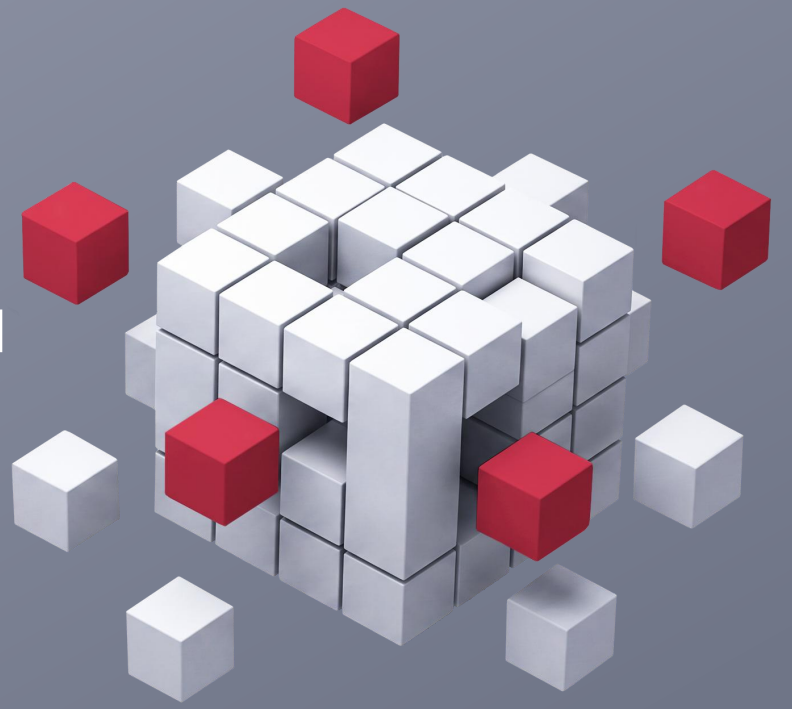
софтлайн РЕШЕНИЯ

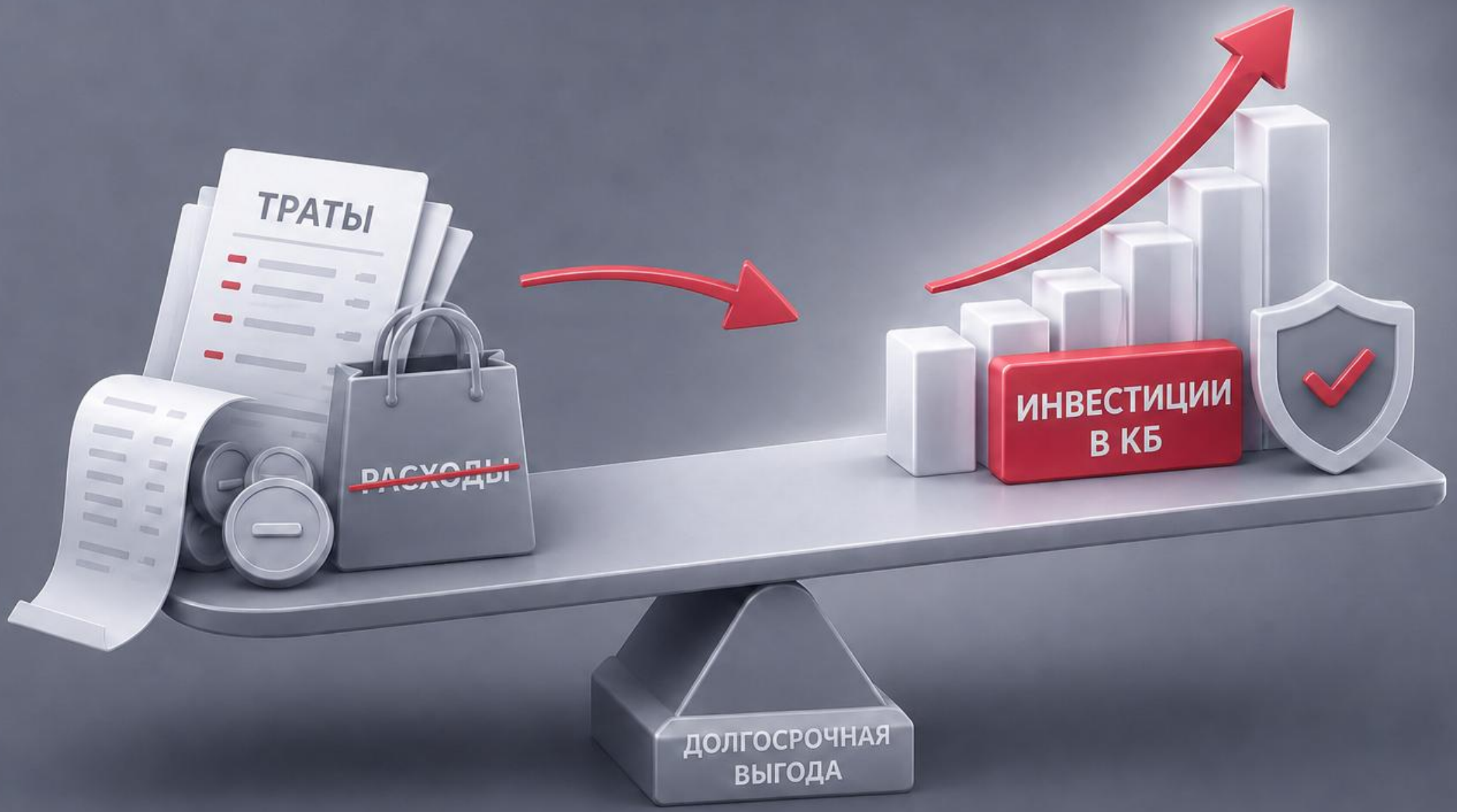
КИБЕРБЕЗОПАСНОСТЬ – фундамент устойчивого роста компании

Как снижение рисков обеспечивает непрерывность бизнеса и сохраняет его маржинальность



Елизавета Маркова

Руководитель отдела риск-менеджмента кибербезопасности



Снижение рисков → Стабильность бизнеса → Доверие клиентов и партнёров → Рост стоимости компании

КЕЙС ИЗ НАШЕЙ ПРАКТИКИ

О компании

- Сфера деятельности: разработка ПО
- Работников: > 1 300
- Конечных точек: > 4 000
- Площадок: > 30

