JET SECURITY TEAM

ИССЛЕДОВАНИЕ

КУРС НА КИБЕР-УСТОЙЧИВОСТЬ: КАК ИЗМЕНИЛИСЬ СТРАТЕГИИ CISO

Инфосистемы Джет
JET.SU

АВТОРЫ

АЛЕКСАНДР МОРКОВЧИН

Руководитель группы аналитики и исследований департамента консалтинга, «Инфосистемы Джет»

ЕЛЕНА АГЕЕВА

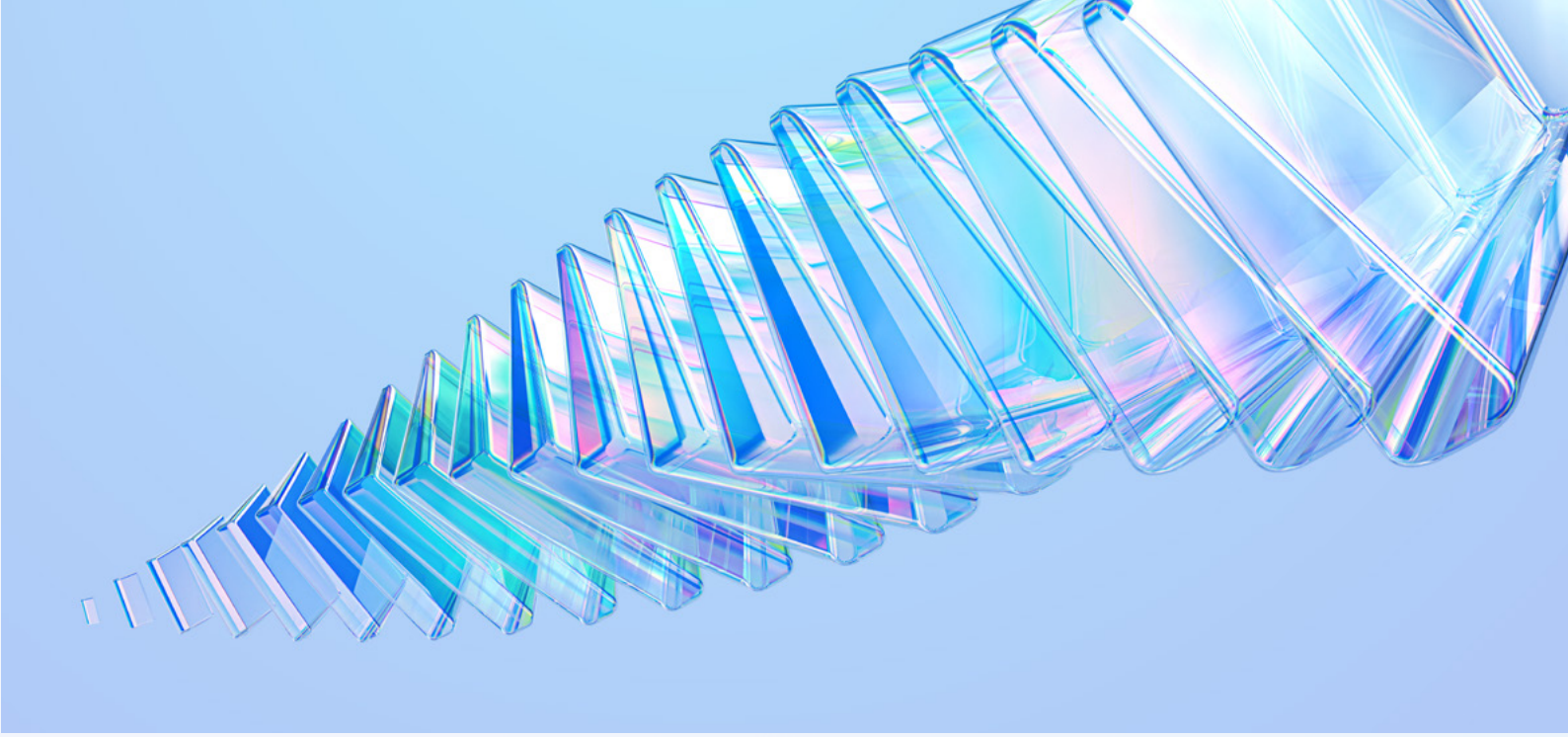
Эксперт по информационной безопасности, «Инфосистемы Джет»

АСКАР МУСАЕВ

Эксперт по информационной безопасности, «Инфосистемы Джет»

ИРИНА ПАВЛОВА

Эксперт по информационной безопасности, «Инфосистемы Джет»



КЛЮЧЕВЫЕ ВЫВОДЫ

- Уровень зрелости процессов ИБ опрошенных компаний распределился между «начальным» и «повторяемым». Компании с уровнем «определенный» и выше составляют около трети выборки.

