Axellect

Почему нам отказывают в бюджете? Системный подход к обоснованию инвестиций в ИБ в эпоху AI

Количественная оценка рисков информационной безопасности

20.11.2026



Copyright © 2023 All rights reserved.

БИЗНЕС ОБЩАЕТСЯ НА ЯЗЫКЕ РИСКОВ И ДЕНЕГ

Качественная оценка рисков и бюджетный комитет

Служба ИБ:
Уровень риска по сценарию высокий. Требуется X млн. ₸ на компенсирующие меры.

Финансовый блок:
Сколько мы потеряем, если меру не реализовать?

Служба ИБ:
Уровень потерь – крайне высокий.

Финансовый блок:

Бюджет не выделен

ИБ

- Уязвимости и векторы атак
- Архитектура и инфраструктура
- Контрольная среда
- Регуляторные требования

Единицы измерения:
- уровни критичности
- уровень зрелости мер ИБ
- количество инцидентов

ОБЩАЯ ОБЛАСТЬ

Риски и деньги

Ожидаемые годовые потери
Стоимость инициативы
Остаточный риск
ROSI

«Высокий риск»
или
«1,31 млрд ₸ в год»

Бизнес

- Продуктовая стратегия
- Бизнес-процессы и операционная модель
- Инвестиционный портфель
- Обязательства перед клиентами

Единицы измерения:
- тенге
- сроки окупаемости
- доля рынка

Axellect ©

Методика соответствует требованиям регулятора, дополняет их и не противоречит им

	Постановление Правления НБ РК № 48 *Обеспечение ИБ*	**Постановление Правления Агентства РК № 111** *Оценка рисков ИБ*	**Постановление Правления НБ РК № 188** *СУР и внутренний контроль*
СООТВЕТСТВУЕТ	Общие положения, требования к организации СУИБ, требования к мерам защиты ИБ	Прямых пересечений нет	Состав участников системы управления рисками ИБ
ДОПОЛНЯЕТ	Требования к категорированию информационных активов	Перечень критичных информационных активов, оценка рисков по ним, перечень типовых источников угроз	Требования к контролю и мониторингу уровня риска
НЕ ПРОТИВОРЕЧИТ	Требования к мерам защиты ИБ	Общие положения, перечень факторов для учёта при оценке вероятности реализации угроз	Общие положения, функции подразделения по управлению рисками ИБ и владельцев информации

Количественная оценка – надстройка над действующими требованиями, использующая те же исходные перечни

С какой формулировкой в последний раз вам отказывали в ИБ бюджете?

Что может дать количественная оценка рисков ИБ?

ДАЁТ

- Прогноз, пригодный для инвестиционного решения
- Сопоставимость рисков между собой и со стоимостью мер
- Приоритет инициатив по ROSI
- Прозрачность допущений: каждый параметр можно оспорить и пересчитать

НЕ ДАЁТ

- Точного значения будущих потерь. Это прогноз, а не измерение
- Нулевого риска. Снизить вероятность и ущерб до нуля невозможно и экономически бессмысленно
- Ответа на вопрос соответствия требованиям. Комплаенс – дополнительный эффект упражнения, а не его цель

