SOLAR | Технологии Доверия

Кибербезопасность как конкурентное преимущество

ИССЛЕДОВАНИЕ

МОСКВА, 2025

Содержание

Об исследовании

SOLAR | Технологии Доверия

SOLAR

Технологии Доверия

Цель исследования — анализ актуальных вопросов, связанных с ролью кибербезопасности в крупных компаниях, ее влиянием на конкурентное преимущество, комплексным подходом к обеспечению информационной безопасности (далее – ИБ), а также перспективными направлениями развития. Исследование проводилось среди руководителей функции ИБ крупных компаний РФ

Май
2025

13
вопросов

10
компаний

УЧАСТНИКИ ИССЛЕДОВАНИЯ – 10 КРУПНЕЙШИХ КОМПАНИЙ ИЗ СЛЕДУЮЩИХ ОТРАСЛЕЙ:

- Розничная торговля
- Технологический сектор
- Телекоммуникации
- Финансовый сектор
- Промышленность

В рамках исследования обсуждались следующие области:

- Управление ИБ
- Вовлеченность бизнеса в вопросы ИБ
- Специфика развития ИБ в крупных организациях
- Тенденции развития ИБ
- Практические аспекты оценки эффективности ИБ

Вовлеченность руководства и стратегическое планирование ИБ

Бизнес все глубже интегрируется в вопросы ИБ, рассматривая ее как неотъемлемую часть стратегического управления и операционной деятельности.

Компании с высокой скоростью внутренних изменений на тактическом уровне дополнительно осуществляют контроль реализации стратегических инициатив ИБ каждые 3-6 месяцев.

На фоне роста киберугроз способность компаний демонстрировать свою устойчивость существенно укрепляет репутацию на рынке, в связи с чем топ-менеджмент воспринимает ИБ уже как конкурентное преимущество, а не затратную статью.

> Кибербезопасность становится приоритетом, особенно с учетом специфики бизнеса, если мы не будем обладать свойством киберустойчивости, весь наш бизнес будет под вопросом

100%

Респондентов имеют согласованные с топ-менеджментом стратегические планы развития ИБ

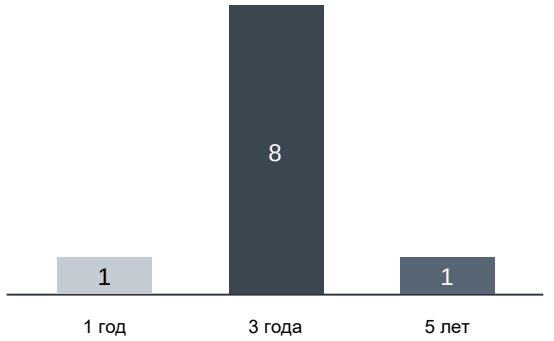
90%

ЕЖЕГОДНАЯ ЧАСТОТА ПЕРЕСМОТРА

9 из 10 участников исследования пересматривают стратегические планы развития ИБ на ежегодной основе

ЗА ПОСЛЕДНИЕ 5 ЛЕТ ГОРИЗОНТ ПЛАНИРОВАНИЯ В ОБЛАСТИ ИБ СОКРАТИЛСЯ С 5 ДО 3 ЛЕТ У БОЛЬШИНСТВА КОМПАНИЙ

Горизонт планирования ИБ



Индикаторы увеличения вовлеченности:

- ИБ чаще интегрируется в бизнес-стратегии
- Усиливается контроль митигации рисков ИБ
- Расширение практики мониторинга КПЭ в области ИБ
- Рост запросов на практическую кибербезопасность

100% Респондентов отметили, что вовлеченность топ-менеджмента в вопросы ИБ увеличилась за последние 3 года

> Переход к среднесрочному горизонту планирования необходим, т. к. мир слишком изменчив: меняется стек технологий, ландшафт угроз, экономическая обстановка