Исходные данные

- Инциденты КБ не случалось
- Попытки кибератак не отслеживались
- Риски КБ никогда не оценивались
- Ресурсы на развитие КБ не выделялись

КЕЙС ИЗ НАШЕЙ ПРАКТИКИ

Инцидент

1. Хакеры скомпрометировали инфраструктуру, закрепились, **украли чувствительные данные**
2. Вредоносная активность была замечена **слишком поздно** и инфраструктуру отключили от Интернета
3. Бизнес-процессы Компании были полностью **парализованы на 7 недель**
4. Сроки по проектам были сорваны и Компания понесла **серьезный финансовый ущерб**

КЕЙС ИЗ НАШЕЙ ПРАКТИКИ

Восстановление

- Поскольку ранее кибербезопасности не уделялось внимание, восстановление начало выполняться **в авральном режиме**
- Средства на восстановление **выдернуты из оборота** внепланово
- Для получения уверенности, что хакер больше не имеет доступ к сети запланирована **полная миграция всех систем** на новую ИТ-инфраструктуру (включая физические устройства)
- Ввиду огромных масштабов компании, разрозненной ИТ-инфраструктуры, отсутствия управления кибербезопасностью полное восстановление требует длительного времени, в течение которого **бизнес-процессы терпят ограничения**

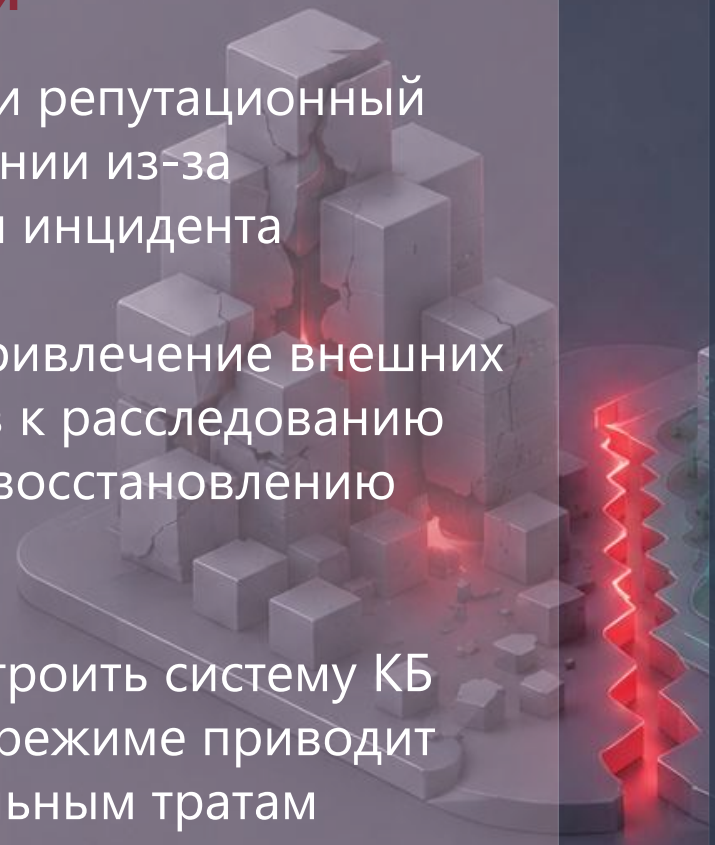
НЕ готовы к инциденту

Потери

Финансовый и репутационный ущерб Компании из-за случившегося инцидента

Затраты на привлечение внешних специалистов к расследованию инцидента и восстановлению после него

Попытка выстроить систему КБ в авральном режиме приводит к нерациональным тратам на средства защиты, которые не работают эффективно из-за нехватки времени на внедрение



Готовы к инциденту

Инвестиции

Вложения происходят не все сразу, а постепенно – в соответствии с планом и приоритетами защиты

Внедряем не все подряд, а подходим «с умом», взвешиваем решения о внедрении с учетом релевантных рисков и выгод бизнеса

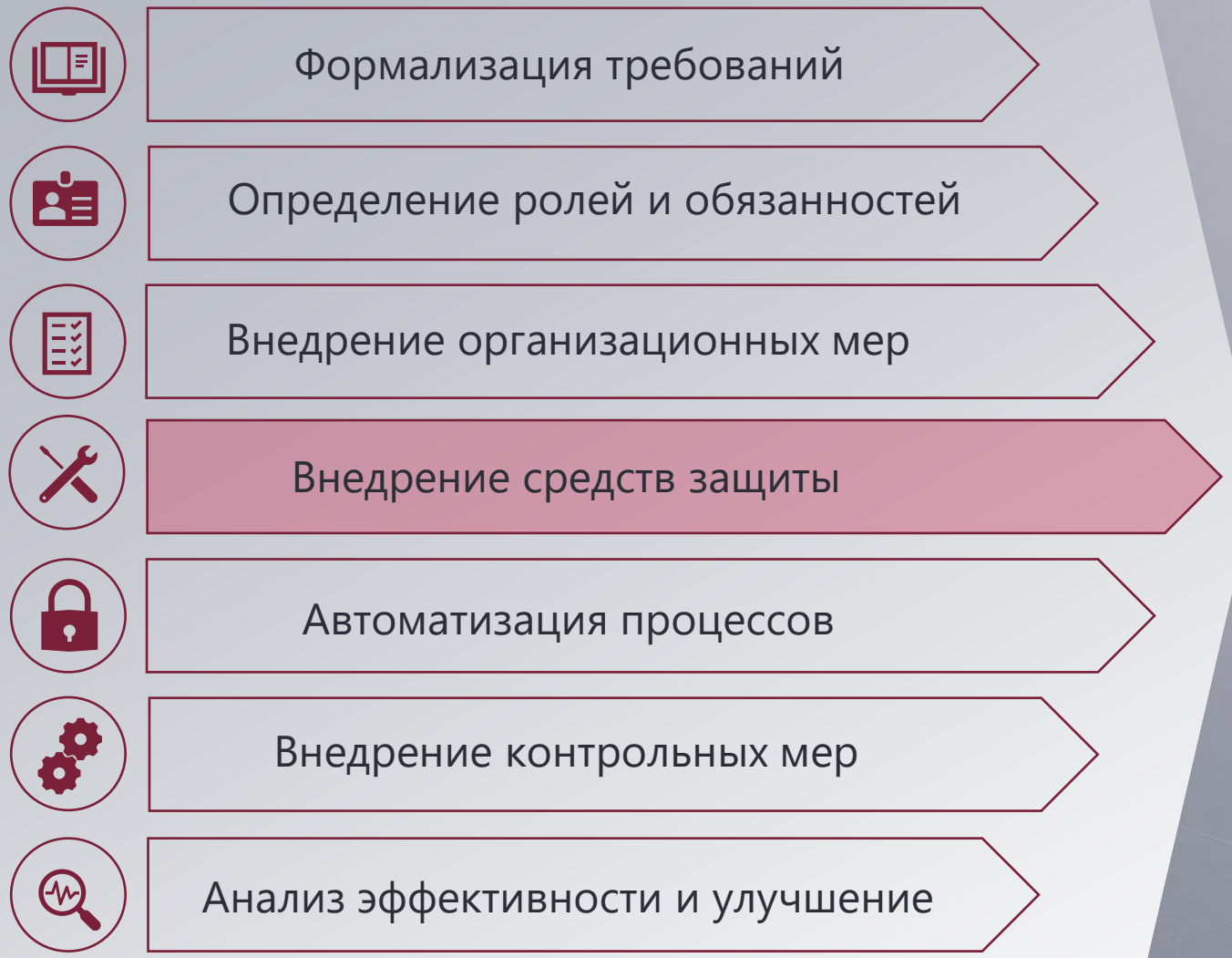
Выстраиваем эффективную защиту в соответствии с приоритизированным планом мероприятий, что позволяет не только отражать попытки атак, но и быстро восстанавливаться в случае инцидентов

