AKTIV.
CONSULTING

Оценка уровня зрелости ИБ.
Взгляд со стороны консультанта

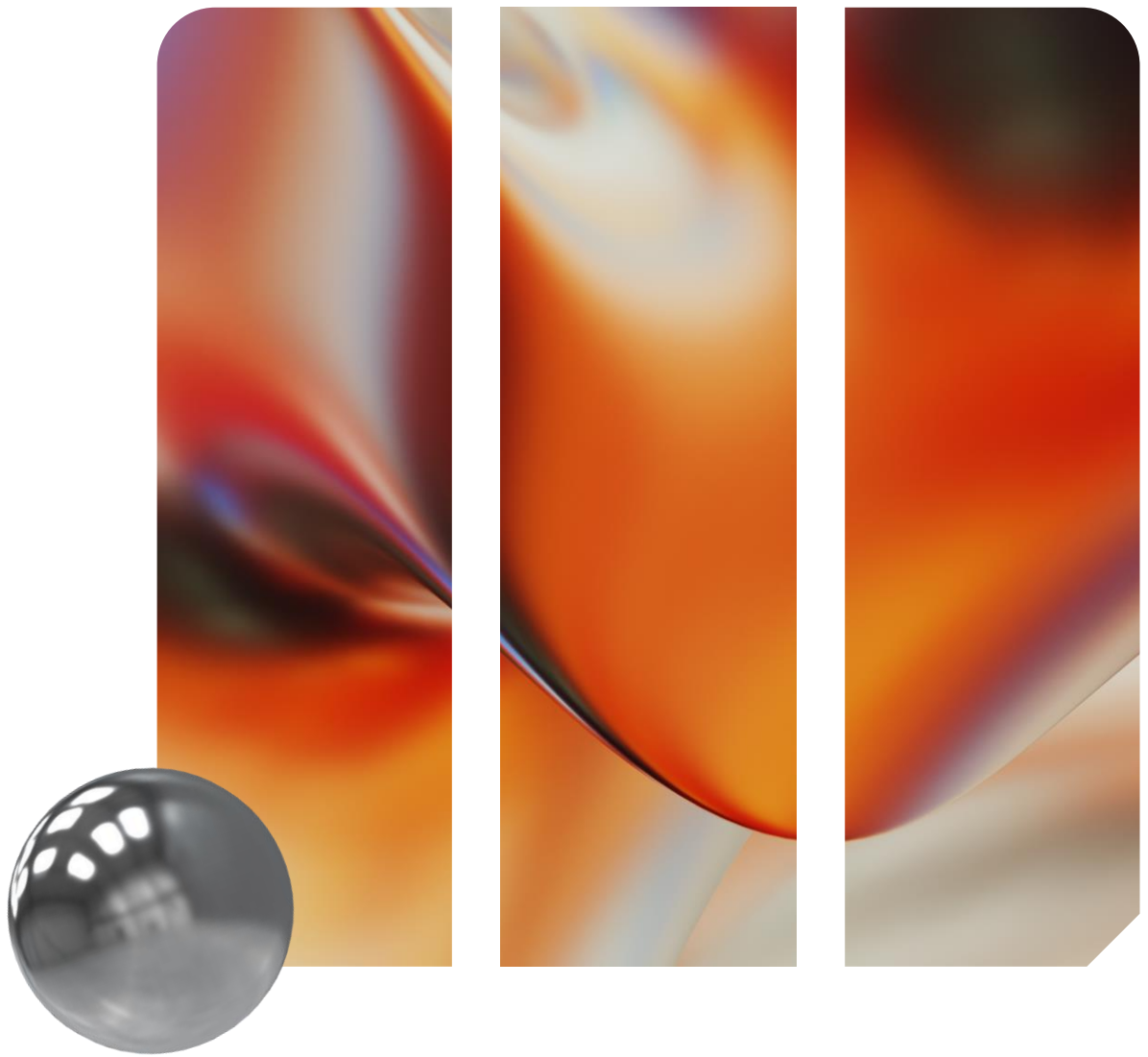
Ольга Копейкина

Руководитель отдела консалтинга
по информационной безопасности

Оценка зрелости.
О чем это?