- Практика пятилетнего планирования в ИБ практически сходит на нет: компании все чаще выбирают планирование короткими временными отрезками (два года), а к планированию до года перешли 4% компаний.

- Руководители ИБ продолжают выбирать «осторожный» метод стратегического планирования, отдавая предпочтение стратегии постепенного улучшения. Количество компаний, которые смотрели в сторону радикальных изменений («инновационные стратегии»), сократилось с 23 до 5%.

- Компании до сих пор отдают предпочтение устаревшей модели «Замок и ров» и модели «Эшелонированная оборона»[1] .

- 14% компаний внедрили сервисный подход[2], 11% реализуют отдельные практики: определение базовых и опциональных сервисов, проработка системы тарификации, выбор инструмента управления сервисами, проработка методологической базы сервисной модели.

- При оценке рисков CISO выбирают качественные шкалы (высокий — средний — низкий) или комбинированные методы, только 8% считают риски в деньгах. Чаще всего считают риски в деньгах в финансовых компаниях, ритейле и крупной промышленности.

- Средний бюджет на кибербезопасность в 2024 году сохранил динамику 2023 года: у трети опрошенных компаний он остался на прежнем уровне, у 60% вырос как минимум на 10%.

[1] Основной принцип модели «Замок и ров» — сосредоточить усилия преимущественно на защите периметра сети. В модели «Эшелонированная оборона» акцент делается на создании нескольких слоев безопасности, которые дополняют друг друга.

[2] Сервисная модель предполагает, что задачи ИБ организуются как набор услуг, которые предоставляются внутренним «поставщиком» (подразделением ИБ) заказчикам с фиксированным SLA.

- С конца 2023 года наблюдается тренд на частичное перераспределение бюджета с функции «предотвращение» (Prevent) на «оперативное выявление угроз» (Detect & Respond).

- Количество компаний, в которых работники ИБ отсутствуют, значительно уменьшилось по сравнению с 2023 годом — всего 6% против 13% в 2024 году.

- Подчинение напрямую топ-менеджменту — самая популярная схема в российских компаниях (61% опрошенных).

- Спрос на работников ИБ остается стабильно высоким — нуждаются в дополнительном штате 78% компаний.

- За три квартала 2024 года число открытых вакансий по ИБ среди опрошенных компаний выросло на 30% по сравнению с аналогичным периодом прошлого года: в 2024 году в 61% компаний была открыта хотя бы одна вакансия специалиста ИБ.

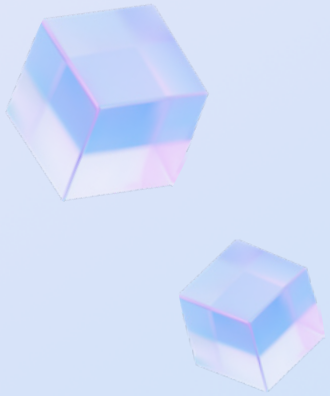
- Нехватка кадров и высокая конкуренция на рынке труда стимулируют работодателей инвестировать в будущие таланты — 52% компаний ответили «Да» на вопрос о готовности найма студентов.

- Предпочтение при поиске отдается кандидатам, способным взяться сразу за несколько направлений ИБ, — с 2023 года количество компаний, которые ищут универсальных специалистов, увеличилось на 18%, ощутимо вырос спрос на руководителей ИБ (CISO) и специалистов в области безопасной разработки.

- Спрос на услуги тестирования Disaster recovery и Business continuity планов для проверки киберустойчивости увеличился более чем на 30%, а самым частым тестируемым сценарием был выбран сценарий успешной атаки вируса-шифровальщика.

- Процесс харденинга (безопасная настройка элементов ИТ) отсутствует более чем в половине компаний.