Только средства защиты

Комплексный подход к защите

Сами по себе средства защиты не обеспечивают достаточный уровень безопасности — только тщательно выстроенные процессы обеспечивают реальную защиту

КОМПЛЕКСНАЯ ЗАЩИТА



Базовые процессы КБ

Организация КБ	Управление активами
Контроль доступа	Безопасность разработки ПО
Безопасность поставщиков	Управление изменениями
Управление уязвимостями	Безопасность конфигураций
Реагирование на инциденты	Сетевая безопасность
Непрерывность бизнеса	Повышение осведомленности
Антивирусная защита	Управление рисками

АНОМАЛИИ, ВЫЯВЛЯЕМЫЕ У НАШИХ ЗАКАЗЧИКОВ

Внедрили сканер уязвимостей
Да, но:

- Покрытие неполное
- Сканирование завершается с ошибками – траблшутинг не выполняется
- Десятки тысяч строк в отчете – не понятно, как агрегировать
- SLA либо вообще отсутствует, либо есть, но не контролируется
- Процесс управления обновлениями не выстроен

Внедрили систему PAM
Да, но:

- Покрыто лишь 30% ресурсов / учетных записей
- Нет понимания: что именно покрывать, кто такие привилегированные пользователи, надо ли контрагентов пускать через PAM, надо ли покрывать Linux-сервера?
- А что с резервным доступом, если PAM «устанет»?

Внедрили антивирусное средство
Да, но:

- Покрыты только хосты Windows
- Отключен ряд модулей, базы не обновляются
- Некорректные настройки несут риски отказа в обслуживании, потере контроля над хостами
- Большое количество ошибок – траблшутинг не выполняется

Внедрили средство защиты от DDoS
Да, но:

- Правила выставлены по умолчанию
- Существенная доля операций ручного переключения трафика
- Планы BCP и DRP не учитывают сценарий реагирования на DDoS-атаки
- Обучение специалистов не проводится

Необходима приоритизация мероприятий ввиду ограниченных ресурсов

Оценка рисков КБ

СВЯЗЬ КИБЕРБЕЗОПАСНОСТИ И БИЗНЕСА

НАШИ ПОДХОДЫ В ОБОСНОВАНИИ БЮДЖЕТА

Оценка рисков КБ

- Расчет ROSI *(опция)*
- Монетизация инцидентов *(опция)*

Кадровый дизайн

- Обоснование численности команды кибербезопасности

ОЦЕНКА РИСКОВ КБ. Где искать риски?

Бизнес-процесс

- Цели
- Этапы
- Участники
- Требования
- Ценная информация
- Ключевые системы
- «Страхи» бизнеса

Что может случиться?

Конфиденциальность будет нарушена:
произойдет утечка чувствительной для компании информации

Целостность будет нарушена
критичная для процесса информация будет подменена или удалена

Доступность будет нарушена:
ключевые информационные системы перестанут работать, и процесс остановится

ОЦЕНКА РИСКОВ КБ. Примеры негативных событий для бизнеса

Негативные события	*Последствия для бизнеса*
Длительные перебои в работе и/или полное отключение кассового обслуживания в торговых точках	• Недополученная прибыль • Отток клиентов • Затраты на восстановление
Утечка значительного количества персональных данных	• Регуляторные штрафы • Отток клиентов и инвесторов • Подрыв репутации
Массовая утечка деталей соглашений с клиентами и партнерами	• Разрыв контрактов с ключевыми партнерами • Отток клиентов и инвесторов
Массовая модификация информации о продуктах, услугах и заказах клиентов	• Отток клиентов • Финансовые потери • Затраты на восстановление
Длительная недоступность клиентских онлайн-сервисов	• Недополученная прибыль • Отток клиентов • Затраты на восстановление

ОЦЕНКА РИСКОВ КБ. Расчет рисков

1 Формирование сценария реализации риска

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

2 Оценка вероятности реализации риска

- Характеристики нарушителя
- Оценка зрелости контрольной среды КБ

3 Оценка последствий реализации риска

- Ценность затронутых активов

или

- Бизнес-метрики:
  - Количество клиентов
  - Прибыль в единицу времени
  - Приток клиентов
  - …

