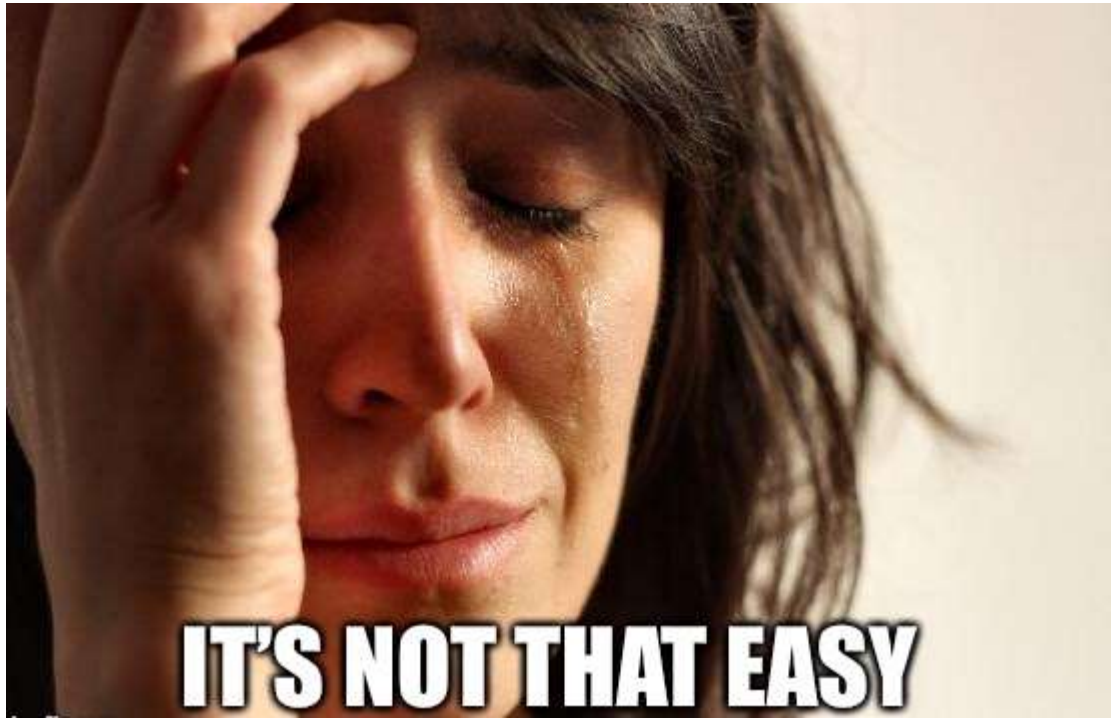
МКБ

Риск-ориентированный подход в условиях современной регуляции

Март, 2024

Риск-ориентированный подход

- Измерить риски
- Сравнить стоимость митигации и величину рисков
- Корректно спланировать митигацию



Плюсы и минусы

- Понятно для бизнеса
- Упрощает бюджетирование
- Упрощает приоритезацию работ
- Требуется большинством стандартов

- Трудоемко
- Не вся статистика доступна
- Нужны эксперты
- Легко сбиться в формальную качественную оценку

Подход МКБ

1. Модель нарушителя
2. Модель угроз
3. Сценарии инцидентов (около 30-40)
4. Поиск статистики по аналогичным инцидентам
5. Опрос экспертов
6. Оценка эффективности мер защиты
7. Первичная оценка рисков
8. Оценка остаточных рисков
9. Обработка остаточных рисков