ВВЕДЕНИЕ



В 2024 году рынок ИБ продолжил перестраиваться. Использование атакующими более продвинутых методов и технологий, ужесточение регуляторных требований, громкие инциденты с приостановкой бизнеса и почти полным уничтожением данных заставляют руководителей служб информационной безопасности (CISO) искать новые подходы к управлению кибербезопасностью.

Традиционные и ранее хорошо работающие методы уже не справляются с современными атаками, вынуждая тратить значительные ресурсы на устранение последствий и восстановление. Многие руководители взяли курс на «переосмысление ИБ» — смещение фокуса на обеспечение непрерывности, проактивное обнаружение атак, эффективное управление ресурсами — то есть «пересборку» архитектуры ИБ с современными практиками киберустойчивости. Мы видим, как руководители служб информационной безопасности вовлекаются в вопросы страхования киберрисков, организацию непрерывности бизнес-процессов и ИТ-инфраструктуры и в целом способствуют интеграции вопросов кибербезопасности на разных уровнях компаний.

Киберустойчивость расширяет подход к безопасности: кратно повышает эффективность реагирования на современные атаки (шифровальщики, атаки на цепочки поставок, APT-атаки и др.) и гарантирует восстановление после них, смещая фокус с классической эшелонированной обороны к адаптивным и гибким архитектурам кибербезопасности

В связи с изменениями мы расширили объем исследования в этом году, включив в него разделы по управлению рисками, в том числе рисками третьих лиц, эффективному управлению и автоматизации ИБ.

В исследовании собраны мнения CISO более чем из 70 российских компаний, принадлежащих к разным сферам бизнеса, и результаты более чем 15 аудитов и проектов по разработке стратегий ИБ.

Результаты исследования позволяют компаниям сравнить свой подход к обеспечению ИБ с подходом других игроков рынка и получить представление о степени развития ИБ в разных сферах. Информация будет полезна руководителям служб ИБ и ИТ, а также консультантам и экспертам в области ИБ.

МЕТОДИКА ПРОВЕДЕНИЯ РАБОТ

Основой для исследования стали результаты опроса CISO (очные интервью и анкетирование), а также накопленные исторические данные по результатам прошлогодних опросов и исследований. Вопросы охватывали следующие области:

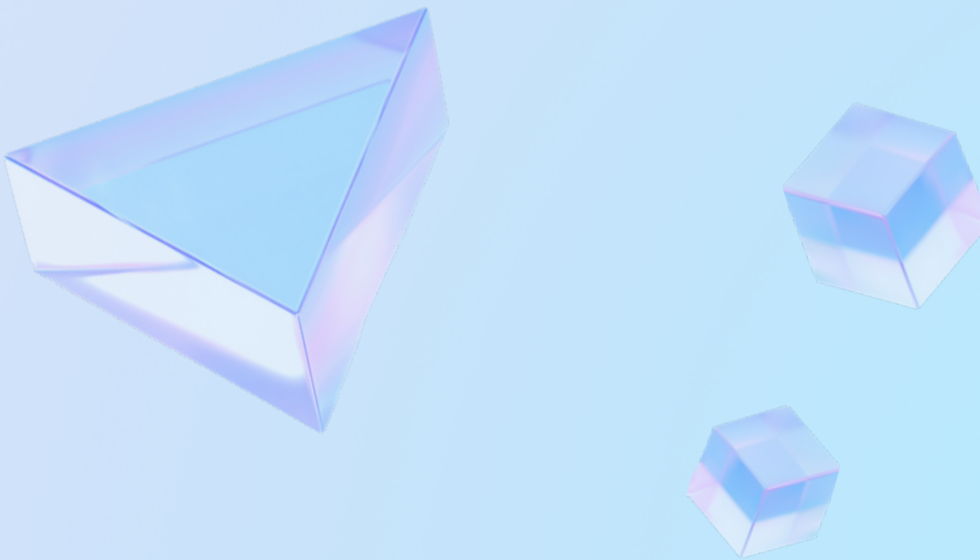
- стратегический менеджмент (постановка и корректировка целей, формирование и защита бюджета на ИБ);
- эффективное управление, использование сервисов и автоматизация;
- организация службы ИБ, поиск и развитие персонала, использование сервисов от внешних провайдеров;
- управление рисками ИБ;
- поддержание киберустойчивости и обеспечение непрерывности бизнеса;
- оценка уровня ИБ и отчетность;
- киберкультура.