4 Уровень риска

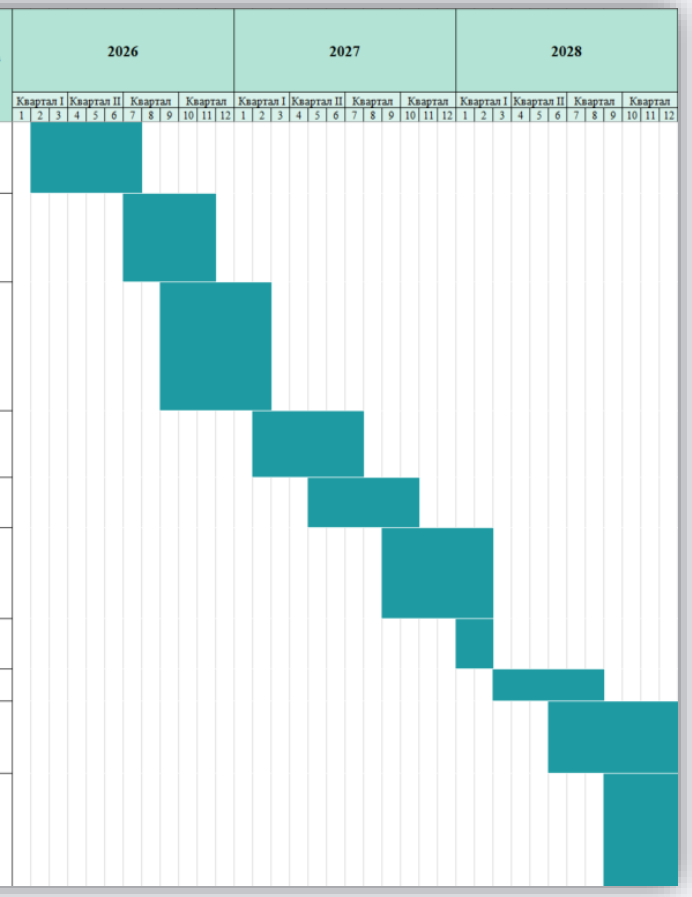
- Качественный подход

или

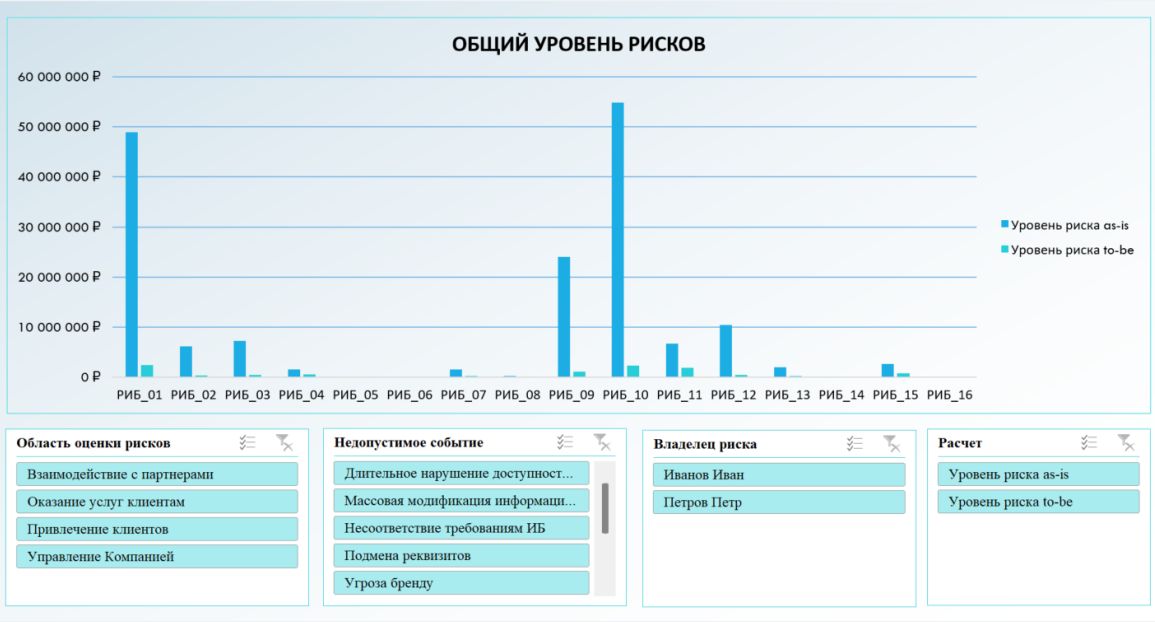
- Количественный подход

ОЦЕНКА РИСКОВ КБ. Дорожная карта приоритизированных мер КБ

Область контроля / направление	Мероприятия по обработке рисков	Массовая модификация информации о товарах 140 000 900 ₽	Подмена реквизитов 24 599 709 ₽	Утечка чувствительной информации клиентов 12 000 089 ₽	Утечка значительного количества ПДн работников 89 970 785 ₽	Уровень влияния на риск низкий - 1 средний - 10 высокий - 30	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	Начало	Завершение	Длительность в месяцах
Защита от вредоносного ПО	1. Обеспечить полное покрытие (АРМ и сервера всех ОС) средством антивирусной защиты. 2. Для исключений из процесса управления антивирусной защитой разработать и реализовать компенсирующие меры (например, изоляция, усиление конфигураций, защита трафика и пр.). Задокументировать исключения с описанием причин и компенсирующих мер по смягчению последствий и принятию остаточных рисков.	Да	Да	Да	Да	высокий (30)	низкая (3)	средняя (2)	2026	Февраль 2026	Июль 2026	6
Управление доступом	1. Рассмотреть возможность передачи логина и пароля разными каналами связи (для всех субъектов доступа, видов доступа, ИС). 2. Обеспечить смену временного пароля для удаленных пользователей (например, после подключения к домену, использование веб-портала для смены пароля). 3. Обеспечить периодическую смену пароля для гостевой Wi-Fi сети (не реже одного раза в год).	Да	Да	Да	Да	средний (10)	низкая (3)	быстрая (3)	2026	Июль 2026	Ноябрь 2026	5
Управление уязвимостями	1. Реализовать планы по выстраиванию процесса приоритизации уязвимостей. Приоритет и сроки устранения уязвимостей определять на основании следующих факторов (при их наличии): - тренды уязвимости; - наличие эксплойта; - критичность ИТ-актива, в котором была выявлена уязвимость; - критичность уязвимости; - трудозатраты на устранение уязвимости. 2. Вести реестр ресурсов / проектов с указанием ответственных - для прозрачности процесса определения ответственного / команды за устранение уязвимости в том или ином активе.	Да	Да	Да	Да	средний (10)	низкая (3)	быстрая (3)	2026	Сентябрь 2026	Февраль 2027	6
Управление уязвимостями	1. Выполнять установку обновлений с периодичностью, определенной Регламентом управления конфигурациями и изменениями в информационной инфраструктуре, не позднее одного месяца с момента публикации обновления. 2. Обеспечить централизованное управление обновлениями ОС и прикладного ПО для серверов и АРМ.	Да	Да	Да	Да	высокий (30)	средняя (2)	средняя (2)	2027	Февраль 2027	Июль 2027	6
Защита от вредоносного ПО	1. Обеспечить мониторинг конечных точек (АРМ и серверов) с целью реагировании на подозрительную активность, например, путем внедрения системы класса EDR. Обеспечить покрытие, как минимум, критичных активов.	Да	Да	Да	Да	высокий (30)	высокая (1)	средняя (2)	2027	Май 2027	Октябрь 2027	6