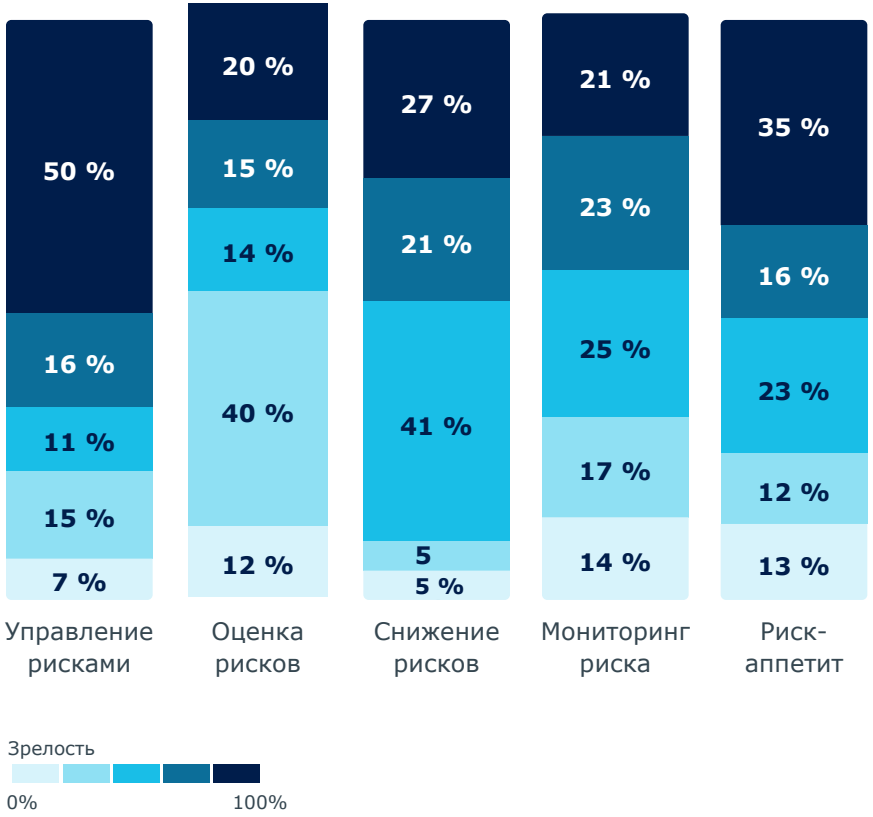
ТРЕБУЕТ

- Контекста компании. Чем он полнее и точнее, тем уже вилка результата
- Вовлечения бизнес-подразделений, а не одного аналитика со стороны
- Выделенной команды и времени. Оценка, выполненная одним риск-аналитиком за неделю, будет неточной

Информационная безопасность не приносит дохода.
Но потери, которых не произошло, – это сохранённые деньги компании.

Наша задача – найти баланс между инвестициями, на которые компания готова, и рисками, которые она готова принять

Риск-менеджмент в целом. Зрелость процессов



Риски информационной безопасности

Измеряют финансовое влияние киберрисков в значительной степени

15 %

PwC Global Digital Trust Insights 2025 ·
4 042 руководителя, 77 стран

Используют преимущественно количественный подход к управлению киберрисками

31 %

FAIR Institute · State of Cyber Risk Management 2025
402 респондента

В риск-менеджменте количественная оценка стала нормой: не применяют её лишь 12 %.
В информационной безопасности финансовое измерение риска ведёт меньшинство

FERMA Global Risk Manager Survey Report 2024. Все категории риска

Axellect ©

СКОЛЬКО НАСТРОЙЩИКОВ ПИАНИНО В МОСКВЕ?

Население Москвы: **~13 млн**. человек

Количество домохозяйств: 12 млн. / **2,5** = 4,8 млн.

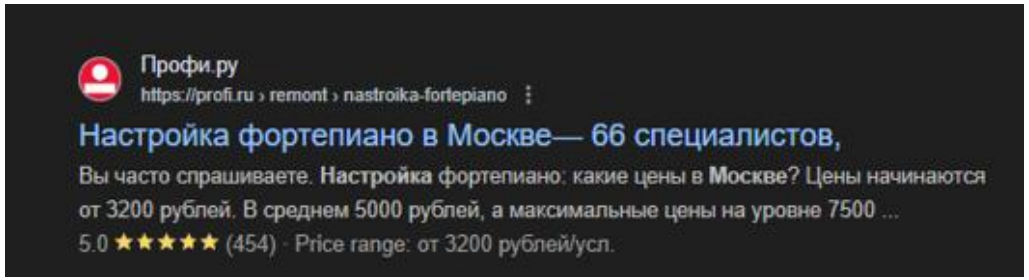
Семей с пианино: 5 млн. * **3%** = 150 тыс.

Частота настройки: 1 раз в **3** года

Рабочих дней настройщика в году: **220**

Пианино, настраиваемых за день: **3**

(((**13 000 000** / 2,5) * **3%**) / **3**) / (**220** * **3**) = **79**



- Лучше иметь **приблизительный ответ**, чем никакого
- **Точность ответа** можно повышать за счёт детальности оценки отдельных параметров
- **Разброс** границ ответа **можно оценить**

Из чего складывается риск ИБ?

РИСК ИБ

КАК ЧАСТО?