Оценка зрелости ИБ проводится в отношении существующей системы защиты информации для **выявления технических и организационных уязвимостей и недостатков**.

Определение критических аспектов позволяет разработать оптимальные пути по их устранению, и является **ключевым этапом в построении стратегии кибербезопасности**.



Зачем оценивать зрелость ИБ?

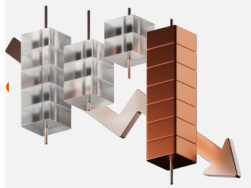
Повышение эффективности мер безопасности

Выявление слабых мест

Комплаенс

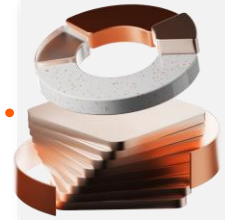
Оптимизация затрат

Улучшение репутации



Снижение рисков

Планирование развития



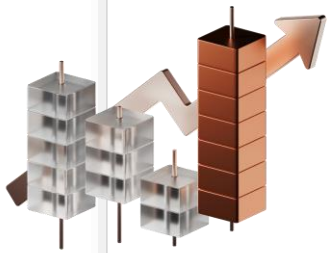
Обеспечение непрерывности бизнеса

Повышение осведомлённости сотрудников

Когда пора задуматься о комплексной оценке?

Компания готова **инвестировать в развитие ИБ**

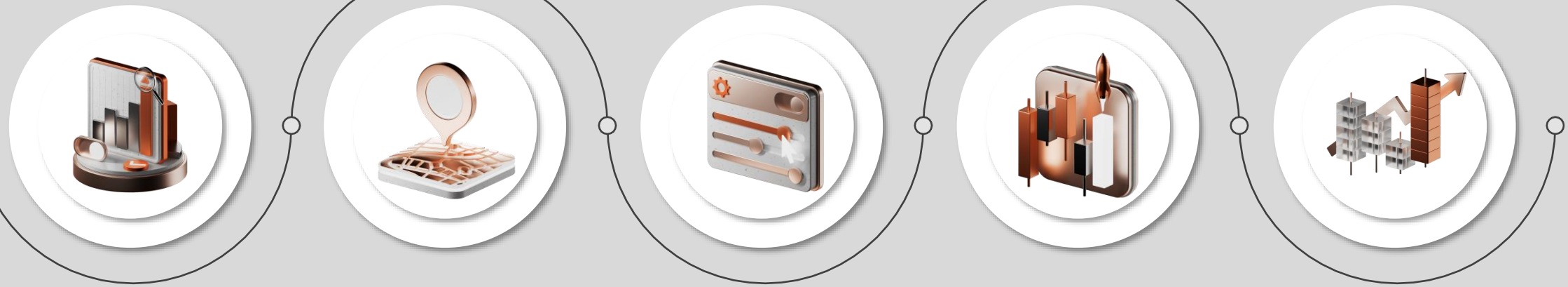
Компания имеет **сложную распределенную сетевую инфраструктуру**



Планируется **внедрение новых информационных технологий** и расширение систем

В основных задачах стоит **приведение в соответствие ИБ требованиям** регуляторов

Этапы проведения оценки



1

Обследование инфраструктуры, бизнес- и технологических процессов

2

Определение целевого уровня зрелости ИБ

3

Проведение комплекса анализов

4

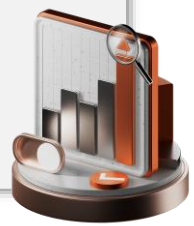
Выявления ключевых расхождений фактических и целевых показателей