Управление безопасностью ПО на стадиях жизненного цикла (практики безопасной разработки ПО)	1. Внедрить автоматизированные инструменты проверки ПО и программного кода (SAST, DAST и SCA) для всех разрабатываемых систем. 2. Проводить тестирование разрабатываемых продуктов с т.з. ИБ как неотъемлемую часть безопасного жизненного цикла. 3. Реализовать периодическое проведение тестирований на проникновение для всех разрабатываемых систем.	Да	Да	Да	-	высокий (30)	высокая (1)	средняя (2)	2027	Сентябрь 2027	Февраль 2028	6
Управление активами	1. Выполнять аудит установленного на АРМ и серверах ПО с помощью автоматизированного средства для сбора сведений об установленном ПО не реже одного раза в квартал.	Да	Да	Да	Да	средний (10)	низкая (3)	быстрая (3)	2028	Январь 2028	Февраль 2028	2
Сетевая безопасность	1. Обеспечить шифрование внешних каналов передачи данных (между ЦОД и офисами; между офисами; между устройствами удаленных работников и внутренней сетью).	Да	Да	Да	Да	высокий (30)	высокая (1)	средняя (2)	2028	Март 2028	Август 2028	6
Управление конфигурациями	1. Разработать или, при необходимости, актуализировать стандарты безопасного конфигурирования для всех компонентов ИТ-инфраструктуры: контроллеров домена, всех используемых ОС АРМ и серверов, сетевого оборудования (в т.ч. коммутаторы, Wi-Fi роутеры), веб-серверов, СУБД, СЗИ, средств контейнеризации. Обеспечить настройку компонентов ИТ-инфраструктуры в соответствии со стандартами безопасных конфигураций.	Да	Да	Да	Да	высокий (30)	высокая (1)	медленная (1)	2028	Июнь 2028	Март 2029	10
Обеспечение непрерывности деятельности и резервное копирование	1. Документировать сквозной процесс для описания порядка резервного копирования, в частности: - постановка ресурса на РК для всех ИС и сервисов; - требования к определению параметров РК: расписания РК, способа выполнения РК, срока хранения РК, места хранения РК. 2. Рассмотреть возможность обеспечения резервного копирования для всех ресурсов Компании. 3. Разработать программу тестирования резервных копий на корректность восстановления для всех ресурсов Компании. 4. Обеспечить тестирование восстановления из резервных копий не реже одного раза в квартал.	Да	Да	-	-	средний (10)	низкая (3)	медленная (1)	2028	Сентябрь 2028	Декабрь 2028	4



ОЦЕНКА РИСКОВ КБ. Дашборды оценки рисков

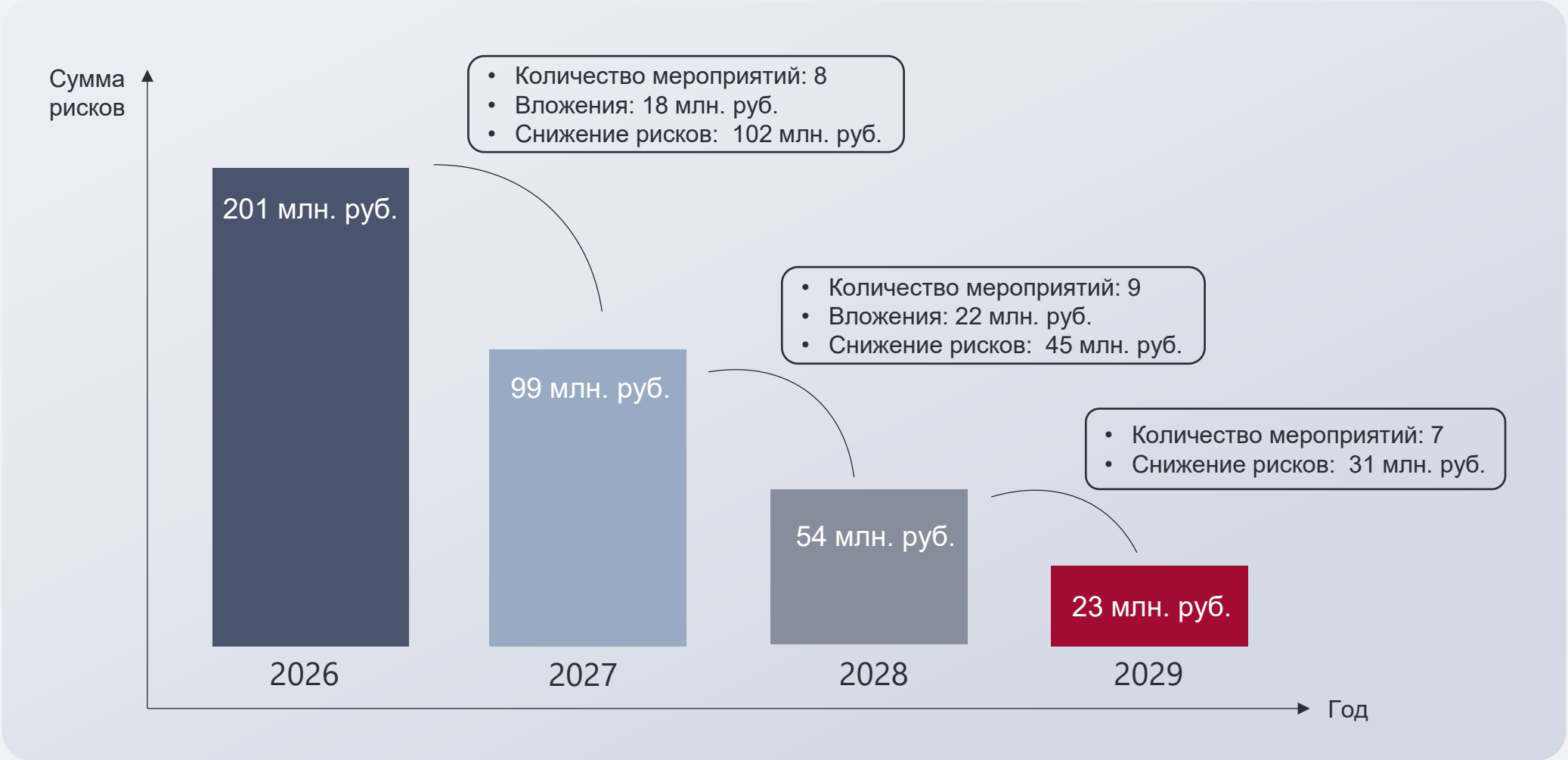


16
Общее количество рисков

166 498 128 ₽
Сумма рисков

54 834 384 ₽
Максимальный риск

ОЦЕНКА РИСКОВ КБ. Влияние вложений на уровень рисков



ОЦЕНКА РИСКОВ КБ. Расчет ROSI

$$RoSI = \frac{(\text{Ожидаемые потери} - \text{Потери после внедрения}) - \text{Стоимость защиты})}{\text{Стоимость защиты}}$$

