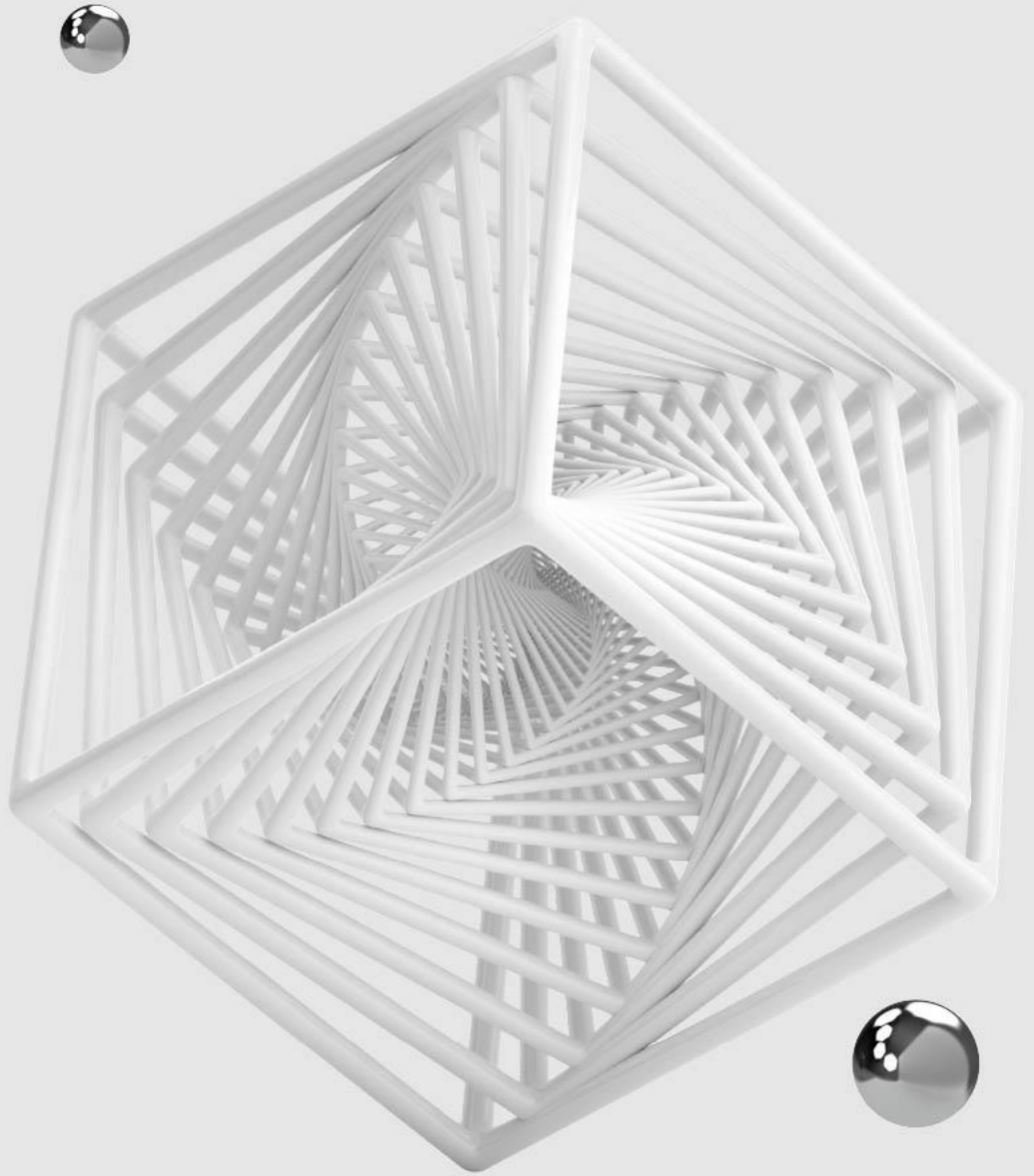
AKTIV.
CONSULTING

КОМПАНИЯ АКТИВ

Вебинар

Какова зрелость информационной безопасности в отечественных компаниях



О чем сегодня пойдет речь?

Про цель и порядок проведения исследования

Полученные данные

Инструмент самооценки

Сравнительный анализ

Финальные выводы

Мнение независимых экспертов

AKTIV.
CONSULTING

Аналитический отчет «Оценка уровня зрелости ИБ» 2026 г.

Варвара Шубина

Руководитель направления маркетинга AKTIV.CONSULTING

Предпосылки исследования

Не все отечественные компании имеют возможность проведения регулярной оценки уровня зрелости ИБ, причины:

Отсутствие простых фреймворков

Отсутствие собственных ресурсов

Отсутствие ресурсов для обращения за консалтингом

Предпосылки исследования

При этом получение регулярной, объективной оценки уровня зрелости функции ИБ становится основой для:

Корректировки стратегии по развитию ИБ *(стратегический уровень)*

Формирования целевого состояния и роадмапа для развития *(тактический уровень)*

Выявления «уязвимых» мест

Обоснования бюджетов и ТЭО для закупки и обновления технического парка

Плана по развитию персонала службы ИБ

Формирования системы мотивации и KPI для службы ИБ

Цели исследования

Цели исследования: Отразить актуальную ситуацию в части обеспечения информационной безопасности в отечественных компаниях с целью гармоничного развития функции ИБ. Аналитическое исследование призвано определить текущее состояние ключевых процессов информационной безопасности в российских компаниях с целью выявления пробелов и выработки рекомендаций по повышению эффективности ИБ.

Объект исследования: 52 специалиста по ИБ.

* Компании с выделенной функцией информационной безопасности.

Методология

Для анонимного исследования был разработан самоопросник для оценки уровня зрелости ИБ, содержащий 100 сценариев. Все сценарии разбиты на пять направлений, посвященных процессам ИБ:

1. **«Управление ИБ»**

   связано с управлением процессами обеспечения информационной безопасностью

2. **«Базовая ИТ- и ИБ-гигиена»**

   касается базовых мер обеспечения ИБ

3. **«Обеспечение ИБ»**

   связано с техническим оснащением службы ИБ

4. **«Мониторинг, реагирование и восстановление»**

   касается обеспечения защиты данных

5. **«Комплаенс»**

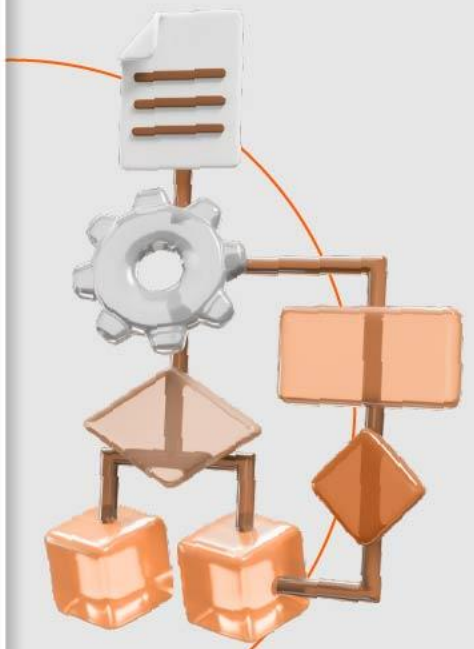
   связано с выполнением требований регуляторов

В каждом направлении 5 вопросов, в каждом вопросе 4 сценария на выбор.

Пример опросника

Категория I.1. Планирование деятельности по ИБ

Сценарий A	Формализованного планирования не осуществляется, оно осуществляется стихийно, исходя из оперативных потребностей
Сценарий B	Планирование деятельности осуществляется в пределах 1 года
Сценарий C	Существует дорожная карта развития ИБ на плановый период. Осуществляется ежегодное планирование в соответствии с дорожной картой
Сценарий D	Существует стратегия развития ИБ на плановый период. Запущены долгосрочные проекты, выделены бюджеты, назначены ответственные



Определение уровня зрелости

Каждому из четырех предложенных сценариев соответствует определенный уровень зрелости от (0 до 3):

- Сценарий A = 0 уровень зрелости.
- Сценарий B = 1 уровень зрелости.
- Сценарий C = 2 уровень зрелости.
- Сценарий D = 3 уровень зрелости.

В каждом направлении мы получили суммарную оценку, а также процент уровня зрелости ИБ

* За 100% принимается максимально возможная суммарная оценка по каждому направлению = 15.

