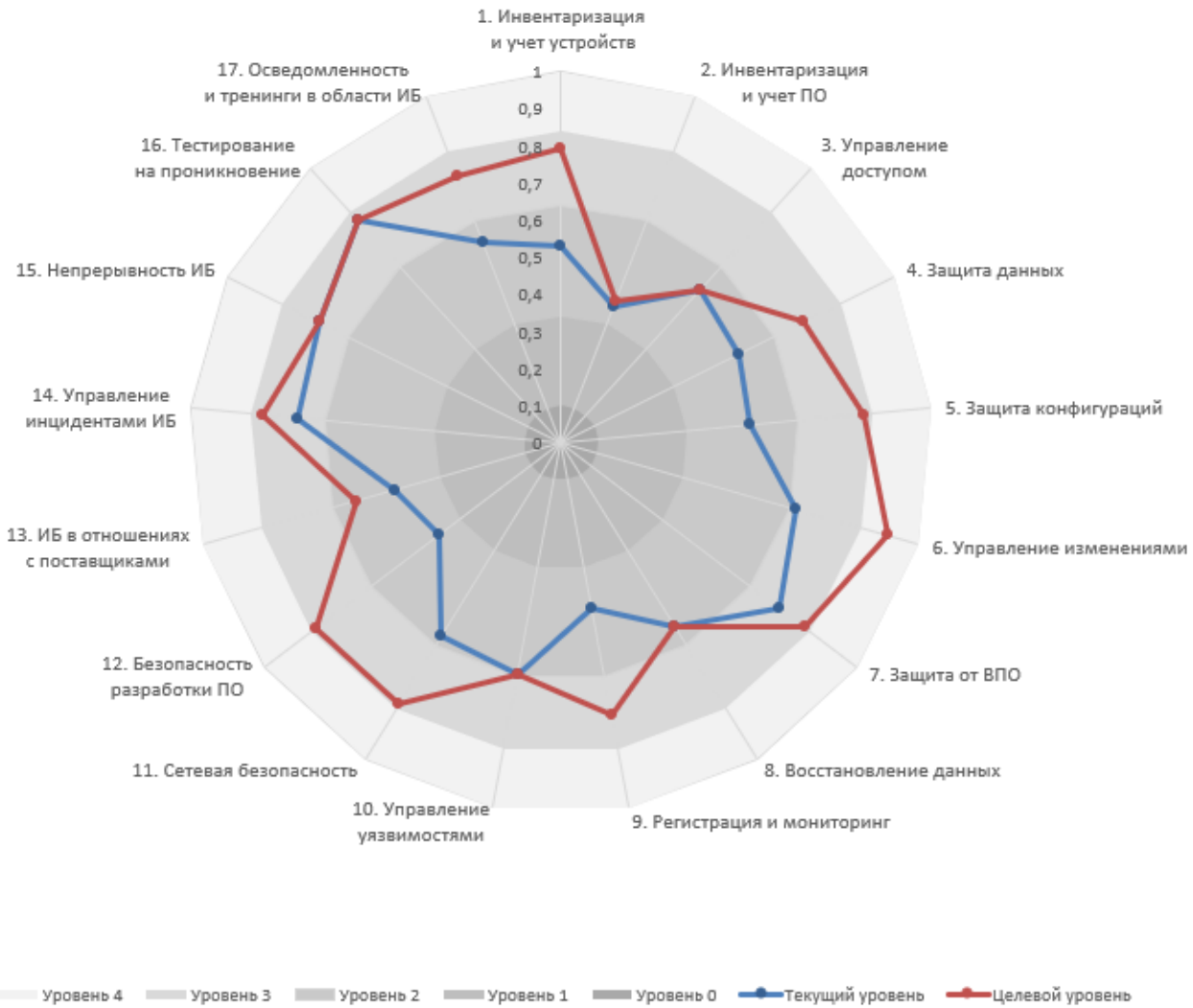
- Программа проведения оценки рисков ИБ «сверху вниз» для каждого направления бизнес-деятельности
- Регулярная самооценка рисков ИБ в разрезе ИС и компонентов ИТ-инфраструктуры
- Разразработка системы ключевых индикаторов риска ИБ
- Интеграция управления рисками ИБ в операционные процессы ИБ и ИТ



Автоматизация управления рисками ИБ

- Доработка и развитие SGRC-платформы
- Интеграция с общекорпоративной автоматизированной системой управления операционными рисками

Оценка целевого уровня зрелости ИБ



Основные улучшения* в результате реализации стратегических инициатив:

- Практики безопасной разработки ПО соответствуют масштабам изменений ИТ-ландшафта
- Надлежащее управление и контроль безопасности средств контейнеризации приложений
- Повышение уровня защищенности инфраструктуры за счет использования встроенных механизмов (харденинг)
- Реализация контроля сетевого трафика и подключений
- Повышение зрелости процессов и практик SOC, включая проактивный поиск угроз
- Системная деятельность в части повышения осведомленности, регулярное проведение киберучений

*оценка достижения целевого уровня зрелости не включает инициативы, реализуемые в рамках операционной деятельности ДИБ, а также проектные и прочие инициативы, реализуемые структурными подразделениями Банка

Q&A