Как будто сложнее стало. Но примеры последуют

Подход МКБ. Модель нарушителя

Внешние злоумышленники

Хакерские группировки

Хактивисты и киберармия

NEW

Мелкие пакостники

NEW

Внутренние злоумышленники

Ошибающийся пользователь

Финансово-мотивированный пользователь

Политически-мотивированный пользователь

NEW

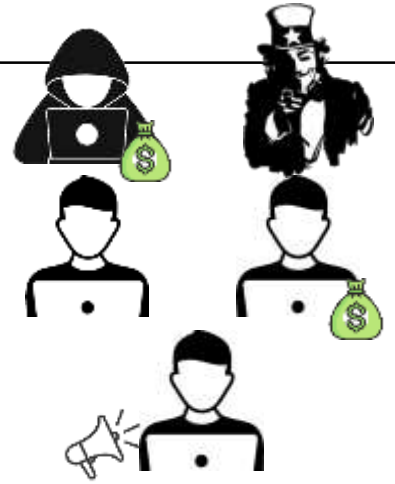
Окологосударственные институты

Санкционные активности

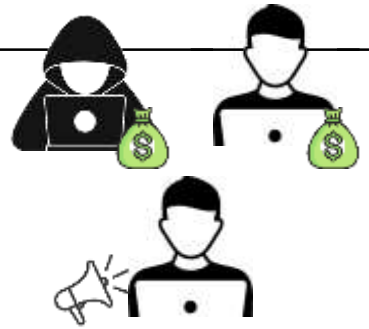
NEW

Подход МКБ. Модель угроз

Утечки данных

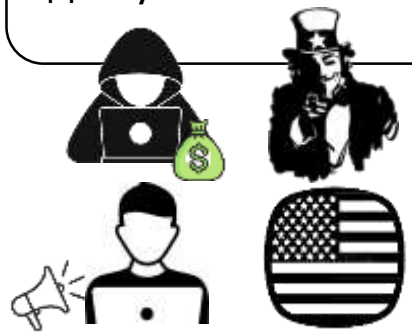


Кража денег у Банка



Кража денег у Клиентов

Нарушение доступности систем



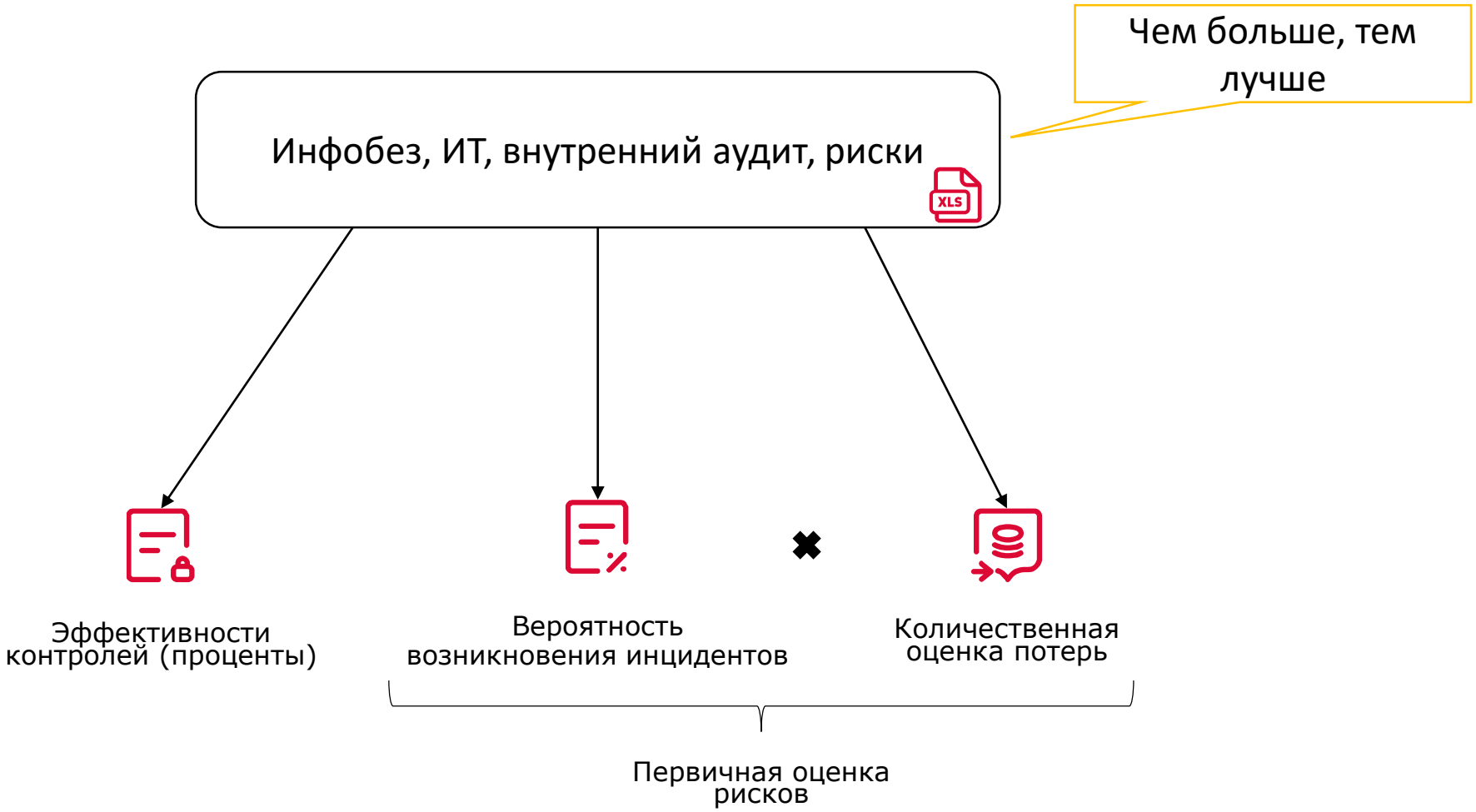
Подход МКБ. Примеры сценариев

- Использование вредоносных библиотек при внутренней разработке ПО
- Смешение контуров теста и боя
- Саботаж
- Распределённые сетевые атаки, направленные на отказ в обслуживании доступных извне контура банка сервисов
- Несоответствие требованиям Банка России