5

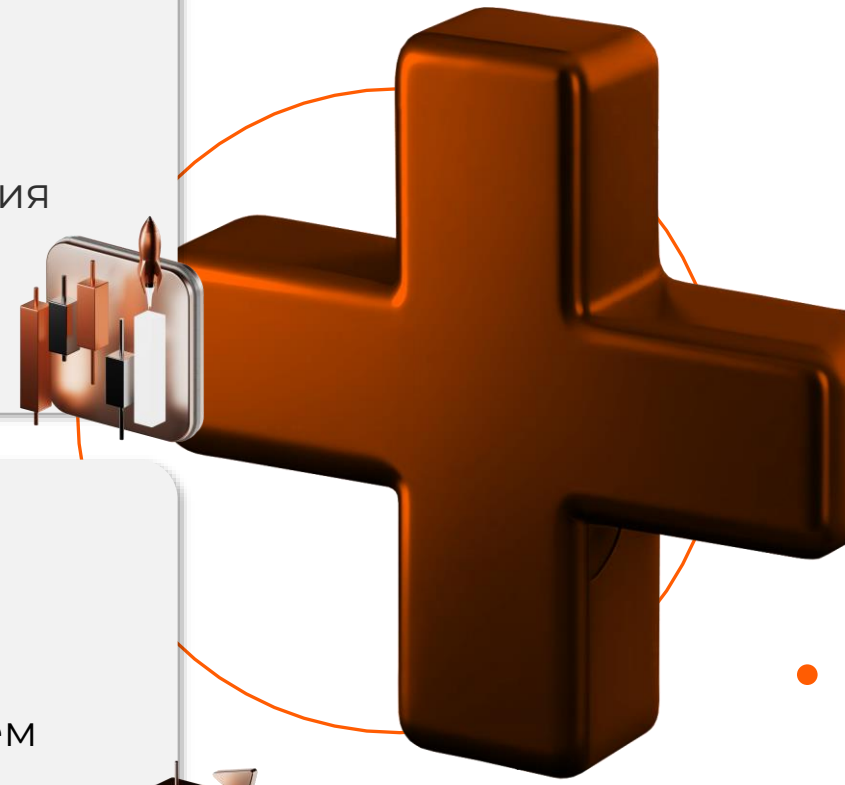
Построение плана мероприятий для оптимизации структуры ИБ

Применяемые виды анализа

Исследование актуального ландшафта угроз
выявление уязвимостей и рисков, которые могут угрожать защищаемой информации

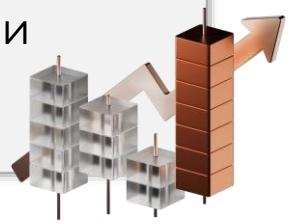


SWOT-анализ
методология анализа текущего состояния организации с точки зрения её сильных и слабых аспектов, а также возможностей и угроз



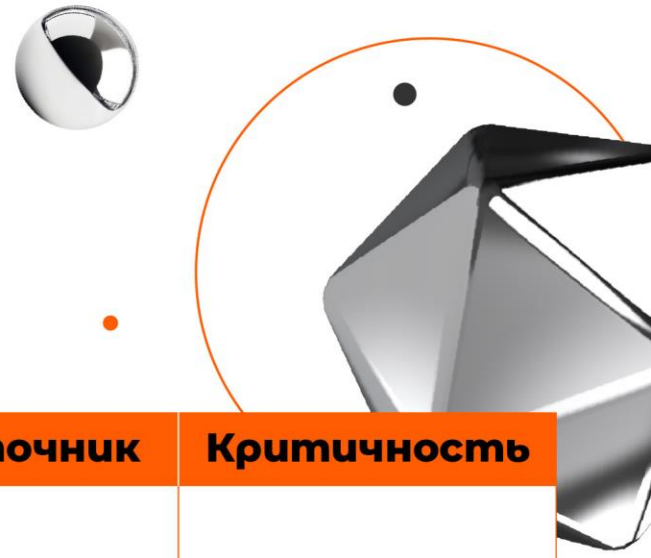
Сценарный анализ
методология оценки потенциальных угроз и рисков, связанных с информационной системой, путём моделирования различных сценариев атак и анализа их последствий