Ключевые бизнес-запросы и метрики на контроле руководства

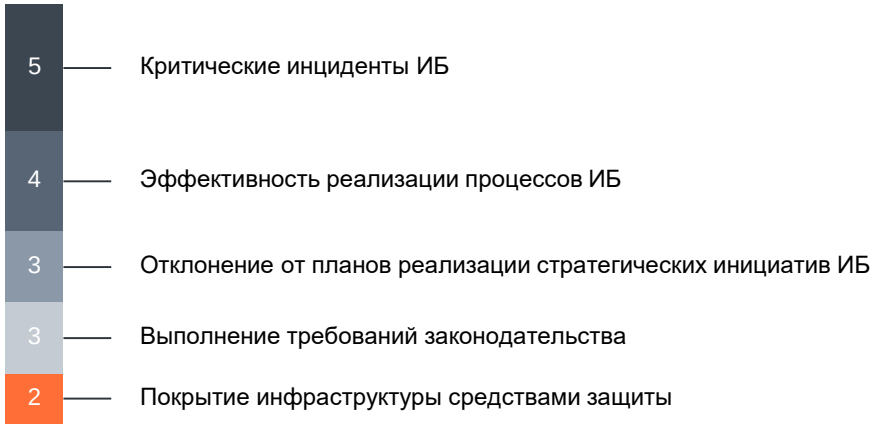
За последние 3 года запросы к ИБ со стороны бизнеса стали больше сфокусированы на обеспечении практической безопасности. Большинство респондентов отметили, что отсутствие инцидентов ИБ является одним из ключевых требований к функции ИБ в их компаниях, в дополнение к обеспечению соответствия требованиям законодательства РФ, выделяя, в частности, обеспечение безопасности ПДн. Также немаловажным аспектом является подконтрольность и управляемость ИБ, то есть повышение прозрачности функции ИБ как в части финансовых затрат, так и в части операционной деятельности и зон ответственности.

Контроль метрик ИБ бизнесом | **80%** | У 8 из 10 участников исследования метрики ИБ находятся на контроле топ-менеджеров

Наблюдается устойчивая тенденция к внедрению практики регулярного контроля метрик и ключевых показателей эффективности обеспечения ИБ топ-менеджментом компаний, что подтверждает рост вовлеченности бизнеса в вопросы ИБ

Ключевые требования бизнеса к ИБ в 2025 г.

Ключевые метрики ИБ на контроле руководства



> Обоснованные потребности ИБ становятся поручениями топ-менеджмента, за исполнением которых осуществляется контроль (не только в рамках формальной отчетности)

Подходы к формированию и выбору метрик обусловлены спецификой бизнеса. Вместе с тем одним из наиболее часто встречаемых КПЭ является отсутствие инцидентов ИБ и отслеживание эффективности реализации процессов, что коррелирует с ключевыми ожиданиями и запросами бизнеса к функции ИБ. Эффективность работы процессов, своевременная реализация стратегических инициатив ИБ, комплаенс, а также покрытие инфраструктуры средствами защиты включены в зону повышенного внимания руководства компаний

Подход к управлению ИБ в ДЗО

Участники исследования отмечают, что выбор подхода зависит в том числе от специфики бизнеса, ИТ-инфраструктуры, размеров и количества ДЗО.

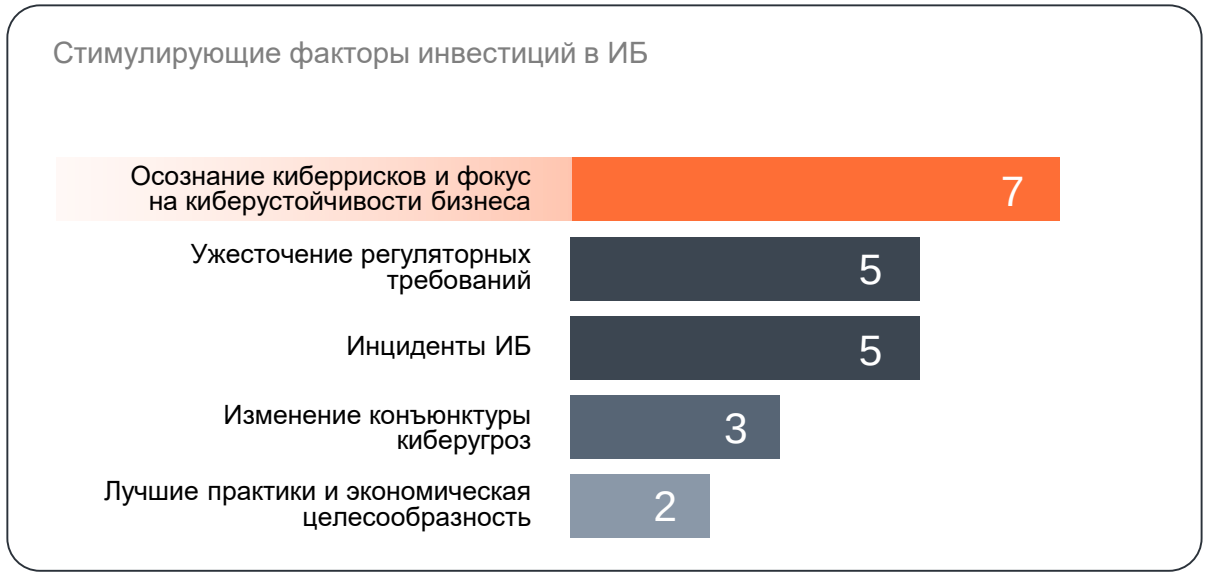
Самым распространенным можно считать комбинированный подход, стремящийся к централизованному, при котором в крупных ДЗО функционирует локальная команда, поддерживающая специфичные СЗИ и процессы ИБ в дополнение к централизованным сервисам, под контролем функции ИБ головной компании.