Выводы исследования получены на основе анализа данных и тестирования различных гипотез, сформированных на основе наших наблюдений. В отчете мы систематизировали анализ более чем по 15 гипотезам, часть из которых подтвердилась за счет накопленных данных за два рассмотренных периода — 2022–2023 годы и 2023–2024 годы.

Тестирование гипотез — статистический метод, используемый для проверки утверждений или предположений на основе выборочных данных. Помогает определить, есть ли достаточные доказательства для поддержки или опровержения определенной гипотезы.

Примеры гипотез, которые мы проверяли:

- Верно ли, что есть корреляция между зрелостью компании и архитектурной моделью ИБ?
- Верно ли, что величина выделяемого бюджета зависит от схемы подчинения подразделения ИБ?
- Верно ли, что есть зависимость между зрелостью процессного управления на уровне компании и внедрения таких практик в подразделении ИБ?
- Верно ли, что отчетность по ИБ свойственна более зрелым компаниям?
- Верно ли что более зрелые компании (по модели жизненного цикла Ицхака Адизеса[3]) в большей степени имеют Стратегии развития ИБ?



[3] Модель жизненного цикла Ицхака Адизеса используется для определения уровня развития компаний. Согласно этой модели, организации, как и живые организмы, проходят несколько стадий развития и демонстрируют прогнозируемые и повторяющиеся модели поведения. На каждой стадии существуют свои вызовы и сложности. Успех организации на рынке определяется способностью менеджеров управлять переходом от одной стадии к другой.

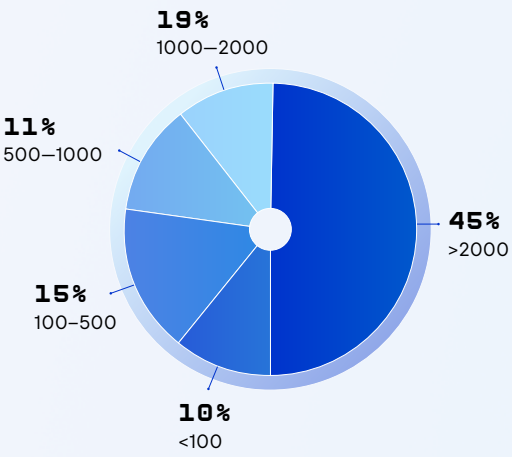
УЧАСТНИКИ ОПРОСА

В опросе приняли участие представители финансового, промышленного и топливно-энергетического сектора, ИТ-компании, организации из сферы телекоммуникаций, транспорта и ритейла. Почти 15% компаний участвовали в опросе повторно.

Сфера деятельности опрошенных компаний

Основные респонденты исследования (75%) — крупные компании со штатом от 500 и до 2000 человек.