Пример расчета

Категория I.4. Ресурсное обеспечение ИБ. Кадры		Оценка
Сценарий B	Планирование деятельности осуществляется в пределах 1 года.	1

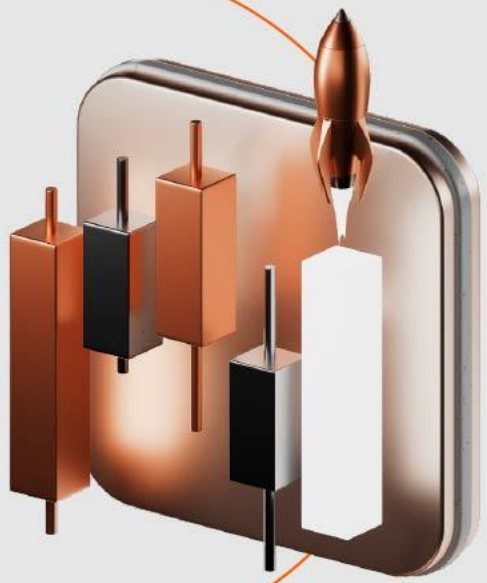
Категория I.2. Вовлеченность бизнеса в вопросы ИБ		Оценка
Сценарий C	ИБ активно вовлечена в бизнес-деятельность собственной организации, и безопасность поставщиков продуктов и услуг. CISO участвует в ключевых совещаниях по основной производственной деятельности.	2

Категория I.3. Ресурсное обеспечение ИБ. Финансирование		Оценка
Сценарий B	Бюджет ИБ не реализуется в полной мере, хоть в него и включаются позиции по самому минимуму. Финансирование ИБ осуществляется бессистемно.	1

Категория I.4. Ресурсное обеспечение ИБ. Кадры		Оценка
Сценарий D	Найм персонала не является проблемой *(предложение в рынке или даже чуть выше)*. Финансовая мотивация осуществляется в должной мере, есть квартальное и годовое премирование.	3

Категория I.5. Управление рисками ИБ		Оценка
Сценарий A	Процедуры управления рисками ИБ не формализованы и не проводятся в явном виде, а осуществляются скорее по наитию.	0

Итоговая оценка	7 (47%)



Обеспечение анонимности

Самооценка проходила в два этапа:

- Первый этап — заполнение анкеты для дальнейшей верификации.
- Второй шаг — анонимная самооценка.

Анонимность собранных данных обеспечивалась **за счет хеширования.**

Схема обеспечения анонимности собранных данных:

- На первом шаге участники заполняли краткую анкету и создавали уникальный идентификатор — пин-код. В системе хранится только хеш от пин-кода.
- Следующий шаг — уникальная ссылка для доступа к опроснику самооценки. Опросник открывался после введения пин-кода.
- В системе не хранились данные участников, только хеш, совпадающий с кодом для доступа к системе.

Независимые эксперты

Александр Дворянский,
Директор по информационной безопасности ПАО «Элемент»

Петухов Алексей,
Лидер центра компетенций «Кибербезопасность»
НТИ Энерджинет

Леонид Плетнев,
Бизнес-партнер по информационной безопасности «1С-Битрикс»

Андрей Нуйкин,
Начальник управления информационной безопасности ЕВРАЗа.

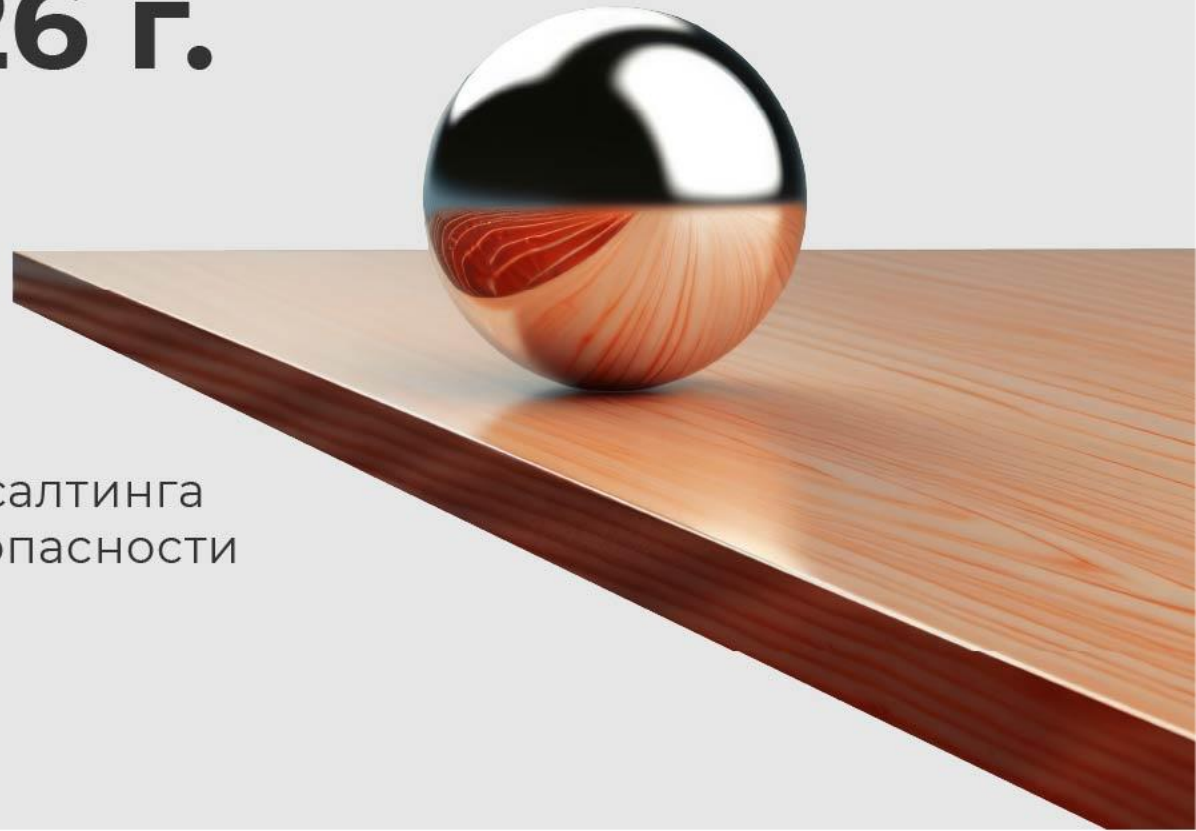
Александр Найко,
CISO АО «БИРЖА "ЦТС"»

Для получения объективной оценки результатов независимые эксперты по информационной безопасности ознакомились с итогами аналитического исследования и ответили на следующие вопросы:

1. **Релевантны ли полученные данные для вашей отрасли?**
2. **Согласны ли вы, что полученные выводы и тенденции можно масштабировать на все отечественные компании?**
3. **Какие ключевые изменения необходимы для повышения уровня зрелости информационной безопасности в разных областях:**
   - Со стороны государства в лице регуляторов?
   - Со стороны рынка ИБ (производители средств СЗИ, компании, оказывающие услуги по ИБ: консалтинговые компании, интеграторы, дистрибутор и т.д.)?
   - Со стороны самих организаций?
   - Со стороны комьюнити специалистов по ИБ?

AKTIV.
CONSULTING

Аналитический отчет «Оценка уровня зрелости ИБ» 2026 г.