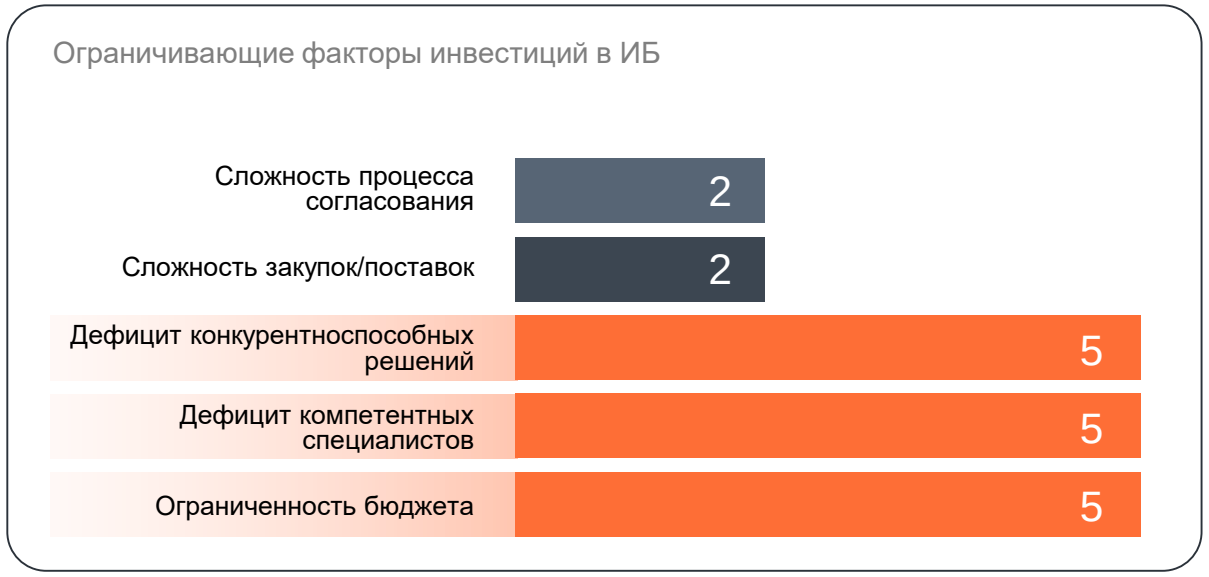
В качестве хорошей практики респондентами отмечается внедрение в ДЗО и бизнес-блоках роли ИБ-бизнес-партнера.

> Комбинированный подход позволяет иметь исполнителей на местах, при этом сохранять управляемость, унификацию, возможность замещения и прогнозирования

Инвестиции в ИБ: стимулы и ограничения

SOLAR | Технологии Доверия





Ключевым изменением за последние 3 года в контексте факторов, стимулирующих инвестирование в ИБ, является не только ужесточение регуляторных требований в области ИБ, но и сближение ИБ с бизнесом, выраженное в понимании зависимости успеха бизнеса от обеспечения кибербезопасности.

Рост количества инцидентов ИБ, повышение сложности кибератак, увеличение ландшафта киберугроз в силу цифровой трансформации крупных предприятий дополнительно мотивирует компании инвестировать в киберустойчивость.