Количество сотрудников

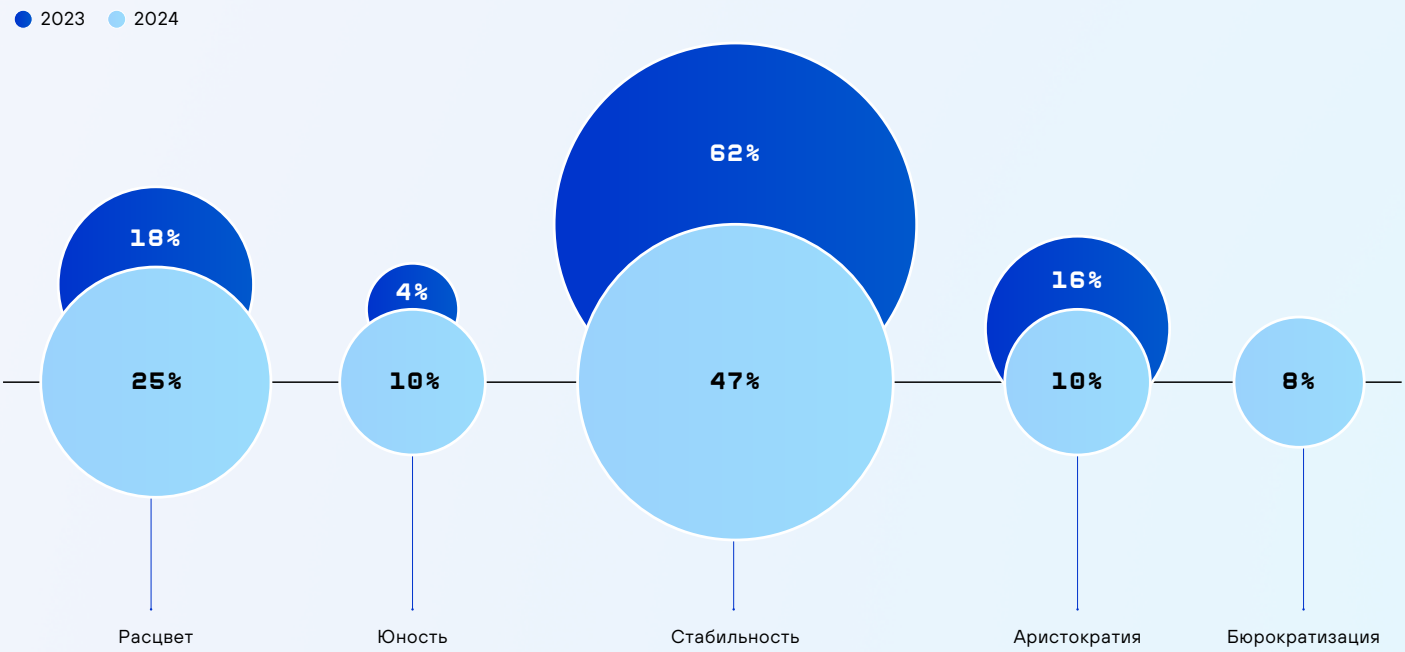


Большинство опрошенных компаний является предприятиями холдингов. Отдельные и самостоятельные организации составляют 36% выборки.

Тип компании

Около половины опрошенных компаний находятся на стадии «Стабильность» по модели жизненного цикла Ицхака Адизеса, то есть чувствуют себя достаточно уверенно. При этом увеличилось количество компаний на стадиях «Расцвет» и «Юность», что обусловлено выборкой опрошенных компаний — почти 20% только начинают выстраивать собственную ИБ, поскольку являются или новыми дочерними обществами крупного холдинга, или молодыми технологическими компаниями.

Модель жизненного цикла Ицхака Адизеса



СТРАТЕГИЧЕСКИЙ МЕНЕДЖМЕНТ

ВЫБОР ВЕКТОРА РАЗВИТИЯ

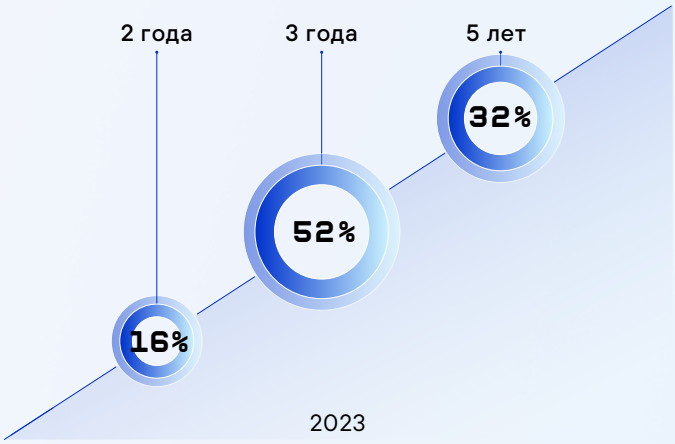
В условиях неопределенности и кризиса стратегическое планирование кибербезопасности требует модернизации и адаптации. Это не означает отказа от стратегического мышления в сторону исключительно тактических шагов — напротив, его роль возрастает, но форма реализации меняется.

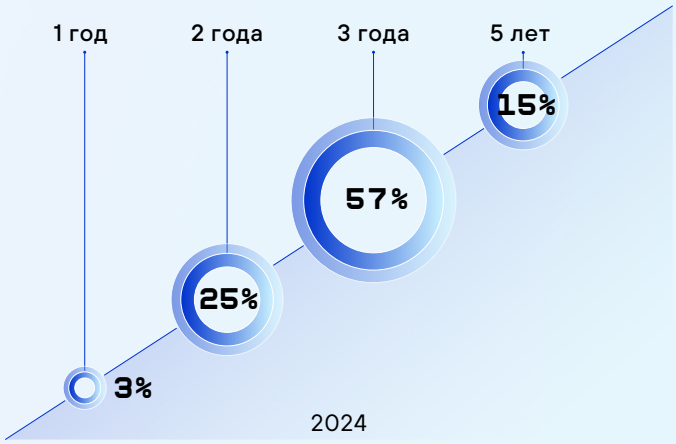
Внешний контекст (санкции, рост ключевой ставки и пр.) продолжает менять подход бизнеса к планированию — классическая модель корпоративной стратегии с детальными планами становится менее применимой: среднесрочные планы (один-два года) становятся оптимальным форматом для управления. Сохранять общее видение («в крупную клетку») и при этом гибко реагировать на изменения — практика, которую мы наблюдаем в большинстве российских компаний как в корпоративных, так и функциональных стратегиях отдельных направлений, в частности в кибербезопасности.