ВЕРОЯТНОСТЬ

Частота атак	Уязвимость
Внешние и внутренние данные	**Контрольный фреймворк**
Статистика активности злоумышленников	Зрелость контрольной среды ИБ
Привлекательность компании для атакующего	Набор применяемых ИТ-технологий
Силы и ресурсы злоумышленников	Архитектура ИТ-сервисов

НА КАКУЮ СУММУ?

ПОТЕРИ

Прямые потери	Косвенные потери
Цифровой двойник	
Снижение выручки	Отток клиентов
Потери в фонде оплаты труда	Судебные издержки и штрафы
Материальные потери и восстановление	Снижение репутации

Что такое цифровой двойник?

Набор параметров, описывающих компанию в денежном выражении.
Формируется один раз, применяется во всех сценариях риска

СОСТАВ ПАРАМЕТРОВ

- прибыль за час работы
- почасовая оплата сотрудника и подрядчика
- численность пользователей систем
- количество серверов и стоимость восстановления
- стоимость привлечения клиента
- стоимость маркетинговой кампании
- предельные размеры штрафов
- оборот, прибыль

РАСЧЁТ УЩЕРБА

Каждый сценарий использует свой набор параметров и свои границы длительности.

Недоступность системы:
часы простоя × прибыль на час + простой пользователей + восстановление инфраструктуры + расследование

Утечка персональных данных:
штраф + уведомление + отток × стоимость привлечения + восстановление репутации

ЧТО ЭТО ДАЁТ

- границы ущерба перестают быть экспертным впечатлением
- обсуждение переходит с выводов на исходные параметры
- новый сценарий рассчитывается за часы
- пересчёт при изменении параметра выполняется немедленно

Как с помощью AI ускорить оценку рисков ИБ?

	1	2	3	4	5
Этап	**Профилирование** • BIA (Референсная таблица ущерба) • Анализ бизнес-контекста компании	**Анализ угроз и контрольной среды** • Список агентов угроз и приоритизация • Реестр мер ИБ и оценка уровня зрелости	**Формирование сценариев** • Вероятность реализации, параметры и границы ущерба • Моделирование сценариев риска	**Обработка риска** • Набор контрольных средств под критичные сценарии • Оценка эффективности мер и дорожная карта	**Мониторинг риска** • Ключевые индикаторы риска • Показатели эффективности реализованных мер
Данные для AI	• Реестр ИТ-активов, оценка критичности по КЦД (CIA)	• Список агентов угрозы • Выгрузки из СЗИ по конкретным решениям, CMDB, каталог УЗ, отчёты, документооборот	• Списки агентов угрозы, событий угрозы и контролей ИБ • Параметры моделирования	• Количественные оценки вероятности реализации и ущерба	• Ключевые индикаторы риска, метрики эффективности мер
Применение AI	• Автоматизация сбора данных об активах через интеграцию с ITSM и CMDB	• Deep research для валидации списка агентов и их параметров • Процентная оценка зрелости контролей	• Проверка актуальности событий • Моделирование сценариев риска Дашборды	• Приоритизация контролей, группировка в инициативы Расчёт ROI Дорожная карта	• Сбор отчетности • Дашборды

От параметров к границам ущерба и ожидаемым потерям

ПАРАМЕТРЫ ИЗ ЦИФРОВОГО ДВОЙНИКА

Количество серверов	100 шт
Время восстановления сервера	100 ч
Почасовая оплата подрядчика	10 000 ₸
Пользователей системы	1 000 чел
Почасовая оплата сотрудника	10 000 ₸
Выдача кредитов в месяц	10 млрд ₸
Расследование и ликвидация	10 млн ₸
Дней недоступности системы	3–5

НИЖНЯЯ ГРАНИЦА | недоступность 3 суток

восстановление серверов + простой пользователей + недовыдача кредитов + расследование

1,64 млрд ₸

ВЕРХНЯЯ ГРАНИЦА | недоступность 5 суток

те же составляющие при увеличенной длительности простоя

2,66 млрд ₸

МОДЕЛИРОВАНИЕ

Метод Монте-Карло, логнормальное распределение. На вход: вероятность реализации, нижняя и верхняя границы ущерба

Ожидаемый годовой убыток (ALE)

1,31 млрд ₸

среднее всех смоделированных значений, включая нулевые

Средний ущерб от единичного случая (SLE)