Gap-анализ
(анализ разрывов)
методология выявления и оценки несоответствий между текущим состоянием и целевыми показателями



Исследование ландшафта угроз

Результат:
Карта вероятных угроз с определением возможных источников реализации, критичности их последствий, затрагиваемых информационных ресурсов



Направление	Угроза	Источник	Критичность
Эксфильтрация данных	• Кража ноу-хау по перспективным проектам с применением стеганографии • Фотофиксация информации ограниченного распространения на личные устройства • Вынос HDD за пределы офиса • Преобразование архивов для обхода СЗИ • Восстановление данных с компонент ИТ-инфраструктуры	Внутренний нарушитель	Высокая
Атака на цепочку поставок	• Компрометация данных через подрядчиков • Атака из границы внутренней сети филиалов или головного офиса	Подрядчик	Средняя
Фишинг + социальная инженерия	• Возможность кражи и шифрования данных • Хищение аутентификационных данных или заражение ВПО в результате перехода по небезопасным ссылкам	Внешний нарушитель	Высокая
Недекларируемые возможности и бэкдоры	• Несанкционированный доступ к устройствам жертвы • Компрометация клиентских аккаунтов через утечки из других сервисов	Внутренний / внешний нарушитель	Средняя
Ошибки конфигурирования элементов ИТ-инфраструктуры	• Некорректная работа средств защиты • Некорректное функционирование ИТ-инфраструктуры	Работник	Средняя

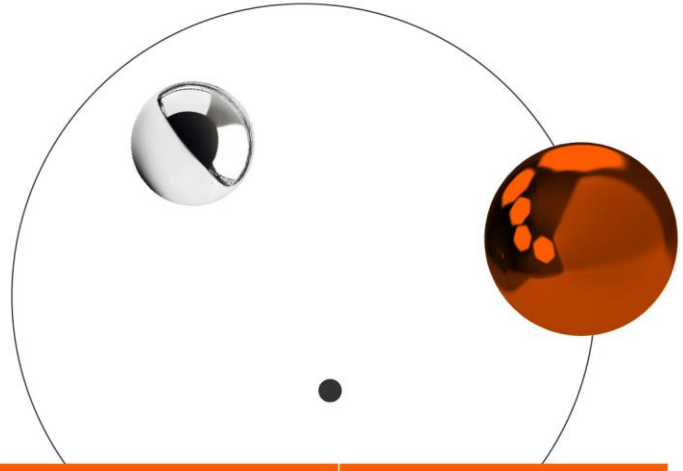
SWOT-анализ

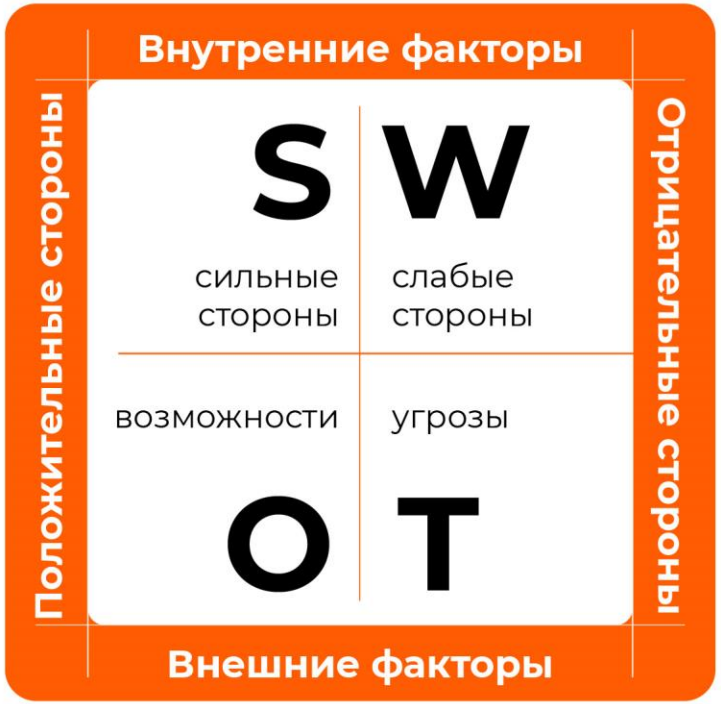
Результат:
Развернутая фактура внутренних и внешних аспектов, влияющих на состояние ИБ организации как в сторону усиления, так и требующих коррекции, а также пути оптимизации