Среди ограничивающих инвестирование в ИБ факторов за последние 3 года одним из наиболее распространенных является ограниченность бюджетов на ИБ, однако наблюдаются изменения в сторону их увеличения. Планомерное и последовательное развитие ИБ позволяет обеспечивать высокий уровень ИБ в организациях без лавинообразных скачков бюджета.

> Ситуация улучшилась, но российские решения на сегодняшний день все еще недостаточно зрелые, по сравнению с решениями, которые мы использовали ранее

! УЧАСТНИКИ ОТМЕЧАЮТ ДЕФИЦИТ КОМПЕТЕНТНЫХ СПЕЦИАЛИСТОВ И ЗРЕЛЫХ РЕШЕНИЙ В ОБЛАСТИ ИБ. НА ПРАКТИКЕ ДАЖЕ ПРИ НАЛИЧИИ БОЛЬШОГО БЮДЖЕТА ДАННЫЕ ФАКТОРЫ МОГУТ НЕ ПОЗВОЛИТЬ ДОСТИЧЬ ЦЕЛЕВОГО СОСТОЯНИЯ ОБЕСПЕЧЕНИЯ ИБ В ЖЕЛАЕМЫЕ СРОКИ, ПО МНЕНИЮ РЕСПОНДЕНТОВ

Драйверы и ограничители реализации комплексных проектов

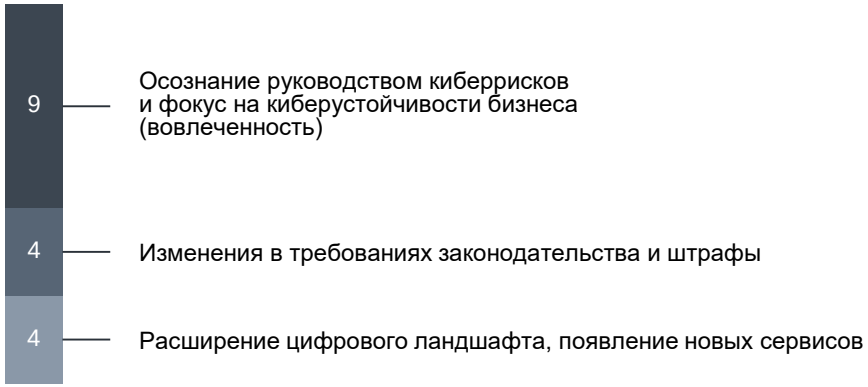
Респонденты указывают, что существует широкий спектр предпосылок к внедрению комплексных проектов в области ИБ. Эти предпосылки обусловлены спецификой деятельности и уникальными особенностями каждой компании, включая ее структуру, отраслевую принадлежность, масштабы и уровень зрелости ИТ-инфраструктуры. При этом ключевым драйвером является стремление компаний обеспечить киберустойчивость.

Масштабные изменения в ИТ-инфраструктуре и требованиях законодательства также приводят к потребности в модернизации обеспечения ИБ.

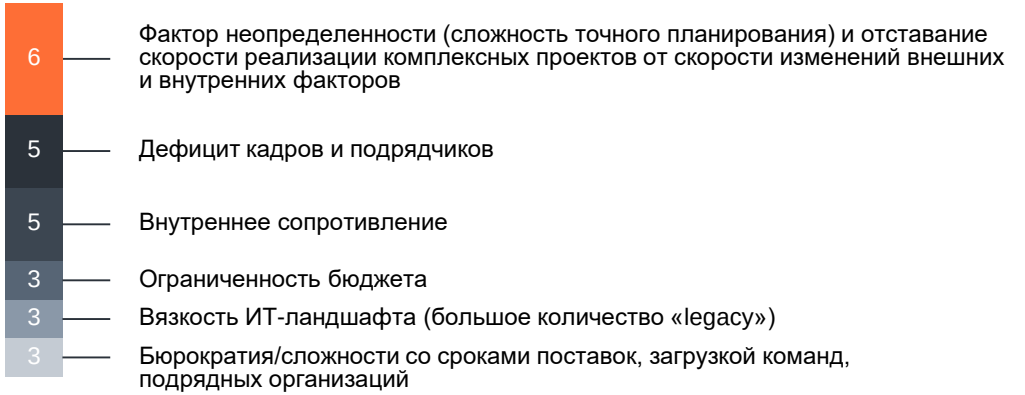
! ОСНОВНЫМ КРИТЕРИЕМ ПРИ ВЫБОРЕ ПОДРЯДЧИКА У БОЛЬШИНСТВА РЕСПОНДЕНТОВ ЯВЛЯЕТСЯ ЕГО КОМПЕТЕНТНОСТЬ, А ТАКЖЕ ПРАКТИЧЕСКОЕ СООТВЕТСТВИЕ ЗАЯВЛЕННОМУ ФУНКЦИОНАЛУ В РАМКАХ ПОСТАВЛЯЕМЫХ УСЛУГ