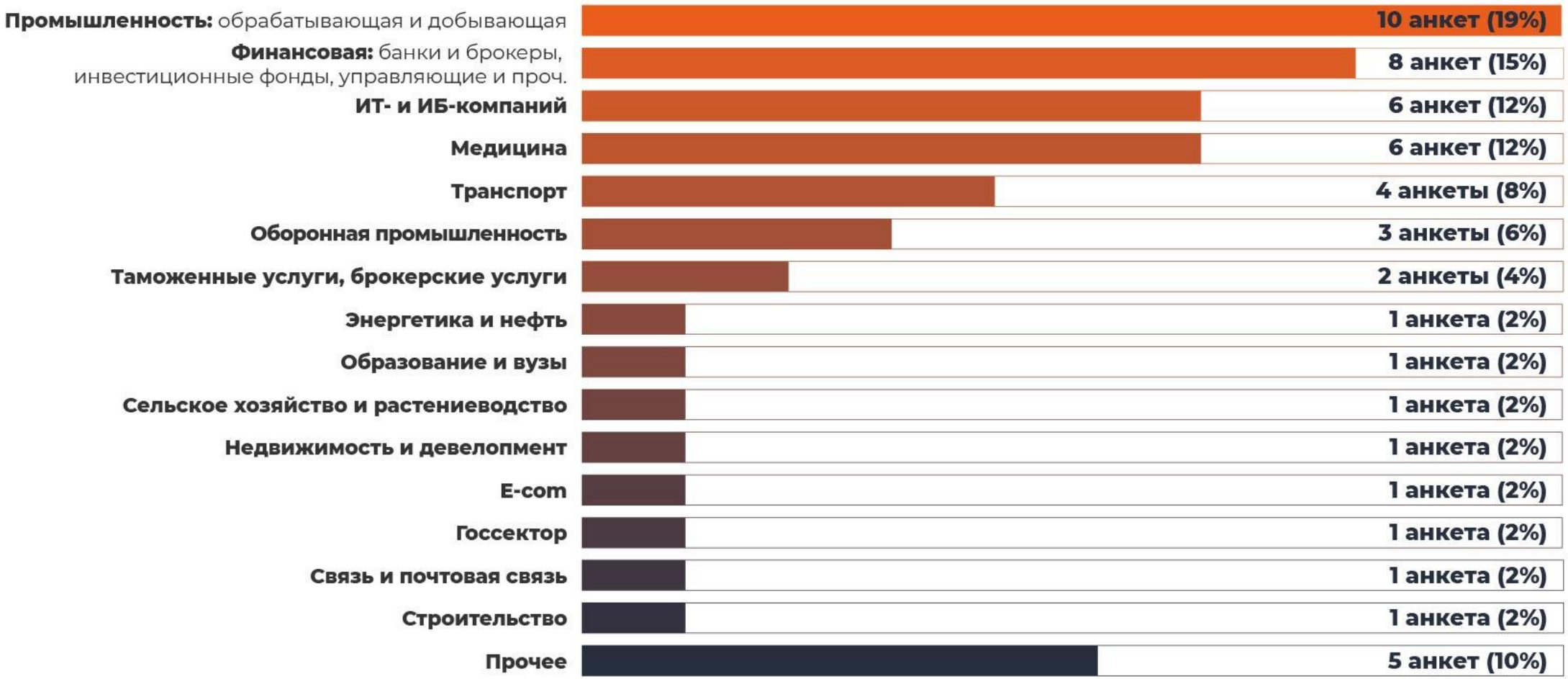


Ольга Копейкина

Руководитель отдела консалтинга
по информационной безопасности
AKTIV.CONSULTING

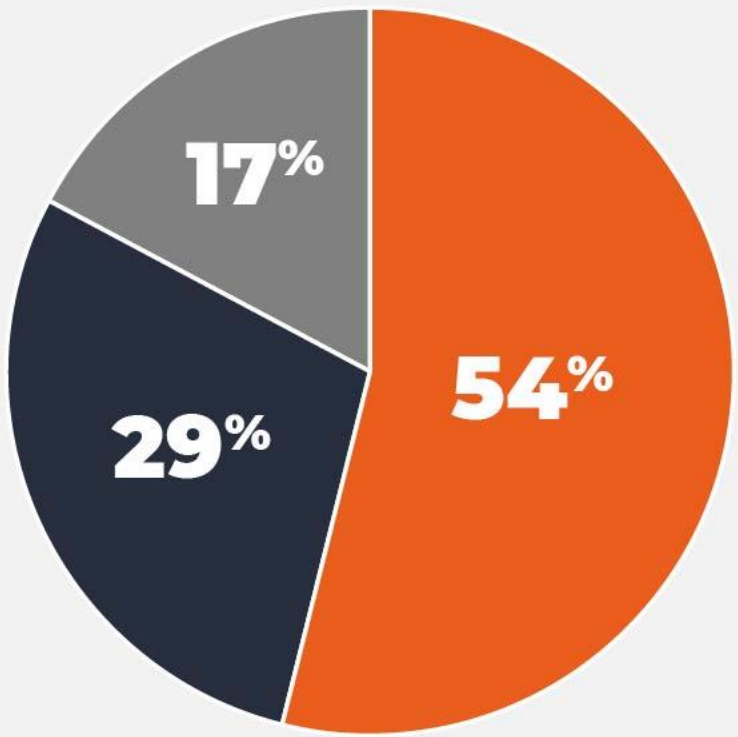
Полученные результаты

В исследовании приняли участие **52 специалиста,** отвечающих за управление службой информационной безопасности, в том числе:



Полученные результаты

В исследовании приняли участие **52 специалиста,** отвечающих за управление службой информационной безопасности, в том числе



- Небольшие компании по объему выручки (до 2 млрд рублей в год) — **28 анкет** (54%)
- Средние компании по объему выручки (от 2 до 10 млрд рублей в год) — **15 анкет** (29%)
- Крупные компании по объему выручки (более 10 млрд в год) — **9 анкет** (17%)

Полученные результаты

	Оценка	Цель	%
Управление ИБ	5.90	15	40%
Базовая ИТ- и ИБ-гигиена	6.85	15	46%
Обеспечение ИБ	4.33	15	29%
Мониторинг, реагирование и восстановление	5.94	15	40%
Комплаенс	6.69	15	45%

Управление ИБ

Средняя оценка 5,90 из 15 (40%)

Сценарии по оценке:

Планирование деятельности осуществляется в пределах 1 года

ИБ взаимодействует с ИТ и другими подразделениями по частным вопросам и в ходе стандартных процедур

Бюджет ИБ включает минимально необходимые позиции, финансирование происходит бессистемно

Найм персонала возможен по нижней границе рынка, кадровая турбулентность присутствует

Процедуры управления рисками ИБ проводятся формально. Результаты оценки рисков не влияют на основные решения бизнеса

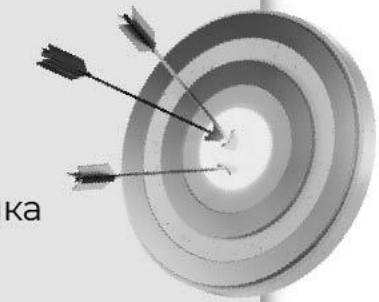
Комментарии:

Структурированное управление ИБ критически важно для защиты ресурсов организаций

На российском рынке наблюдается прогресс в построении процессов управления ИБ

Большинство российских компаний используют технологии изолированно от управления рисками и их интеграции в бизнес-процессы

Для улучшения ситуации необходим анализ и перестройка процессов ИБ



Базовые ИТ- и ИБ-гигиена

Средняя оценка 6.85 из 15 (46%)

Сценарии по оценке:

ИТ-активы управляются вручную в разрозненных таблицах, что ведет к ошибкам и требует бумажных документов для согласования

Наблюдение за ИТ-инфраструктурой осуществляется через наложенные средства и нативные утилиты, но данные разрознены

Обучение персонала нерегулярное, без оценки знаний и систематизации материалов

Для удаленной работы используются VPN + RDP с защитой паролем

Управление доступом основано на стандартной политике, но редко пересматривается

Комментарии:

Базовые ИТ- и ИБ-гигиена являются краеугольным камнем ИБ

Без учета актуальных угроз и обучения сотрудников, никакие средства защиты не обеспечат надежную безопасность

Средняя оценка по данному направлению указывает, что этим процессам уделяется внимание и выделяются ресурсы

Оценка на текущий момент ниже 50%, следовательно необходимо продолжать постоянное развитие направления

Обеспечение ИБ

Средняя оценка 4,33 из 15 (29%)

Сценарии по оценке:

Управление уязвимостями: базовое, с регулярным сканированием. Задачи на устранение через корпоративную почту

Сетевая безопасность: базовый набор средств *(антивирус, межсетевой экран, VPN, сканер уязвимостей)*, централизованное управление политиками

Защита информации: организационные и технические меры *(разграничение прав, классификация, контроль доступа)*

Безопасная разработка ПО: базовый уровень, без интеграции в жизненный цикл, только автотесты

Телеметрия и данные об угрозах: некоторые организации не используют фиды, другие применяют БДУ ФСТЭК, АСОИ ФинЦЕРТ, НКЦКИ

Комментарии:

Мероприятия по ИБ, включенные в направление, требуют значительных финансовых и ресурсных вложений

Такие мероприятия должны постоянно актуализироваться и анализироваться на предмет эффективности

Важность применения мер по харденингу ИТ-инфраструктуры, обеспечению РБПО и митигации рисков ИБ нельзя недооценивать

Реализация таких мероприятий способствует переходу к превентивному обеспечению ИБ, что позволяет предотвращать инциденты, а не только устранять их последствия