В прошлогоднем отчете мы отмечали тренд на сужение горизонта стратегического планирования, при котором стратегия ИБ трансформируется в серию среднесрочных планов. Практика пятилетнего планирования в российских компаниях практически сходит на нет — за последние два года число таких компаний снизилось почти в два раза (с 32 до 15%). Модель планирования короткими временными отрезками (два года) выбрали 25% опрошенных руководителей ИБ, при этом единичные компании перешли к краткосрочным тактическим действиям, планируя стратегию до года (4%).

Компании вынуждены фокусироваться на более коротких сроках и гибких планах, чтобы оставаться адаптивными. В 2024 году горизонт планирования сократился еще сильнее, постепенно смещаясь к двум годам

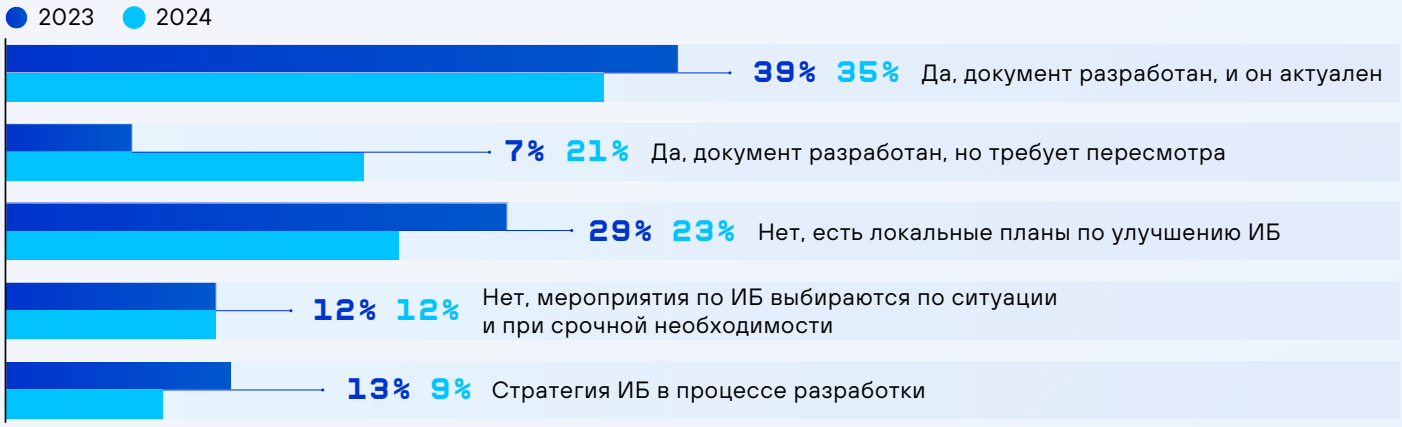
Горизонт стратегического планирования





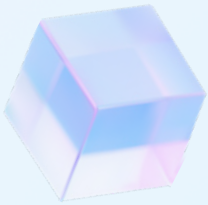
Руководители ИБ постепенно отказываются от исключительно ситуационного менеджмента и локальных планов по улучшению (за год этот показатель снизился на 7%) в пользу стратегического планирования. Стратегию развития ИБ имеет большинство российских компаний (56%), за год этот показатель вырос на 10%. При этом более 20% опрошенных компаний запланировали пересмотр документа — чаще всего причиной пересмотра становилась запланированная цифровая трансформация бизнеса (новая стратегия ИТ), а также окончание прошлого стратегического периода.