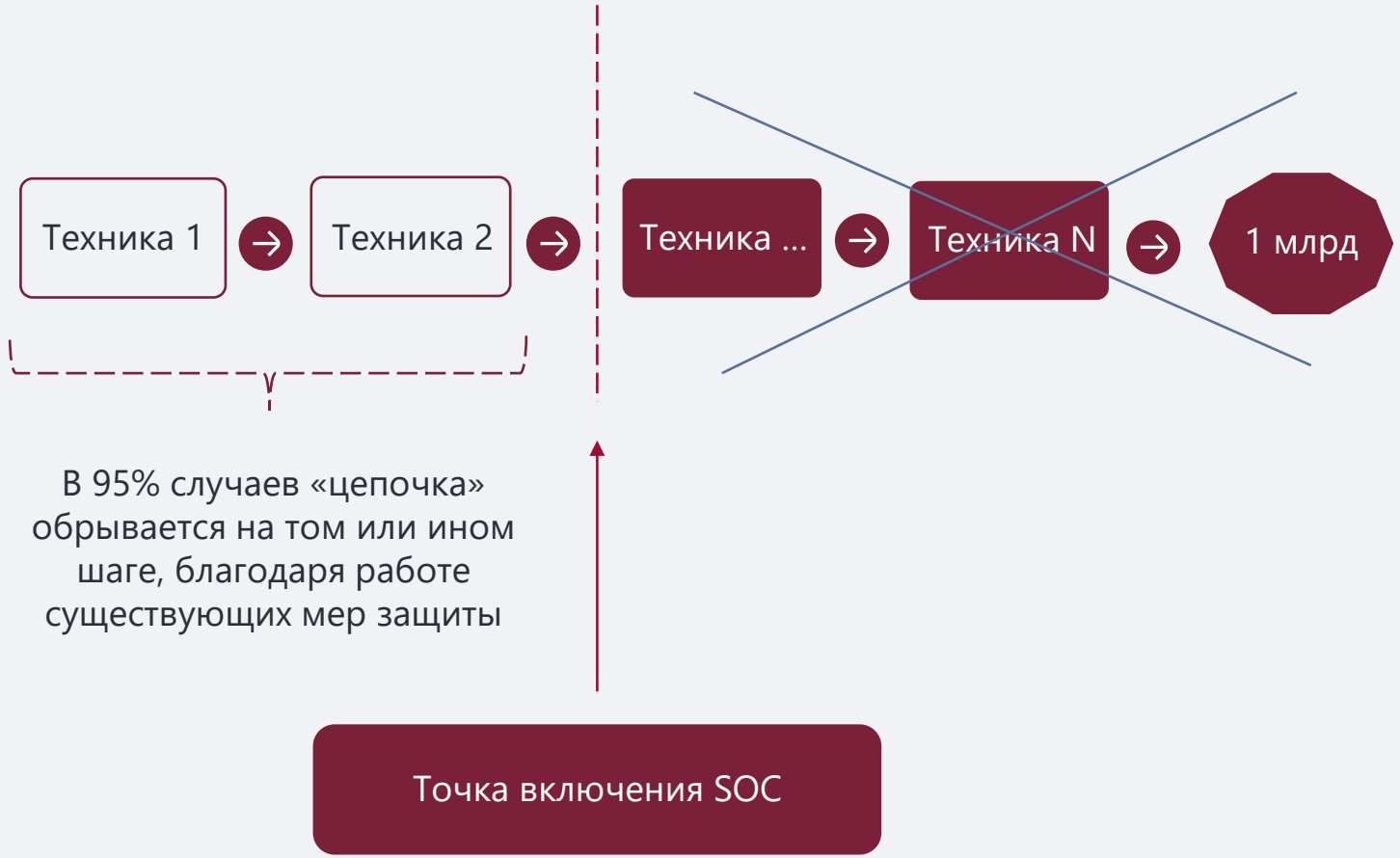
Return on Security Investment

Окупаемость инвестиций в безопасность

ОЦЕНКА РИСКОВ КБ.

Монетизация инцидентов

1. Формирование ТОПа наиболее распространенных инцидентов на основе статистики SOC
2. Формирование тепловых карт по наиболее релевантным техникам MITRE ATT&CK
3. Формирование релевантных цепочек атак на основе полученной статистики
4. Расчет величины риска от непредотвращения инцидента
5. Расчет RoSI



КАДРОВЫЙ ДИЗАЙН. Проблематика кадрового планирования в КБ

Компаний испытывают сложности с наймом специалистов по КБ

Организаций сталкивается с дефицитом навыков в своих командах КБ

Компаний описывают свои команды КБ как частично или значительно недоукомплектованные

Сложность обоснования штата КБ перед руководством

Отсутствие прозрачной модели, позволяющей аргументированно защищать потребность в ресурсах

Несоответствие кадровых решений реальным рискам и критичности активов

Штат КБ формируется без учета контекста бизнеса, специфики ИТ-инфраструктуры, текущего и целевого уровня зрелости процессов ИТ и КБ

Неэффективное распределение ресурсов

Где-то наблюдается перегруз ключевых ролей КБ, где-то функции избыточны и не дают прироста защищенности