Мониторинг, реагирование и восстановление

Средняя оценка 5,94 из 15 (40%)

Сценарии по оценке:

Организация делает предварительный анализ инфраструктуры и постоянный мониторинг только в рабочее время через штатные инструменты

Критерии инцидентов ИБ не определены, реагирование происходит по прецедентам, а ролевая модель не формализована

Для реагирования на атаки применяется изоляция хостов на АВЗ

Процессы резервного копирования по срезу разнообразны: одни используют инкрементное ежедневное копирование штатными средствами, другие — агентские методы с еженедельным полным копированием и ежедневным инкрементным и применяя виртуализацию для восстановления

Роли и обязанности распределены фрагментарно, что затрудняет управление инцидентами ИБ, так как они решаются ситуативно ИТ-подразделениями

Комментарии:

Процессы мониторинга, реагирования и восстановления играют ключевую роль в управлении инцидентами информационной безопасности и минимизации их последствий

Отсутствие или некорректная организация этих процессов может привести к серьезным последствиям для бизнеса

Компании осознают важность этих задач и активно работают над их оптимизацией

Внедрение процессов должно быть комплексным и интегрированным в общий план обеспечения информационной безопасности, учитывающий приоритеты

Комплаенс

Средняя оценка 6,69 из 15 (45%)

Сценарии по оценке:

Многие организации формально соблюдают регуляторные требования, но не всегда эффективно защищают чувствительную информацию, что создает риски

Баланс между безопасностью и бизнес-процессами часто неидеален, вызывая напряжение между командами

Контроль в сфере ИБ фрагментарен, страдает от человеческого фактора, задержек и слабой масштабируемости

Практикуется привлечение внешних экспертов

Документооборот автоматизирован у некоторых, но бумажные визирования замедляют процессы. Другие компании полностью цифровизировали документооборот, ускоряя работу и снижая риски

Комментарии:

Регуляторные требования часто становятся главной мотивацией для организаций, сосредоточиваясь на «регуляторных рисках» вместо реальных угроз

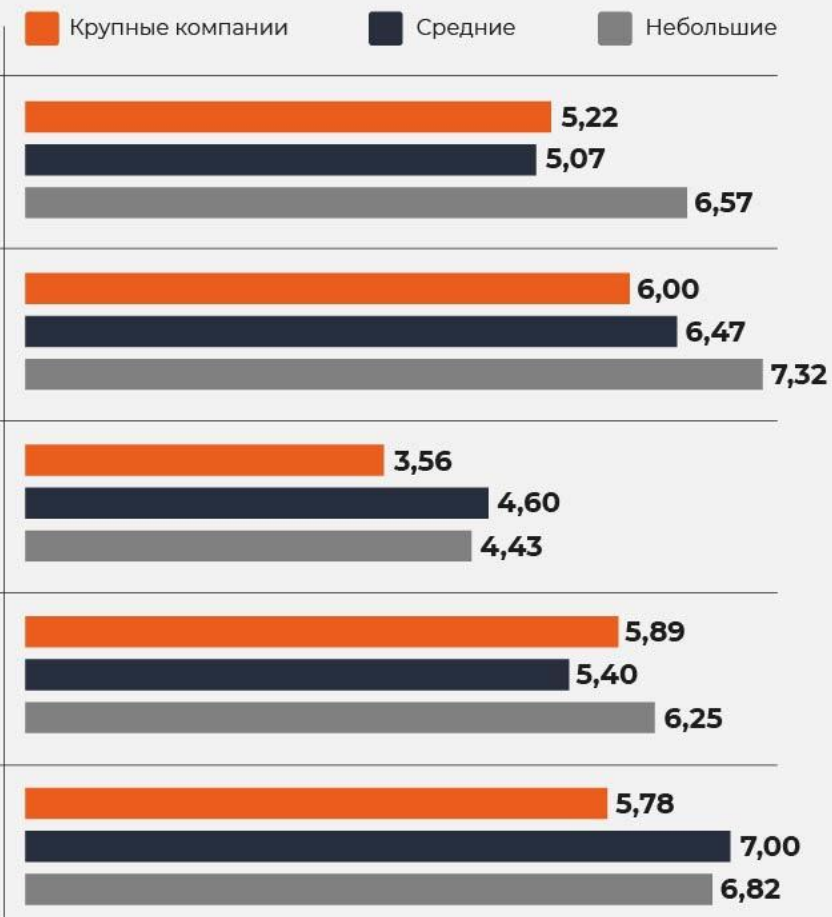
Выполнение требований регуляторов ниже 50%, с акцентом на штрафные и уголовные последствия

Формальное внедрение ИБ-инструментов неэффективно против современных угроз и создает иллюзию безопасности

Для эффективной защиты нужно учитывать как нормативные требования, так и реальные актуальные угрозы

Сравнительный анализ

Небольшие компании	Средние компании	Крупные компании	
6.57 (44%)	5.07 (34%)	5.22 (35%)	Направление I. «Управление ИБ»
7.32 (49%)	**6.47 (44%)**	**6 (40%)**	Направление II. «Базовая ИТ и ИБ гигиена»
4.43 (30%)	4.6 (31%)	3.56 (24%)	Направление III. «Обеспечение ИБ»
6.25 (42%)	5.4 (37%)	**5.89 (40%)**	Направление IV. «Мониторинг, реагирование и восстановление»
6.82 (46%)	**7 (47%)**	**5.78 (39%)**	Направление V. «Комплаенс»



Основные выводы

- Тенденции, выявленные на всем массиве данных, **актуальны и для каждой группы по отдельности.**
- Наличие больших ресурсов **не гарантирует высокий уровень зрелости ИБ.** Распределение имеющихся ресурсов всегда обусловлено потребностями основных бизнес-процессов, в то время как вопросы ИБ относятся к обеспечивающим.
- Дельта от малого к крупному бизнесу по направлениям «Управление ИБ» и «Обеспечение ИБ» (6-9%) обусловлена тем, что **обеспечить грамотное управление ИБ** в небольшой компании **проще и дешевле.** С ростом компании растет и составляющая бюрократизации процессов.
- Направление **с наивысшей оценкой** для всех организаций — **«Базовая ИТ и ИБ гигиена»**. Данное направление не требует существенного вливания бюджета и позволяет решать задачи собственными силами.
- **На втором месте** для небольших и средних компаний — **«Комплаенс»,** который является в некотором смысле «драйвером» для внедрения требований информационной безопасности и для обоснования выделения ресурсов и финансов на развитие функции ИБ.
- **Крупные компании фокусируются на «Мониторинге, реагировании и восстановлении».** Основные сложности для них связаны с большим объемом данных и масштабными системами, которые трудно контролировать.
- Различия в тех направлениях, которые получают наибольшую и наименьшую оценку уровня зрелости, для малых, средних и крупных компаний — это **следствие разных приоритетов бизнеса** и ресурсных ограничений.

Экспертные мнения

Все независимые эксперты подтвердили **релевантность полученных данных,** с допущением о несоответствии для крупнейших компаний.

Эксперты согласились, что **полученные выводы можно масштабировать на все отечественные компании.** Отметив, что выводы находятся не только в российском, но и общемировом тренде.

Какие **ключевые изменения необходимы** для повышения уровня зрелости информационной безопасности в разных областях:

- Со стороны государства в лице регуляторов необходим **баланс между реальными мерами и регуляторными требованиями,** желательно с учетом масштаба и значимости деятельности организации.
- Со стороны рынка ИБ важно **повысить доступность СЗИ,** а также идти по пути доработки отечественных решений, стремясь к международному качеству и продуктивности.
- Со стороны самих организаций требуется выстраивать **диалог с Бизнесом,** а также обратить особое внимание на грамотное выстраивание процессов ИБ.
- Не забывать про **рост роли AI-технологий:** необходимо учиться защищать AI-инфраструктуру, а также использовать технологии для противодействия атакам.
- Со стороны комьюнити специалистов по ИБ создавать больше площадок **с целью обмена информацией,** и выработки совместных решений по борьбе с киберугрозами.
- Важно, чтобы представители комьюнити помогали государству в определении **реалистичных и выполнимых требований,** а также работали с бизнесом, чтобы доносить ценность ИБ.