	Внутренние факторы	Отрицательные стороны
Положительные стороны	**S** сильные стороны	**W** слабые стороны
	O возможности	**T** угрозы
	Внешние факторы	

SWOT-анализ

Результат:
Развернутая фактура внутренних и внешних аспектов, влияющих на состояние ИБ организации как в сторону усиления, так и требующих коррекции, а также пути оптимизации





	Критические угрозы	Критические угрозы	Критические угрозы
Высокая вероятность	Уход сотрудника, обладающего доступом к чувствительной для компании информации, в организацию-конкурента	Недостаточное покрытие инцидентов в нерабочее время	Угрозы, связанные с распределенной структурой организации
Средняя вероятность	Внедрение программных уязвимостей в ПО с открытым исходным кодом злоумышленником	Устаревшие версии инструментов анализа	Срывы сроков ключевых задач из-за внедрения новых процессов
Малая вероятность	Использование устаревших образов с уязвимостями	Недостаточное покрытие тестирования из-за нехватки персонала	Сложности интеграции новых инструментов

Сценарный анализ

Результат: модели возможных атак, учитывая такие факторы, как уязвимости в системе, методы и инструменты, используемые злоумышленниками, а также потенциальные последствия для организации

Угроза	БДУ ФСТЭК	Описание	Сценарий реализации		
			Техника (методика ФСТЭК)	Название техники	MITRE ATT&CK
Использование привилегированной учетной записи для изменения конфигурации	УБИ.83 УБИ.98 УБИ.99 УБИ.103 УБИ.104 УБИ.132	Уход сотрудника, обладающего доступом к чувствительной для компании информации, в организацию-конкурента	T2.1	Использование внешних сервисов организации в сетях публичного доступа *(Интернет)* **Примеры:** 1) доступ к веб-серверу, расположенному в сети организации; 2) доступ к интерфейсу электронной почты OutlookWebAccess *(OWA)* почтового сервера организации	Отсутствует
	УБИ.185		T2.4	Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке	Отсутствует
	УБИ.175		T2.8	Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы	T1566
	УБИ.8 УБИ.100		T2.10	Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя *(методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)*	T1110
	УБИ.8 УБИ.175 УБИ.181		T2.11	Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля *(для личных или служебных нужд)*	T1078

Сценарный анализ

Сценарий «Кража интеллектуальной собственности инсайдером»

Область: Обеспечение конфиденциальности информации

Краткое описание сценария атаки: злонамеренные действия сотрудника с легитимным доступом к корпоративным системам, направленные на кражу конфиденциальной информации

Классификация сценария атаки:

Фаза 1: {T1591}.{002} + {003} : {T1083}.

Фаза 2: {T1588}.{005} : {T1078}.{001} : {T1059}.{001} + {003} : {T1053}.{005} : {T1036}.{005} : {T1552}.{001} + {004} : {T1016} + {T1135}.

Фаза 3: {T1005} + {T1213} : {T1078}.{002} : {T1070}.{004} + {1140} : {T1555}.{003} : {T1046} + {T1049} : {T1570} + {T1563}.{001} : {T1005} + {T1213} : {T1567}.{002} + {T1048}.{003}.

Фаза 4: {T1550}.{003}.

Описание сценария атаки:

...текстовое описание каждой фазы...