КАДРОВЫЙ ДИЗАЙН. Что в основе при планировании команды

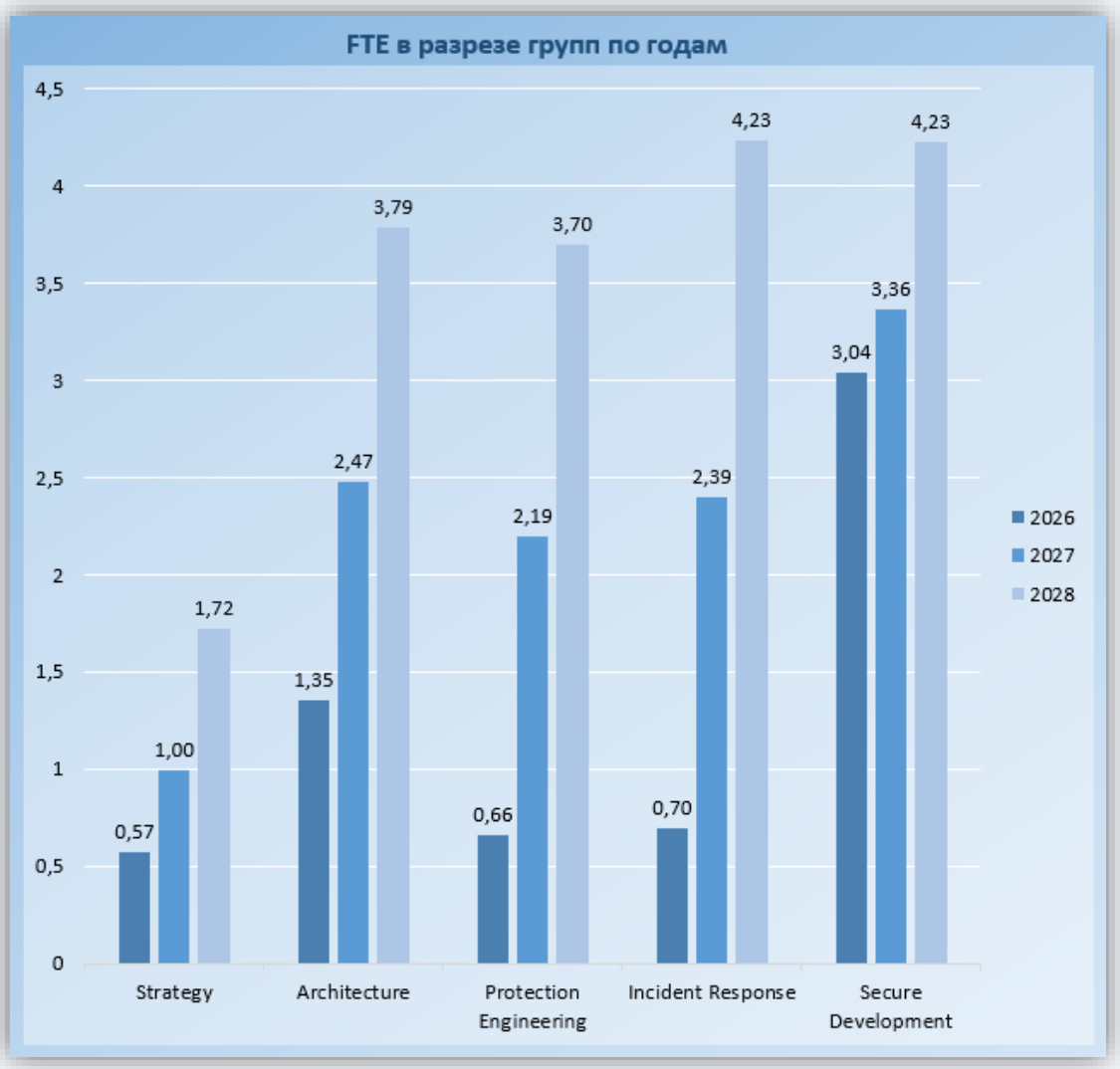
Формирование ключевых критериев*,
влияющих на численность функции КБ и уровень компетенций персонала

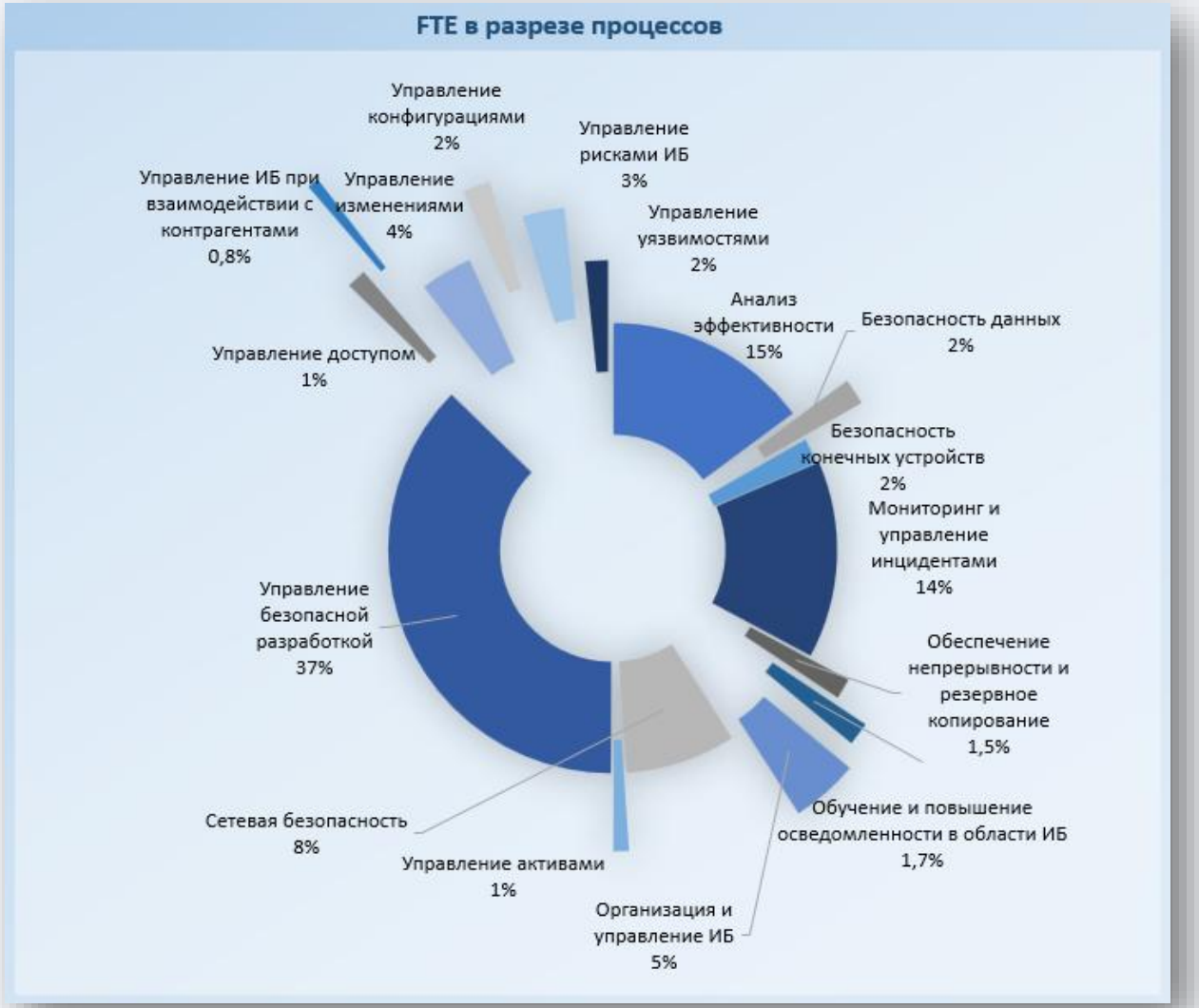
1	Изучение специфики бизнеса Компании и выявление ключевых направлений деятельности	• отраслевая принадлежность • контекст бизнеса, влияющий на процессы и меры КБ • наличие собственной разработки ПО …
2	Выявление негативных для бизнеса событий КБ и критичных процессов	• степень и значимость производственных объектов • интенсивность деятельности предприятий • негативные для бизнеса события КБ …
3	Анализ применимых требований в части формирования функции КБ	• требования регуляторов в области КБ • требования стандартов • требования материнской компании и/или контрагентов …
4	Сбор сведений о текущем составе функции КБ и планах по модернизации	• численность персонала • планы по модернизации функции КБ …
5	Сбор сведений о специфике ИТ-инфраструктуры и уровне зрелости процессов КБ	• специфика ИТ-инфраструктуры • текущий целевой уровень зрелости процессов КБ …