Рекомендации для ИБ-специалистов

1. **Выстраивайте диалог с Бизнесом:** Зрелость ИБ проявляется в том, что специалист по ИБ может выстроить диалог с бизнесом, подсветить все возможные варианты и риски для ТОПов. Такое взаимодействие дает возможность бизнесу и ИБ находить компромисс.
2. **Становитесь помогающей функцией:** Ресурсы компании всегда ограничены, поэтому распределяйте их в соответствии с потребностями основных бизнес-процессов. Функции ИБ должны поддерживать бизнес, а не мешать его развитию.
3. **Выстраивайте бизнес-процессы:** ИБ должно стать управленческим инструментом, обеспечивающим прозрачность, контролируемость и надёжность процессов. Без выстроенных бизнес-процессов ни один технологический стек не будет работать эффективно.
4. **Оптимизируйте процессы с ростом компании:** С ростом компании растет и бюрократизация процессов, что, в том числе, усложняет задачи ИБ. Следует регулярно пересматривать и оптимизировать процессы, чтобы сохранить эффективность.
5. **Используйте новые технологии:** Применение AI-технологий будет получать все большее распространение, в том числе и в направлении «Мониторинг, реагирование и восстановление».
6. **Не забывать о базовых мерах защиты:** Внедрение простых, но эффективных мер, таких как создание сложных паролей, регулярное резервное копирование и двухфакторная аутентификация, защищает от 80% кибератак и не требует значительных финансовых вложений.
7. **Используйте внешние ресурсы для крупных компаний:** Крупные компании могут привлекать внешние SOC и исполнителей для решения специфических вопросов ИБ. Это позволяет эффективно использовать сложные инструменты защиты данных, а также сократить затраты на ФОТ.

AKTIV.
CONSULTING

Аналитический отчет «Оценка уровня зрелости ИБ» 2026 г.

Варвара Шубина

Руководитель направления маркетинга AKTIV.CONSULTING

Пройти самоопросник по оценке уровня зрелости ИБ

AKTIV.CONSULTING

AKTIV.
CONSULTING

Мы
Самооценка уровня зрелости ИБ
Экспертиза
Консалтинг
Карьера
Общественные ИБ-проекты
Дискуссионный клуб
Подкаст «Безопасный выход»
Дегустационная консультация

Услуги
Руководителям ИБ

Пресс-центр
Новости

Находим самоопросник на сайте

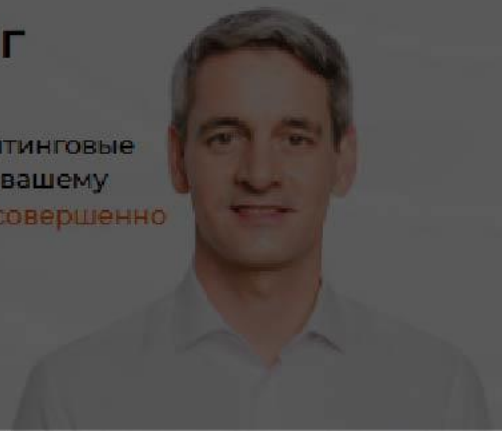
Дегустационная консультация

Руководителям службы ИБ

Управление функцией ИБ →
Обеспечение ИБ →
Соответствие требованиям ИБ →

Консалтинг

Специальные консалтинговые продукты обеспечат вашему бизнесу переход на совершенно новый уровень



Самооценка уровня зрелости ИБ

Мы разработали простой инструмент для самооценки уровня зрелости ИБ, заполните самоопросник и получите представление о текущем уровне зрелости и рекомендации по дальнейшему развитию функции ИБ.

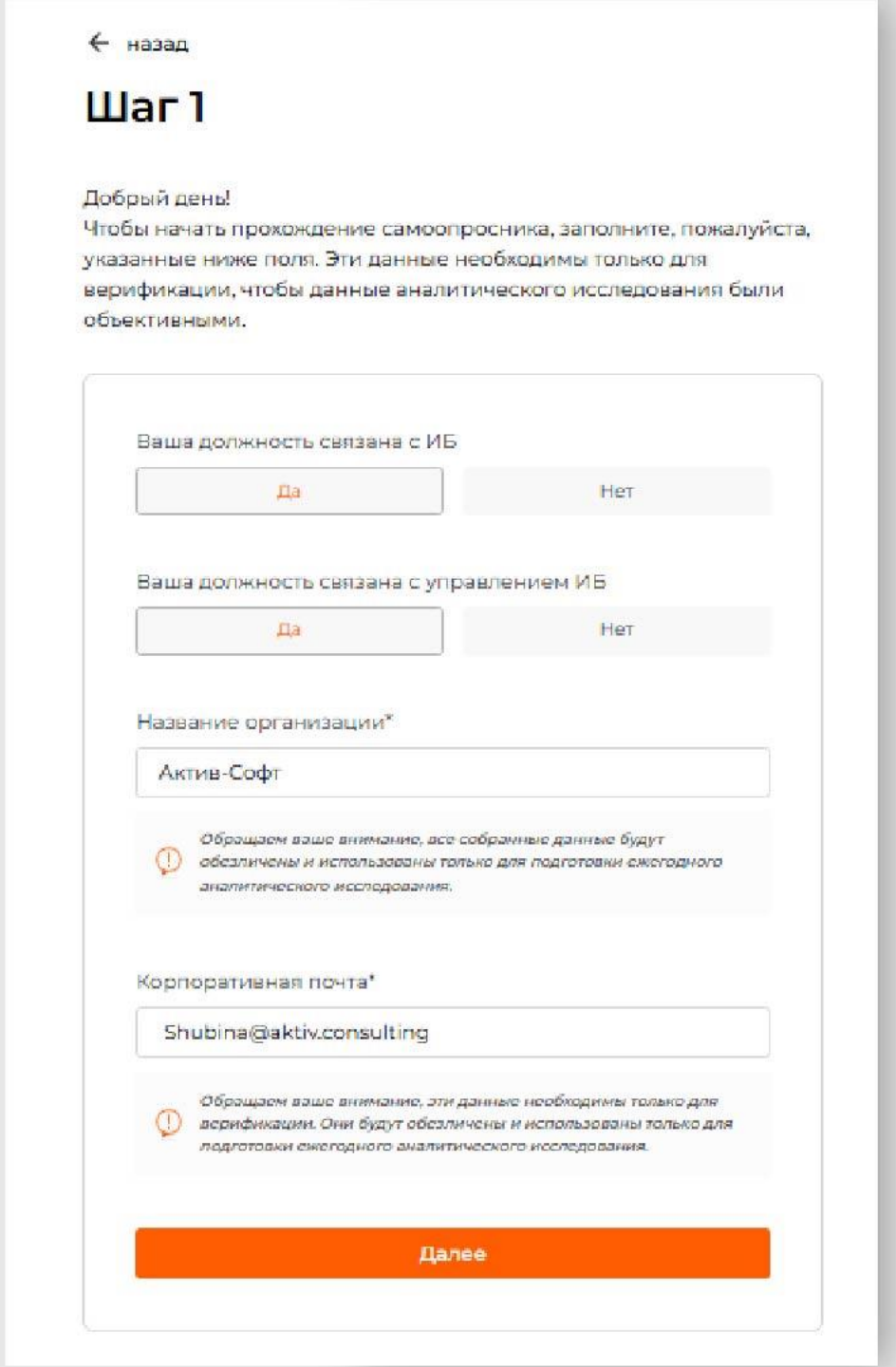
Перейти к опросу

Находим самоопросник на сайте

Актуальность

Одним из ключевых шагов к качественному развитию системы управления и обеспечения информационной безопасности является проведение регулярной оценки уровня зрелости ИБ.