2,07 млрд ₸

среднее только ненулевых значений

Иллюстративный пример

Зрелость мер переводится в деньги, а деньги – в приоритизацию инициатив

	Уровень зрелости мер ИБ	Вероятность реализации	Финансовый ущерб
Меры не внедрены потенциальный риск	**0 %**	**64 %**	**1,31 млрд ₸**
Меры как есть фактический риск	**55 %**	**18 %**	**0,30 млрд ₸**
Меры целевые остаточный риск	**72 %**	**5 %**	**0,05 млрд ₸**

ЭФФЕКТИВНОСТЬ ВЛОЖЕНИЙ ЗА 3 ГОДА

Митигируемый ущерб: 0,30 – 0,05 = **0,25 млрд ₸ в год**

Внедрение **60 млн ₸**, поддержка **20 млн ₸ в год**

250 × 3 / (60 + 20 × 3) =

625 %

ROSI (возврат инвестиций в ИБ)

Иллюстративный пример

Как наличие расчёта изменяет подход

Риск – не абстрактная категория, а инструмент для принятия решений

Высокий уровень риска при низком ROSI

До расчета: риск оценён как высокий, в план заложено решение стоимостью 48 млн ₸ и 14 млн ₸ ежегодно.

После расчёта: ожидаемые годовые потери 26 млн ₸, мера снижает их на 12 млн ₸ при стоимости владения 30 млн ₸. ROSI – 40%.

Решение: область применения сужена до двух процессов, остальное закрыто организационными мерами. В бюджет возвращено 42 млн ₸.

Средний уровень риска при первом месте в портфеле

До расчета: длительная недоступность ключевой системы оценена как средний риск, инициатива не получала приоритета два бюджетных цикла.

После расчёта: ожидаемые годовые потери 1,31 млрд ₸, первое место в портфеле по потерям. ROSI за 3 года – 625 %.

Решение: инициатива профинансирована в том же бюджетном цикле.

Иллюстративный пример

Ограничения AI

Несуществующая статистика
Модель приводит частоты и ссылки на отчёты, которых нет. Источник проверяется вручную

Отсутствие контекста компании
Параметры двойника берутся из отчётности, а не из ответа модели

Искажение верхней границы
Ошибка в параметре максимума кратно меняет результат при внешне корректном расчёте

Три уровня внедрения

Модель формирует черновик. Эксперт – выбирает границы диапазонов, принимает допущений, отбирает применимые сценарии, подтверждает параметры с бизнес-подразделениями

LIGHT

Обычный чат, без доступа к данным компании

1. По промпту провалидировать список агентов угрозы
2. Сгенерировать черновик сценариев, отобрать применимые
3. Собрать диапазоны ущерба и частоты по своему сценарию
4. Получить код расчета и выполнить моделирование

Результат: расчёт по одному сценарию, пригодный для комитета

MEDIUM

Внутренняя модель работает с выгрузками компании

1. Обучить внутреннюю модель (skills)
2. Определить перечень выгрузок и правила обработки
3. Загрузить в модель отчетность и выгрузки, собрать цифровой двойник
4. Разметить историю инцидентов по типам и величине потерь
5. Определить зрелость контролей по выгрузкам из СЗИ и CMDB

Результат: более точный цифровой двойник, портфель сценариев на собственных данных

HARD

Агент в конуре компании

1. Настроить интеграции с ITSM, CMDB, СЗИ
2. Автоматизировать пересчет сценариев при выдаче параметров
3. Вывести ключевые индикаторы риска (KRI/КИР) на дашборд
4. Интегрировать пересчёт в регулярный процесс оценки и мониторинга рисков

Результат: оценка обновляется автоматически

Что делать дальше?

1. Сформировать цифровой двойник – **15 параметров**
2. Выбрать наиболее очевидный **1 сценарий** (с уже предложенными мерами)
3. **Описать сценарий**: агент угрозы, актив, ущерб
4. Задать минимальные и максимальные **границы**
5. Выполнить моделирование и **рассчитать**: потери, стоимость меры, остаточный риск, ROSI

TG: @mgravita

Чек-лист:
один риск за месяц

Axellect ©

Контакты:

Республика Казахстан, г. Алматы

Проспект Аль-Фараби, 77/7

Бизнес-центр «Esentai Tower»

+7 727 355 10 86

info@axellect.kz

Axellect