Фаза	Разведка	Подготовка ресурсов	Первоначальный доступ	Выполнение	Закрепление	Повышение привилегий	Предотвращение обнаружения	Получение учетных данных	Обнаружение	Перемещение внутри периметра	Сбор данных	Организация управления	Эксфильтрация данных	Деструктивное воздействие
1	{T1591}.{002} + {003}	—	—	—	—	—	—	—	{T1083}	—	—	—	—	—
2	—	{T1588}.{005}	{T1078}.{001}	{T1059}.{001} + {003}	{T1053}.{005}	—	{T1036}.{005}	{T1552}.{001} + {004}	{T1016} + {T1135}	—	—	—	—	—
3	—	—	—	{T1005} + {T1213}	—	{T1078}.{002}	{T1070}.{004} + {1140}	{T1555}.{003}	{T1046} + {T1049}	{T1570} + {T1563}.{001}	{T1005} + {T1213}	—	{T1052}	—
4	—	—	—	—	—	—	{T1070}{004} + {005} + {001} + {007} + {003}	—	—	—	—	—	—	—

Gap-анализ

Результат:
идентифицированные «разрывы» между установленными целями и фактическими результатами, причины данного несоответствия и основания для построения стратегии для его преодоления

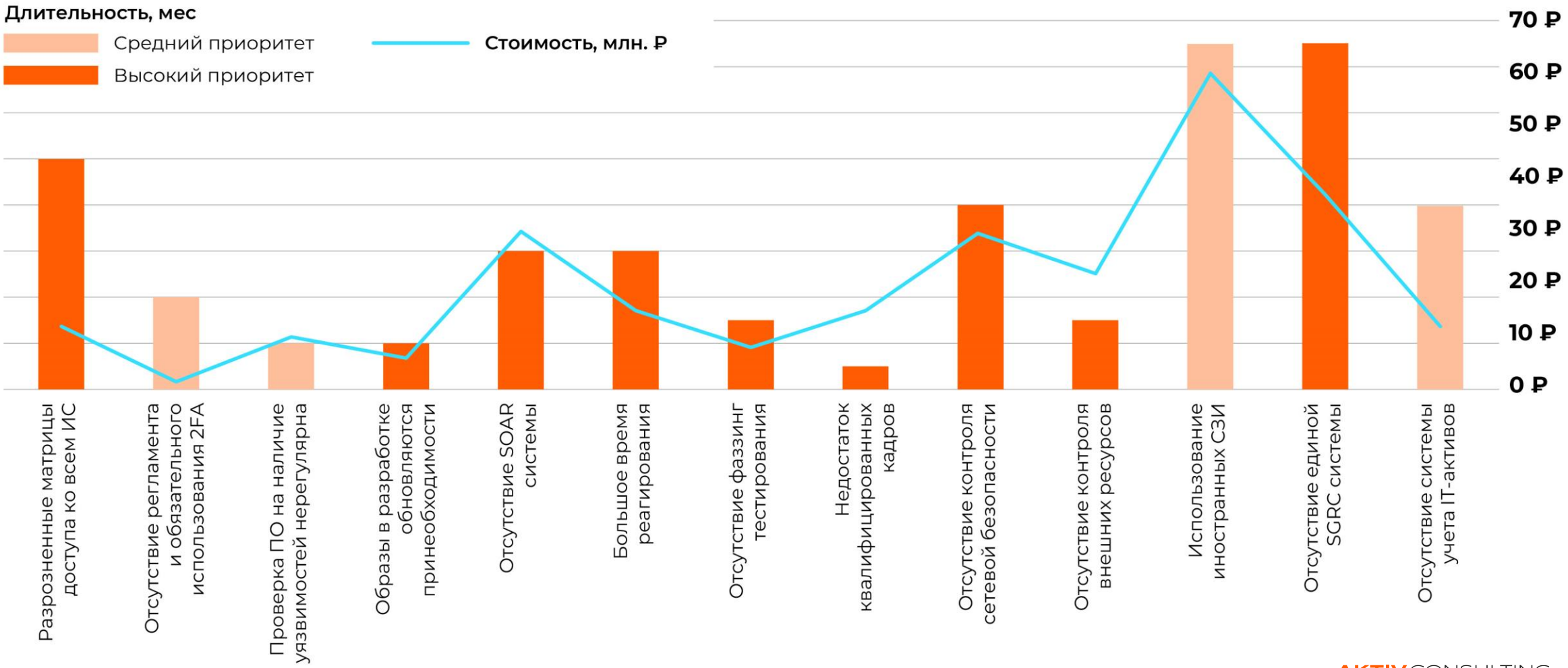
Разрыв	Эталон	Приоритет
Разрозненные матрицы доступа ко всем ИС	Единая ролевая модель доступа с четким разграничением прав доступа к информации	**Высокий**
Отсутствие регламента и обязательного использования 2FA	Невозможность использования чужой учетной записи для доступа в ИС	**Средний**
Проверка ПО на наличие уязвимостей и его обновление выполняется нерегулярно	Отсутствие программных уязвимостей в используемом ПО *(ПО с открытым исходным кодом, ПО, разработанное компанией)*	**Средний**
Отсутствие централизованного контроля сетевой безопасности	Единая система управления политиками сетевой безопасности	**Высокий**