- Несоответствие требованиям ФСТЭК
- Несвоевременная замена сертификата ключа проверки электронной подписи

Подход МКБ. Поиск статистики

- **Фрод в отношении клиентов**
  - https://www.cbr.ru/statistics/ib/
- **Атаки на организации**
  - https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q4/
  - https://www.kaspersky.ru/enterprise-security/resources/white-papers
  - https://rt-solar.ru/analytics/reports/
  - https://www.facct.ru/resources/research-hub/
- **Если в деньгах**
  - Узнать у бизнеса стоимость простоя либо просто поделить прибыль на единицу времени
  - Оценить уровень фрода в отношении самой организации
  - Проанализировать остатки на счетах
  - Воспользоваться пугалочками (https://www.techtarget.com/searchsecurity/tip/The-biggest-ransomware-attacks-in-history)
  - Попробовать оценить с бизнесом отток клиентов

Подход МКБ. Опрос экспертов



Подход МКБ. Пример контролей

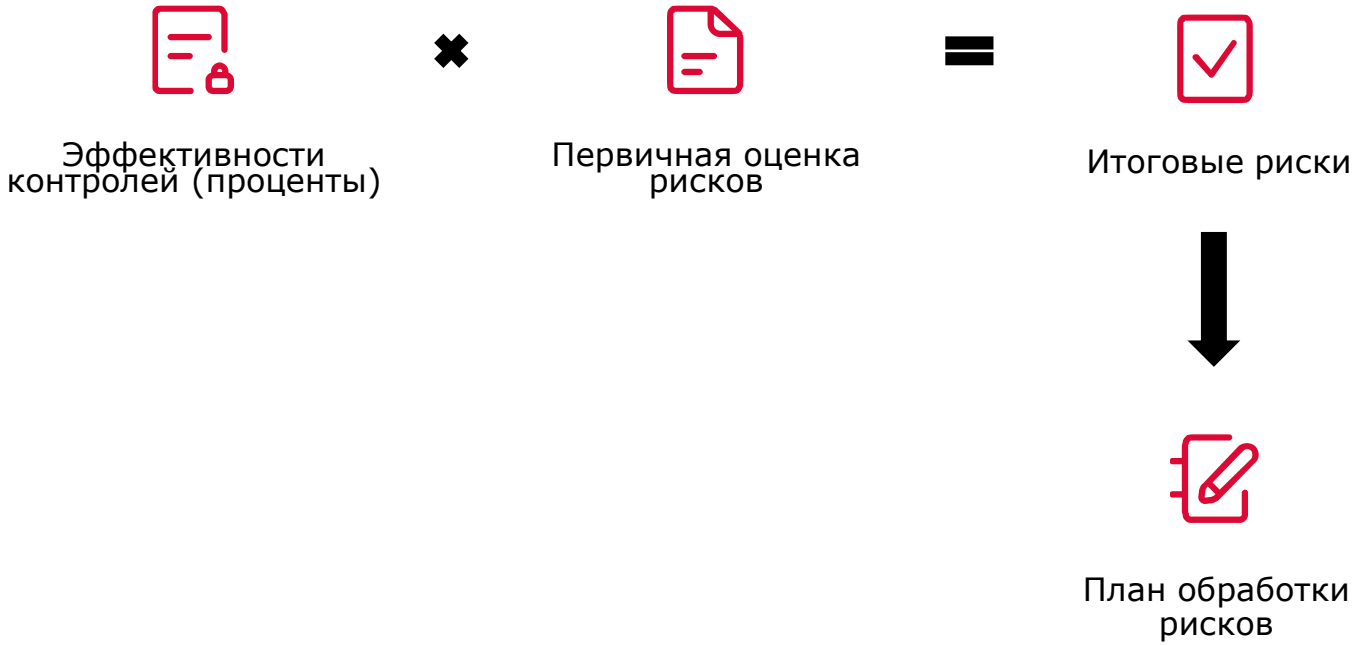
Эффективности контролей (проценты)