> Риск-ориентированный подход (обоснованность принятия решений), требует от CISO умения «видеть глазами бизнеса». Необходимо мыслить шире – следить на развитием компании и подходить к ней с точки зрения компании, а не процессов

Драйверы внедрения комплексных проектов



Барьеры при внедрении комплексных проектов

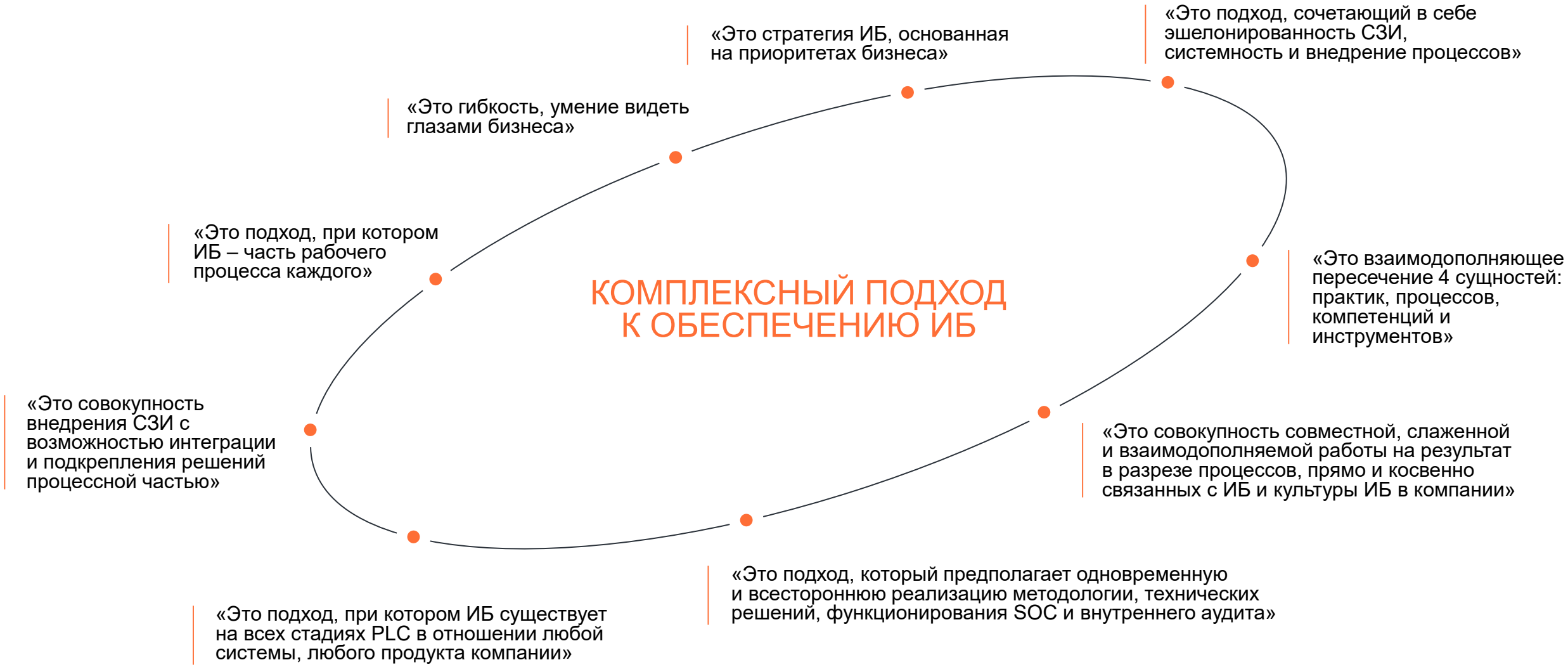


Комплексный подход к обеспечению ИБ

SOLAR | Технологии Доверия

!