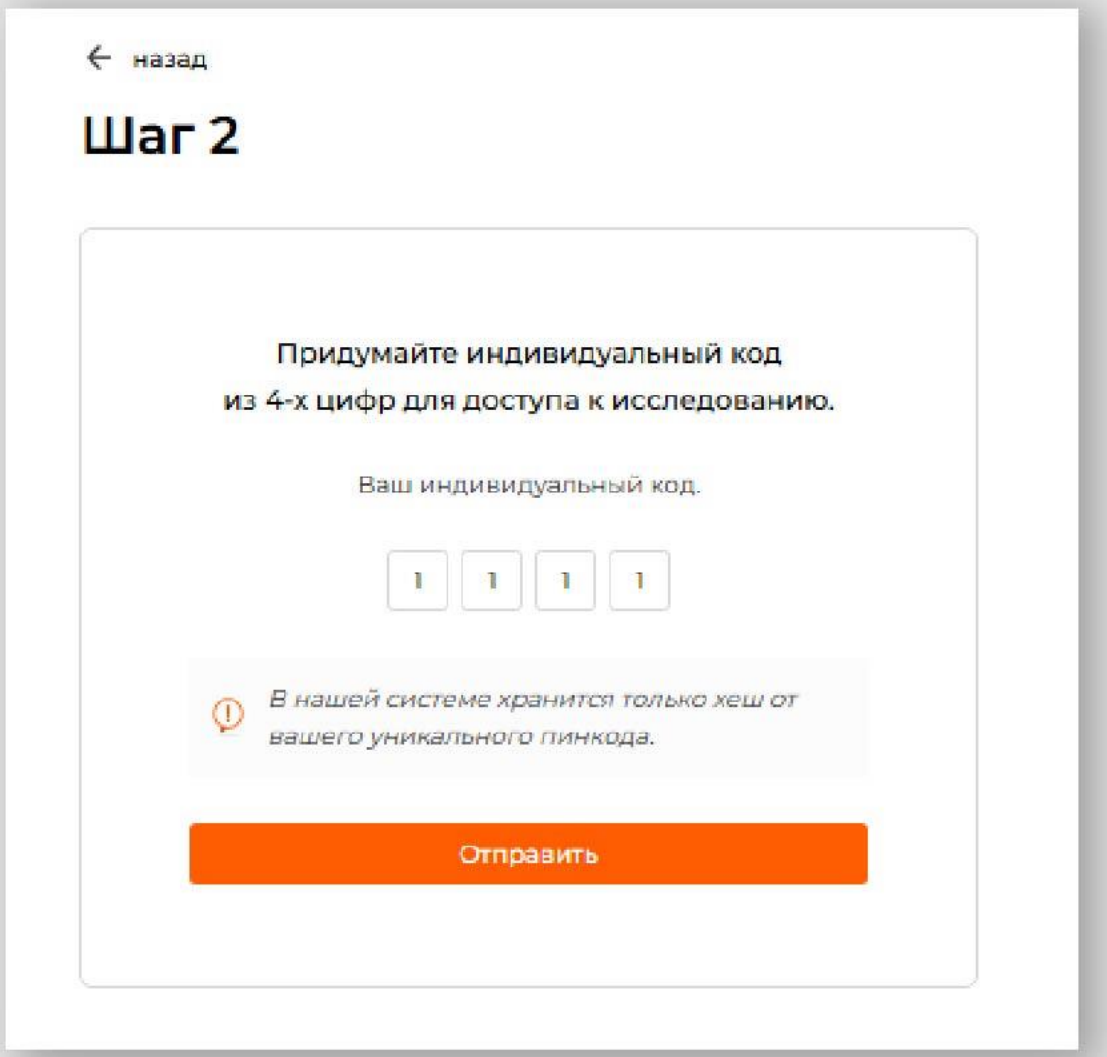
Получение объективной оценки уровня зрелости функции ИБ становится основой для краткосрочного и долгосрочного планирования ее развития в организации. В своей работе мы сталкиваемся с тем, что не все компании имеют возможности обратиться за экспертной оценкой, поэтому опираясь на свой опыт и лучшие мировые практики, мы разработали простой инструмент для самооценки уровня зрелости ИБ.