Gap-анализ

Результат:
идентифицированные «разрывы» между установленными целями и фактическими результатами, причины данного несоответствия и основания для построения стратегии для его преодоления

Приоритет	Мероприятия по устранению разрыва	Тип мероприятия	Необходимые ресурсы, время реализации
Разрозненные матрицы доступа ко всем ИС	Разработка единой матрицы доступа к информации	Организационно-техническое	10-15 млн руб. *(лицензии на IAM)* + 2-3 млн руб. *(интеграция)* + обучение персонала **9-12 месяцев**
Отсутствие регламента и обязательного использования 2FA	Разработать регламент по многофакторной аутентификации \ рассмотреть дополнительно внедрение 2FA на физ. носителе *(токен)*	Организационное	1-2 млн руб. *(разработка регламентов)* + 1-2 млн руб. *(закупка токенов)* **3-4 месяца**
Проверка ПО на наличие уязвимостей и его обновление выполняется нерегулярно	Внедрение регулярного обновления используемого ПО с обязательной проверкой на уязвимости при обновлении	Техническое	8-12 млн руб. *(системы управления уязвимостями)* + 2-3 млн руб. *(интеграция)* **1-2 месяца**
Отсутствие централизованного контроля сетевой безопасности	Внедрение NAC-решения, автоматизация контроля политик	Техническое	20-25 млн руб. *(NAC-решение)* + 5-7 млн руб. *(автоматизация)* **6-8 месяцев**

Gap-анализ


Длительность, мес
Средний приоритет
Высокий приоритет
Стоимость, млн. ₽
70 ₽
60 ₽
50 ₽
40 ₽
30 ₽
20 ₽
10 ₽
0 ₽
Разрозненные матрицы доступа ко всем ИС
Отсутствие регламента и обязательного использования 2FA
Проверка ПО на наличие уязвимостей нерегулярна
Образы в разработке обновляются принеобходимости
Отсутствие SOAR системы
Большое время реагирования
Отсутствие фаззинг тестирования
Недостаток квалифицированных кадров
Отсутствие контроля сетевой безопасности
Отсутствие контроля внешних ресурсов
Использование иностранных СЗИ
Отсутствие единой SGRC системы
Отсутствие системы учета IT-активов

Участники оценки

Правильный состав участников команды проекта — один из ключевых критериев успешности оценки уровня зрелости ИБ, последующего планирования и реализации мероприятий по его оптимизации

1

ИБ-подразделения
Основные заинтересованные в эффективности проекта лица, наиболее погруженные в проблемы безопасности