В СИЛУ РАЗЛИЧИЙ В ОПЫТЕ РУКОВОДИТЕЛЕЙ ИБ И СПЕЦИФИКИ ИХ БИЗНЕСА, ПОНИМАНИЕ КОМПЛЕКСНОГО ПОДХОДА К ОБЕСПЕЧЕНИЮ ИБ СУЩЕСТВЕННО ВАРЬИРУЕТСЯ:



«Это стратегия ИБ, основанная на приоритетах бизнеса»

«Это подход, сочетающий в себе эшелонированность СЗИ, системность и внедрение процессов»

«Это гибкость, умение видеть глазами бизнеса»

«Это подход, при котором ИБ – часть рабочего процесса каждого»

«Это взаимодополняющее пересечение 4 сущностей: практик, процессов, компетенций и инструментов»

«Это совокупность внедрения СЗИ с возможностью интеграции и подкрепления решений процессной частью»

«Это совокупность совместной, слаженной и взаимодополняемой работы на результат в разрезе процессов, прямо и косвенно связанных с ИБ и культуры ИБ в компании»

«Это подход, который предполагает одновременную и всестороннюю реализацию методологии, технических решений, функционирования SOC и внутреннего аудита»

«Это подход, при котором ИБ существует на всех стадиях PLC в отношении любой системы, любого продукта компании»

Процессы: критичность и ресурсоемкость

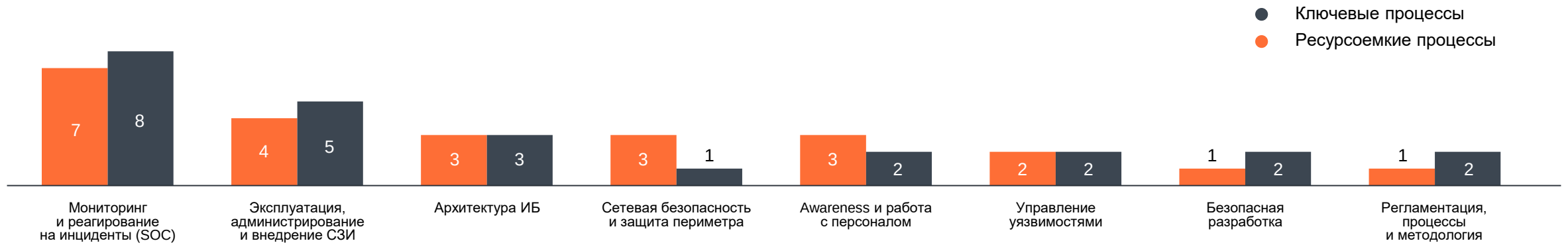
Участниками исследования отмечается, что процесс «Мониторинг и реагирование на инциденты ИБ» наряду с процессом «Эксплуатация и администрирование СЗИ» являются одновременно как наиболее критичными, так и требующими наибольшего объема человеческих ресурсов функции ИБ.

Особое внимание также уделяется процессам «Архитектура ИБ», «Управление уязвимостями» и «Обеспечение сетевой безопасности и защиты периметра», что подтверждает фокус компаний на «реальной безопасности».

ВОПРОС РАЗВИТИЯ ОСВЕДОМЛЕННОСТИ ПЕРСОНАЛА В ОБЛАСТИ ИБ ТАКЖЕ СТОИТ НА ПОВЕСТКЕ В КРУПНЫХ КОМПАНИЯХ, Т. К. ФОРМИРУЕТ КУЛЬТУРУ ИБ И СНИЖАЕТ РИСКИ, СВЯЗАННЫЕ С ЧЕЛОВЕЧЕСКИМ ФАКТОРОМ

> Культура ИБ (сознание, внутренние убеждения) – это элемент корпоративной культуры, когда работники всех уровней знают и помнят про ИБ. Важны не только СЗИ и процессы ИБ, но и культура ИБ как часть рабочего процесса каждого

Топ ключевых и ресурсоемких процессов ИБ



Также среди ключевых процессов ИБ участники исследования называли:

- Управление доступом
- Управление проектами ИБ
- Управление изменениями
- Управление активами
- Управление рисками
- Резервное копирование и восстановление
- Харденинг
- Коммуникация с руководством
- Проработка и выполнение требований по ИБ к инфраструктуре
- Обеспечение ИБ в рамках PLC

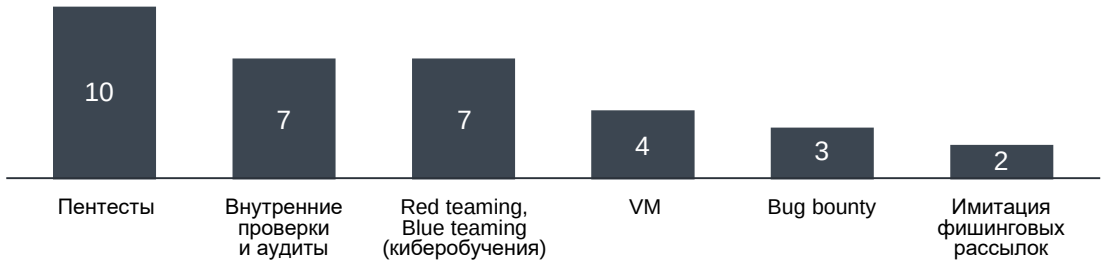
Практическая оценка эффективности ИБ

«Лучшая проверка любой реализованной меры – моделирование действий реального злоумышленника»

«Регулярные попытки атак поддерживают высокий уровень подготовленности»

Большинство респондентов оценивают размер материального ущерба от реализации критичных инцидентов ИБ, при этом оценка осуществляется как с помощью моделирования, так и ретроспективно (использование совокупности данных мер также присутствует).

Распространенные практики проверки эффективности ИБ



Процедура оценки ущерба | 70% | 7 из 10 участников исследования имеют процедуру оценки материального ущерба в случае наступления инцидента ИБ

> Культура качественного подсчета простоев, а также косвенных затрат мало распространена. Зачастую все сводится к подсчету стоимости затрат на восстановление, например через ФОТ и объем штрафов

Практическая оценка эффективности обеспечения ИБ обозначается участниками исследования как базовая потребность в условиях запроса бизнеса на «реальную безопасность» и отсутствие инцидентов ИБ. Участники отмечают разнообразие применяемых инструментов и подходов к оценке эффективности ИБ, что обусловлено как зрелостью процессов, так и доступностью ресурсов. Наиболее распространенными методами оценки эффективности среди участников являются: тестирование на проникновение (в том числе CPT), Red teaming (включая киберучения), анализ уязвимостей, а также внутренние проверки и аудиты.

Респонденты, использующие в качестве оценки эффективности Bug bounty, отмечают его высокую ценность. Ряд участников имеют планы по внедрению практики использования Bug bounty в ближайшем будущем.

Формат оценки материального ущерба в случае наступления инцидента ИБ

- Путем моделирования и в случае возникновения (ретроспективно)
- Путем моделирования
- В случае возникновения (ретроспективно)

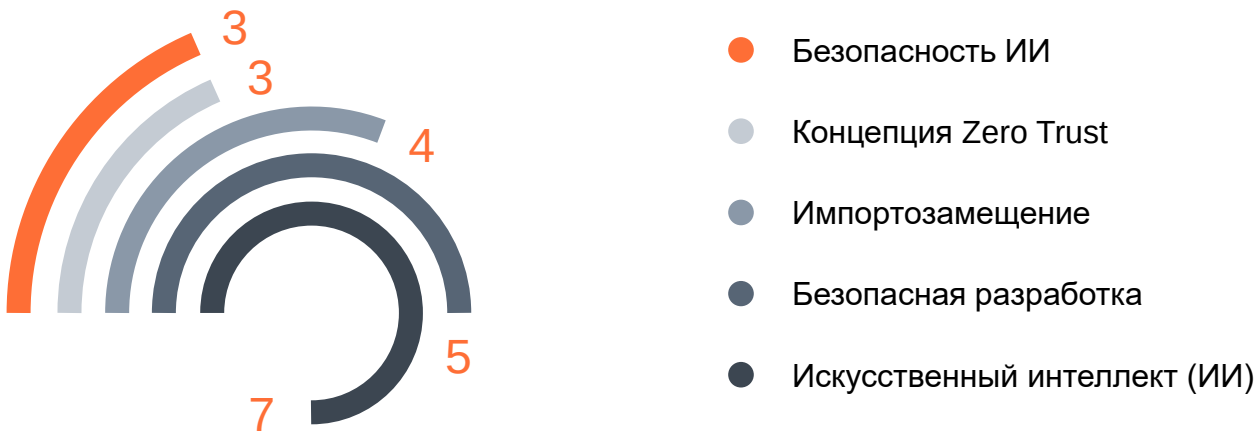
Приоритетные направления развития и тренды ИБ