Шаг 1

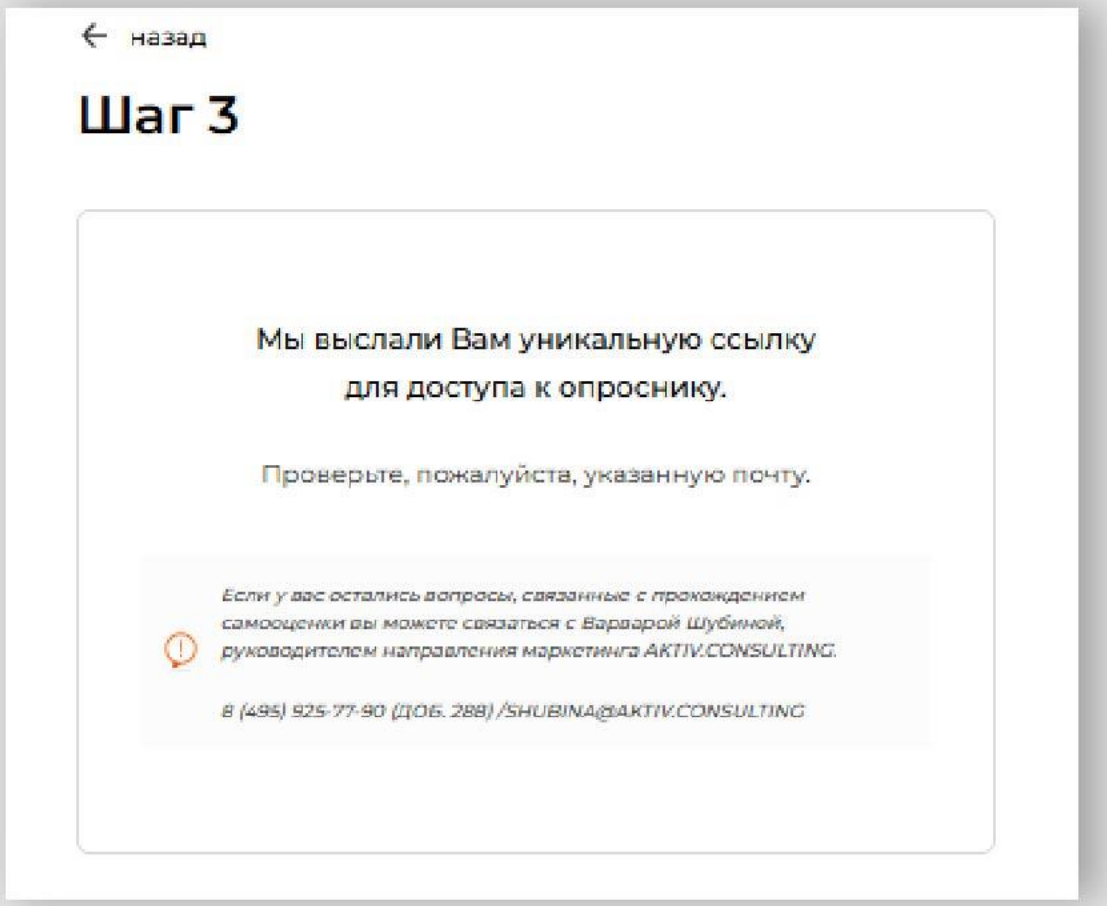
Верификация

AKTIV.CONSULTING



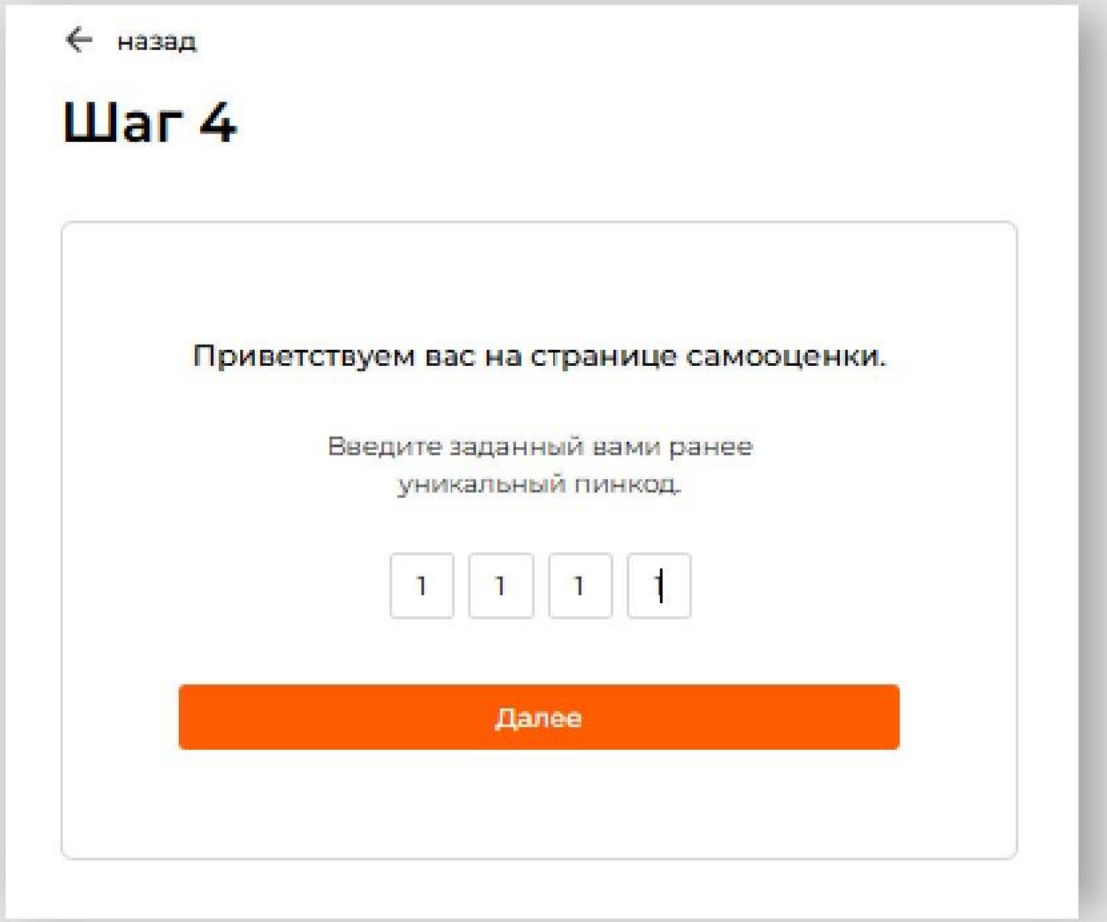
Шаг 2

Уникальный пинкод



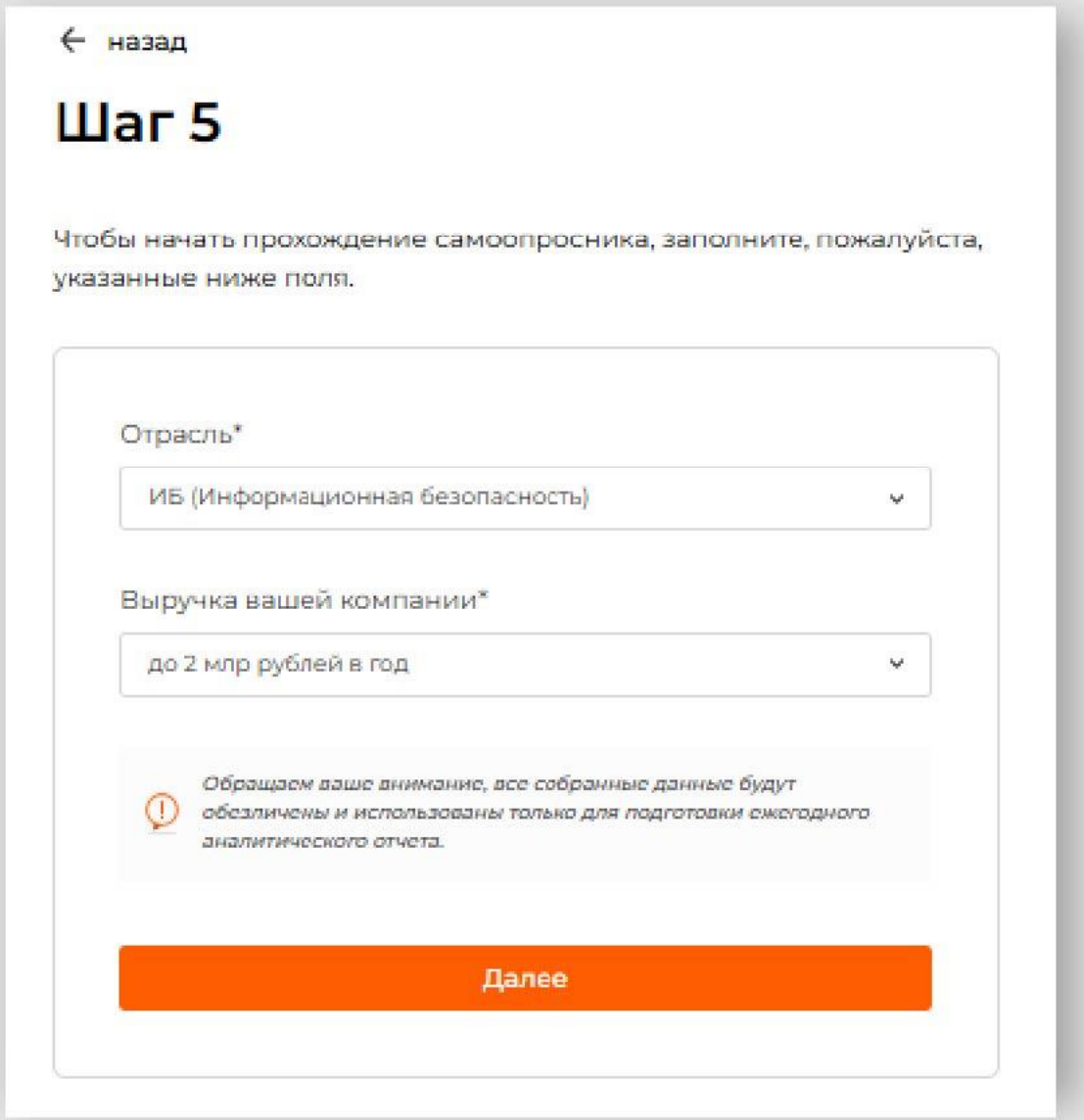
Шаг 3

Уникальная ссылка



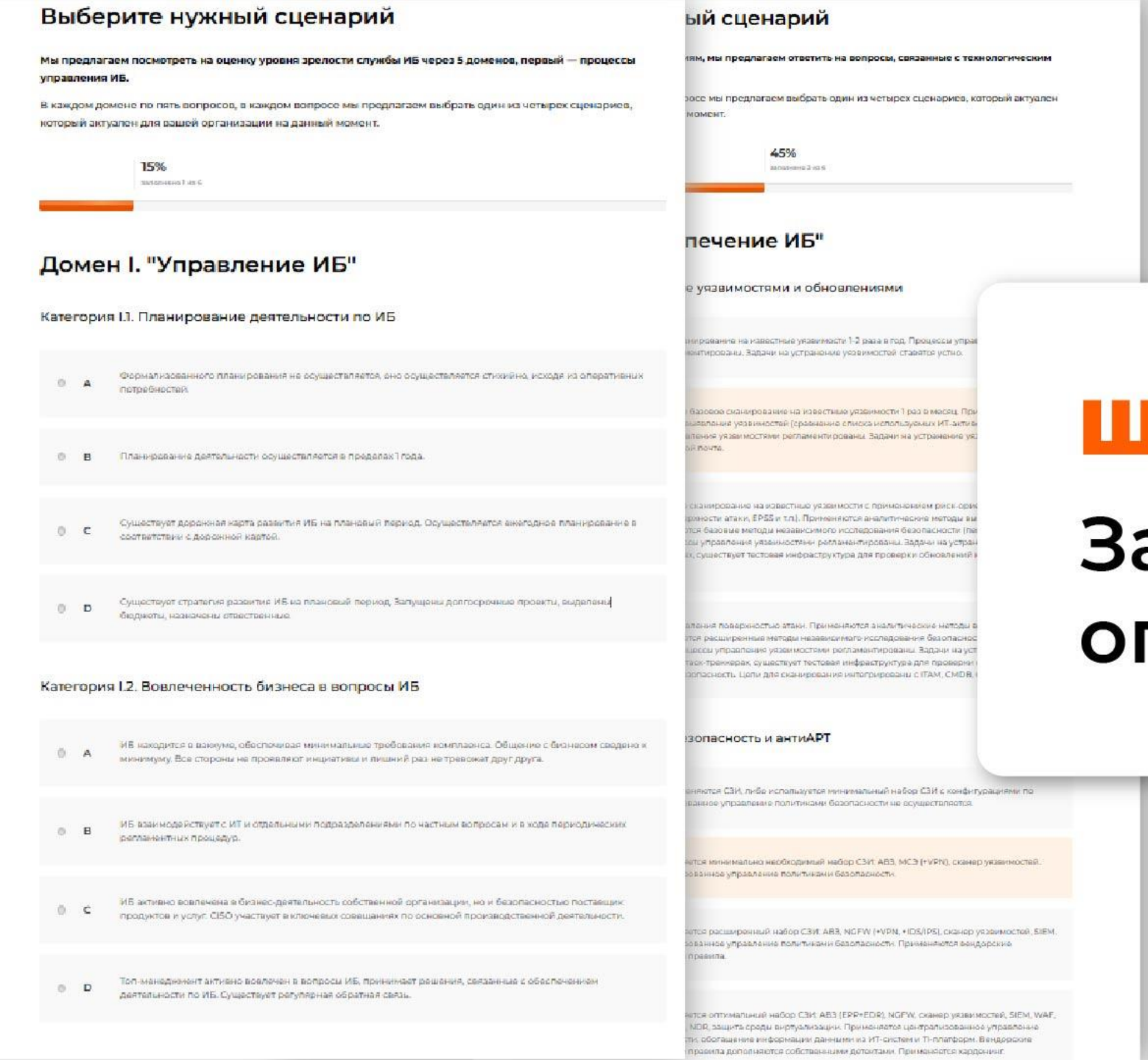
Шаг 4

Переход к самооценке



Шаг 5

Отрасль и размер компании



Выберите нужный сценарий

Мы предлагаем посмотреть на оценку уровня зрелости службы ИБ через 5 доменов, первый — процессы управления ИБ.