Участники оценки

Правильный состав участников команды проекта — один из ключевых критериев успешности оценки уровня зрелости ИБ, последующего планирования и реализации мероприятий по его оптимизации

1

ИБ-подразделения
Основные заинтересованные в эффективности проекта лица, наиболее погруженные в проблемы безопасности

2

ИТ-подразделения
Эксплуатирующие ИС подразделения, обладающие детальной информацией об инфраструктуре

Участники оценки

Правильный состав участников команды проекта — один из ключевых критериев успешности оценки уровня зрелости ИБ, последующего планирования и реализации мероприятий по его оптимизации

1 **ИБ-подразделения**
Основные заинтересованные в эффективности проекта лица, наиболее погруженные в проблемы безопасности

2 **ИТ-подразделения**
Эксплуатирующие ИС подразделения, обладающие детальной информацией об инфраструктуре

3 **Бизнес-подразделения**
Меры по ИБ принимаются в интересах бизнеса, и не могут быть отделимы от бизнес-процессов

Участники оценки

Правильный состав участников команды проекта — один из ключевых критериев успешности оценки уровня зрелости ИБ, последующего планирования и реализации мероприятий по его оптимизации

1

ИБ-подразделения
Основные заинтересованные в эффективности проекта лица, наиболее погруженные в проблемы безопасности

2

ИТ-подразделения
Эксплуатирующие ИС подразделения, обладающие детальной информацией об инфраструктуре

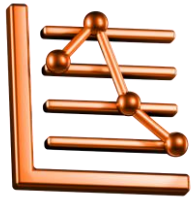
3

Бизнес-подразделения
Меры по ИБ принимаются в интересах бизнеса, и не могут быть отделимы от бизнес-процессов

4

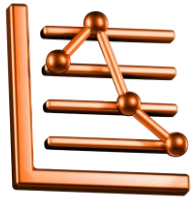
Независимый оценщик
Взгляд со стороны позволяет обеспечить объективность обследования и исключает «замыленность» взгляда на системы и процессы

Типичные сложности



Сопротивление ИТ и бизнес-подразделений

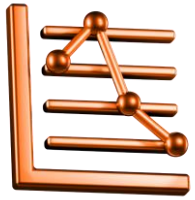
Типичные сложности



Сопротивление ИТ и бизнес-подразделений

Отсутствие детальных данных об инфраструктуре

Типичные сложности

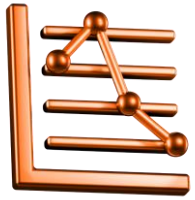


Сопротивление ИТ и бизнес-подразделений

Отсутствие детальных данных об инфраструктуре

Неготовность делиться информацией

Типичные сложности



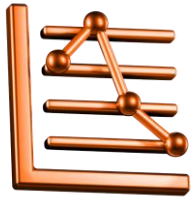
Сопротивление ИТ и бизнес-подразделений

Отсутствие детальных данных об инфраструктуре

Неготовность делиться информацией

Отсутствие четко поставленных целей

Типичные сложности



Сопротивление ИТ и бизнес-подразделений

Отсутствие детальных данных об инфраструктуре

Неготовность делиться информацией

Отсутствие четко поставленных целей

Неготовность видеть недостатки

Что в результате?

По итогам оценки уровня зрелости достигаются ответы на вопросы «Что? Зачем? Как? С какой целью?» в отношении построения ИБ

В результате:

CISO → Детальный и обоснованный **план мероприятий** по укреплению и оптимизации ИБ компании

CEO + CISO → **Минимизация затрат** на обеспечение ИБ за счет расстановки приоритетов рисков и возможности их реализации

CEO + CISO → **Единое понимание целей и задач ИБ** у всех подразделений организации

AKTIV.
CONSULTING

БЛАГОДАРЮ
ЗА ВНИМАНИЕ!

Ольга Копейкина

Руководитель отдела консалтинга
по информационной безопасности

kopeikina@aktiv.consulting

AKTIV.
CONSULTING