Приведены примеры критериев

КАДРОВЫЙ ДИЗАЙН.

Дашборды инструмента планирования команды КБ

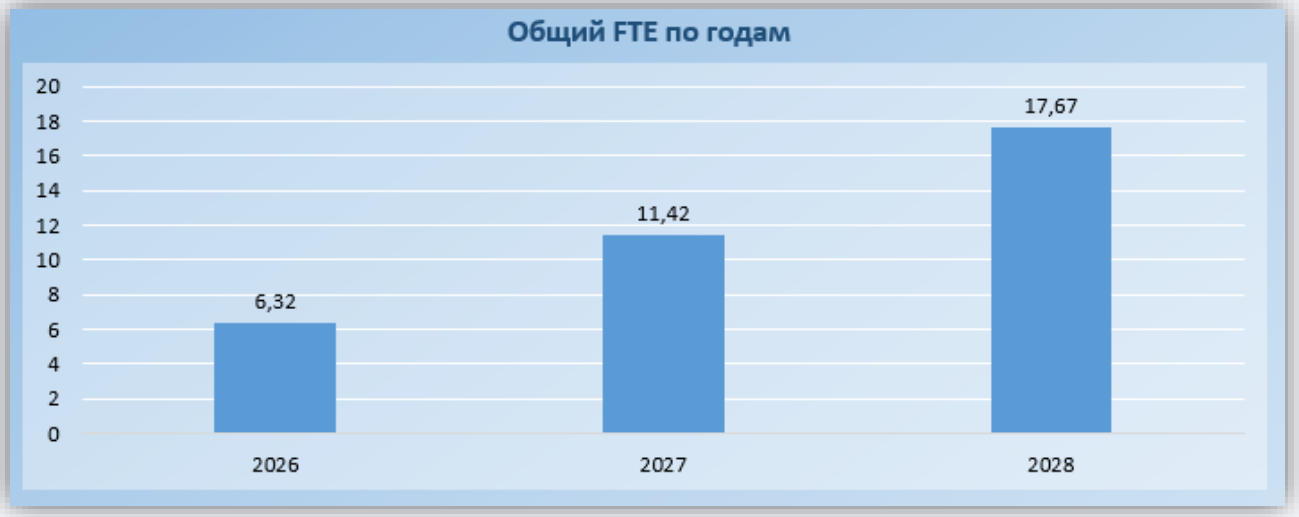




КАДРОВЫЙ ДИЗАЙН.

Дашборды инструмента планирования команды КБ

Роль	FTE 2026	FTE 2027	FTE 2028
CISO	0,279	0,555	1,000
Методолог ИБ	0,781	1,448	2,287
Архитектор безопасности	0,232	0,437	0,667
Руководитель проектов	0,059	0,170	0,325
Риск-менеджер	0,230	0,272	0,398
Аналитик эффективности процессов ИБ	0,038	0,255	0,397
Аудитор ИБ	0,160	0,177	0,222
Организатор обучения по ИБ	0,139	0,159	0,215
Инженер ИБ	0,440	1,333	2,422
Сетевой инженер	0,163	0,662	0,942
Аналитик SIEM	0,130	0,802	1,458
Инженер реагирования на инциденты	0,503	1,375	2,390
AppSec	1,519	1,681	2,113
DevSecOps	1,519	1,681	2,113



КЛЮЧЕВЫЕ АСПЕКТЫ ОБОСНОВАНИЯ БЮДЖЕТА

Приоритизация с учетом интересов бизнеса
Ресурсы всегда будут ограничены, необходимо долгосрочное планирование с учетом риск-ориентированного подхода

Киберустойчивость – главный приоритет
Пока ИТ-инфраструктура простаивает, бизнес теряет деньги

Диалог на языке бизнеса
На языке финансов, рисков, выгод и потерь

Компактность и наглядность
Для ТОП-менеджмента важна скорость приятия риск-ориентированных решений

ОСТАВЛЯЕМ КАК ЕСТЬ

Принимаем риски:

- Подрыв репутации
- Финансовый ущерб
- Регуляторные штрафы
- Судебные иски
- Отток клиентов

СТРАТЕГИЧЕСКИЙ ПОДХОД

- Используем правильные инструменты для прозрачного обоснования бюджета на КБ перед руководством
- Внедряем систему КБ с учетом актуальных рисков и приоритетов бизнеса
- Выстраиваем команду КБ с учетом специфики компании и уровня зрелости КБ

КОНТАКТЫ

Елизавета Маркова

Руководитель отдела риск-менеджмента кибербезопасности

elizaveta.markova@softline.com