100% Участников исследования видят тенденцию роста использования ИИ в ИБ

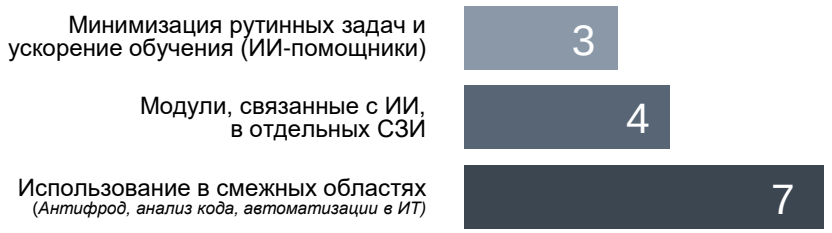
> Есть ожидание, что ИИ начнет применяться более широко в продуктах ИБ в ближайшем будущем

> Присутствует настороженность относительно использования ИИ в боевых процессах ИБ

Приоритетные области на ближайшие 3-5 лет



Основные области использования ИИ в ИБ



Большинство участников исследования полагают, что повышенное внимание будет уделяться в ближайшие годы технологиям, связанным с ИИ. Грамотная интеграция возможностей ИИ в процессы и решения ИБ, как и обеспечение его безопасности, способна стать конкурентным преимуществом и повлиять на киберустойчивость компаний.

Некоторые респонденты при этом все же испытывают недоверие и скептицизм по отношению к данным технологиям.

Актуальным направлением для приложения ресурсов также респонденты считают технологии DevSecOps, так как крупные компании практикуют внутреннюю разработку в большом объеме, что, в свою очередь, требует повышенного внимания к обеспечению безопасности разрабатываемых продуктов.

В качестве актуального направления респонденты также отмечают импортозамещение, которое сопряжено с определенными сложностями, но при этом является новой реальностью, а также регуляторной необходимостью.

Среди прочих актуальных направлений респонденты выделяют концепцию Zero Trust и безопасность ИИ.

Выводы

ПРО ВОВЛЕЧЕНИЕ БИЗНЕСА

Компании в 2025 г. решают стратегическую задачу по синхронизации ИБ и бизнеса, т. к. киберустойчивость становится важным элементом бизнес-ценности и рыночного доверия.

Усиление вовлеченности топ-менеджмента в вопросы ИБ обусловлено необходимостью получения целостного представления о состоянии ИБ для принятия обоснованных решений, направленных на оптимизацию стратегий развития, а также ужесточением законодательства РФ, связанного с ИБ.

ПРО ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ИБ

Искусственный интеллект в ИБ сегодня является как минимум областью повышенного внимания, а как максимум объектом ожиданий технологического прорыва в части противодействия кибератакам и оптимизации рутинных задач специалистов ИБ.

Живой интерес, а также стремление к инновациям в крупных компаниях позволяют ожидать значительного роста применения ИИ в области ИБ. Формирование объективной оценки роли ИИ в кибербезопасности станет возможным на основе накопленного практического опыта и реальных кейсов применения в ближайшие несколько лет.

ПРО ИБ КАК КОНКУРЕНТНОЕ ПРЕИМУЩЕСТВО

Современный подход к обеспечению ИБ строится на принципах комплексности, экономической целесообразности и стратегической значимости, что позволяет интегрировать ИБ в бизнес-процессы и рассматривать ее как источник конкурентных преимуществ, а не только как затратную статью бюджета. Компании, инвестирующие в кибербезопасность, позиционируются как более зрелые и надежные.

SOLAR

+7 (499) 755-07-70
info@rt-solar.ru

Центральный офис.
125009, Москва,
Никитский переулок, 7с1