Процессы агрегированы в соответствии с CISSP

	Процессы и контроли для митигации							
Вид угрозы	**Поддержка соответствия стандартам и требованиям законодательства**	**Выявление и предотвращение утечек данных**	**Участие в стадиях ЖЦ ИТ систем**	**Криптографическая защита информации**	**Управление изменениями в ИТ**	**Повышение осведомленности**	**Управление инцидентами ИБ**	**Упр уязв**
Смешений контуров теста и боя	0,3				0,5	0,1		

Эффективность контролей, для оценки совокупности – сумма вероятностей

Подход МКБ. Оценка остаточных рисков



Подход МКБ. Добавим регуляторов

Внешние злоумышленники

Хакерские группировки

Хактивисты и киберармия

NEW

Мелкие пакостники

NEW

Внутренние злоумышленники

Ошибающийся пользователь

Финансово-мотивированный пользователь

Политически-мотивированный пользователь

NEW

Окологосударственные институты

Санкционные активности

NEW

Российские регуляторы

Подход МКБ. Добавим сценарии

Несоответствие требований Банка России	Невыполнение или неполное выполнение требований по ИБ со стороны Банка России, способное привести к значительным трудозатратам на устранение и опциональным штрафам
Несоответствие требований ФСТЭК	Невыполнение или неполное выполнение требований по ИБ со стороны ФСТЭК, способное привести к значительным трудозатратам на устранение и опциональным штрафам
Несоответствие требований ФСБ	Невыполнение или неполное выполнение требований по ИБ со стороны ФСБ, способное привести к значительным трудозатратам на устранение и опциональным штрафам
Несоответствие требований РКН	Невыполнение или неполное выполнение требований по ИБ со стороны Роскомнадзора, способное привести к значительным трудозатратам на устранение и опциональным штрафам

Подход МКБ. Количественная оценка

- **Фрод в отношении клиентов**
  - https://www.cbr.ru/statistics/ib/
- **Атаки на организации**
  - https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q4/
  - https://www.kaspersky.ru/enterprise-security/resources/white-papers
  - https://rt-solar.ru/analytics/reports/
  - https://www.facct.ru/resources/research-hub/
- **Если в деньгах**
  - Узнать у бизнеса стоимость простоя либо просто поделить прибыль на единицу времени
  - Оценить уровень фрода в отношении самой организации
  - Проанализировать остатки на счетах
  - Воспользоваться пугалочками (https://www.techtarget.com/searchsecurity/tip/The-biggest-ransomware-attacks-in-history)
  - Попробовать оценить с бизнесом отток клиентов
  - Штрафы от регуляторов
  - Стоимость оперативного устранения несоответствий
  - Оценка стоимости бизнеса в целом (потеря бизнеса)

Подход МКБ. Примеры учета регуляторных требований

Вид угрозы	Сценарий	Вариант обработки	Что становится нестрашно?
Использование работниками и аутсорсерами чужих учетных записей	Использование чужих логинов и паролей для доступа к недоступной под своей учетной записью конфиденциальной информации или совершения каких-либо операций в ИТ-системах	1. Переход на двухфакторную аутентификацию 2. Усиление мониторинга за сессиями пользователей	• 700+ мер от ФСТЭК • Положения Банка России
Использование уязвимого программного обеспечения	Уязвимости регулярно обнаруживаются в широко используемом ПО и не всегда своевременно устраняются. Их эксплуатация может приводить к удаленному доступу, который в свою очередь может быть использован для управления ИТ-инфраструктурой Банка, краже данных или нарушения работоспособности / разрушению ИТ-инфраструктуры, когда злоумышленник находится ВНУТРИ ИТ-инфраструктуры	1. Vulnerability management 2. Набор компенсирующих мер 3. IPS/WAF/переход на альтернативное ПО	• 700+ мер от ФСТЭК • Внезапные проверки Банка России
Разработка небезопасного ПО / ИТ-систем	Уязвимости могут вносится работниками в ПО при разработке ИТ-систем как случайно, так и умышленно. Например, подготовленное обновление интернет-банка содержит уязвимости, позволяющие скопировать информацию о клиентах внешним пользователем или совершать платежи от имени другого клиента	1. AppSec 2. DevSecOps 3. Анализ open-source компонент 4. Bugbounty	• Грядущие меры ФСТЭК • ОУД4

МКБ

Спасибо
за внимание!