В каждом домене по пять вопросов, в каждом вопросе мы предлагаем выбрать один из четырех сценариев, который актуален для вашей организации на данный момент.

15%

Домен I. "Управление ИБ"

Категория I.1. Планирование деятельности по ИБ

A — Формализованного планирования не осуществляется, оно осуществляется стихийно, исходя из оперативных потребностей.

B — Планирование деятельности осуществляется в пределах 1 года.

C — Существует дорожная карта развития ИБ на плановый период. Осуществляется ежегодное планирование в соответствии с дорожной картой.

D — Существует стратегия развития ИБ на плановый период. Запущены долгосрочные проекты, выделены бюджеты, назначены ответственные.

Категория I.2. Вовлеченность бизнеса в вопросы ИБ

A — ИБ находится в вакууме, обеспечивая минимальные требования комплаенса. Общение с бизнесом сведено к минимуму. Все стороны не проявляют инициативы и лишний раз не тревожат друг друга.

B — ИБ взаимодействует с ИТ и отдельными подразделениями по частным вопросам и в ходе периодических регламентных процедур.

C — ИБ активно вовлечена в бизнес-деятельность собственной организации, но и безопасностью поставщик продуктов и услуг. CISO участвует в ключевых совещаниях по основной производственной деятельности.

D — Топ-менеджмент активно вовлечен в вопросы ИБ, принимает решения, связанные с обеспечением деятельности по ИБ. Существует регулярная обратная связь.

ый сценарий

45%

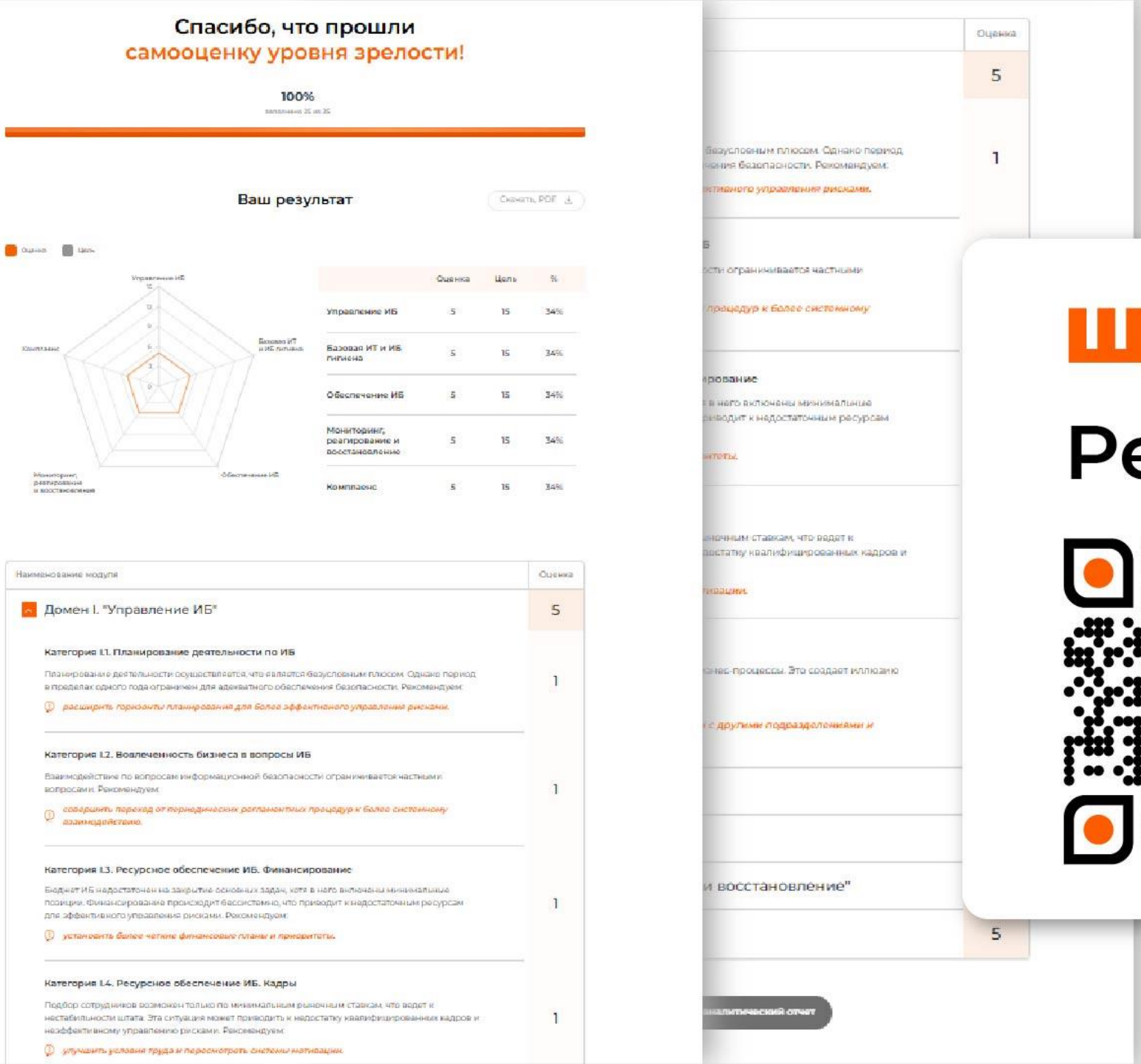
печение ИБ"

е уязвимостями и обновлениями

зопасность и антиAPT

Шаг 6

Заполняем опросник


Спасибо, что прошли
самооценку уровня зрелости!
100%
Ваш результат
Скачать PDF
Оценка
Цель
Управление ИБ
Базовая ИТ и ИБ гигиена
Обеспечение ИБ
Мониторинг, реагирование и восстановление
Комплаенс
Оценка
Цель
%
Управление ИБ 5 15 34%
Базовая ИТ и ИБ гигиена 5 15 34%
Обеспечение ИБ 5 15 34%
Мониторинг, реагирование и восстановление 5 15 34%
Комплаенс 5 15 34%
Наименование модуля
Оценка
Домен I. "Управление ИБ"
5
Категория I.1. Планирование деятельности по ИБ
Планирование деятельности осуществляется, что является безусловным плюсом. Однако период в пределах одного года ограничен для адекватного обеспечения безопасности. Рекомендуем:
расширить горизонты планирования для более эффективного управления рисками.
1
Категория I.2. Вовлеченность бизнеса в вопросы ИБ
Взаимодействие по вопросам информационной безопасности ограничивается частными вопросами. Рекомендуем:
совершить переход от периодических регламентных процедур к более системному взаимодействию.
1
Категория I.3. Ресурсное обеспечение ИБ. Финансирование
Бюджет ИБ недостаточен на закрытие основных задач, хотя в него включены минимальные позиции. Финансирование происходит бессистемно, что приводит к недостаточным ресурсам для эффективного управления рисками. Рекомендуем:
установить более четкие финансовые планы и приоритеты.
1
Категория I.4. Ресурсное обеспечение ИБ. Кадры
Подбор сотрудников возможен только по минимальным рыночным ставкам, что ведет к нестабильности штата. Эта ситуация может приводить к недостатку квалифицированных кадров и неэффективному управлению рисками. Рекомендуем:
улучшить условия труда и пересмотреть системы мотивации.
1
Оценка
5
1
5
Шаг 7
Результаты
AKTIV.CONSULTING

ВОПРОС-
ОТВЕТ




AKTIV.
CONSULTING

БЛАГОДАРИМ
ЗА ВНИМАНИЕ!