Наличие стратегии ИБ в компании

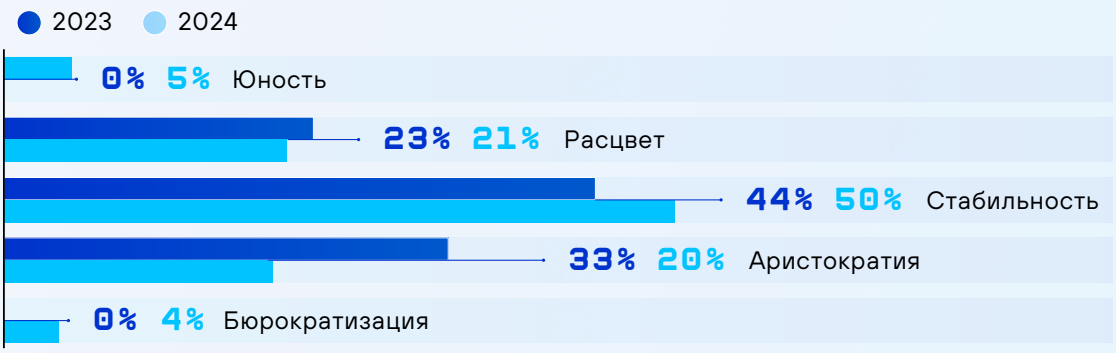


Как правило, стратегическое планирование ИБ развивается вместе с общекорпоративным стратегическим менеджментом. Чтобы проследить эту зависимость, мы использовали модель развития организации, разработанную Ицхаком Адизесом.

На ранних этапах развития компании чаще всего фокусируются на выживании и росте, а ИБ часто воспринимается как второстепенная задача, поэтому процент компаний, где задумываются о наличии стратегии ИБ, невысок (5%). Компании начинают системно подходить к стратегическому планированию ИБ только на этапе «Расцвета» (21%), на этапе «Стабильности» уже имеются устоявшиеся процессы и ресурсы для поддержания ИБ (50% опрошенных).



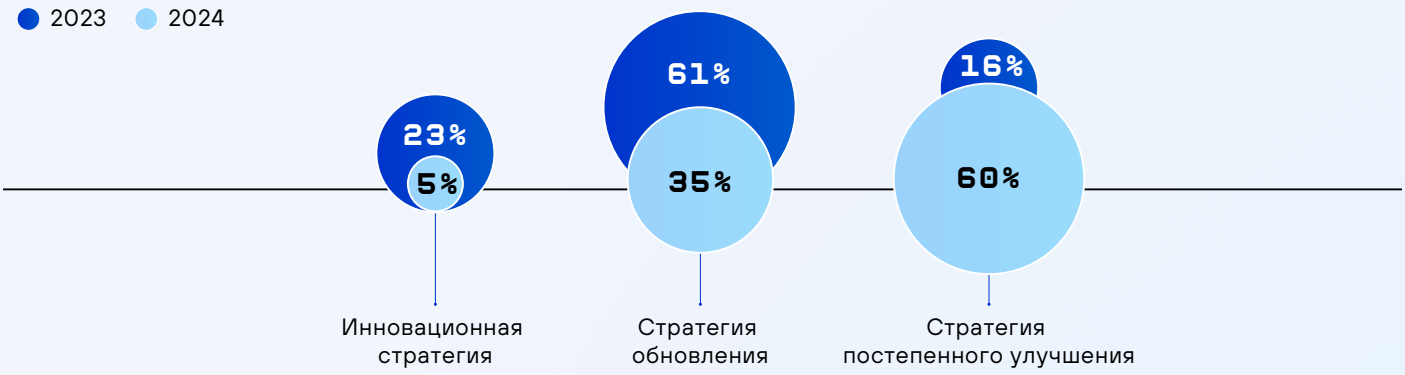
Зависимость наличия стратегии ИБ от стадии жизненного цикла компании



Руководители ИБ продолжают выбирать «острожный» метод стратегического планирования, отдавая среди прочих предпочтение стратегии постепенного улучшения. Она наименее рискованна и требует регулярных, но небольших усилий. К 2024 году большинство компаний уже либо заменили, либо находились в процессе замены ИБ-решений в рамках стратегии импортозамещения. В связи с этим стратегию обновления[4], которая характеризуется модернизацией существующей архитектуры ИБ, в частности технических решений, выбрало только 35% руководителей ИБ, что на 26% меньше 2023 года.

Инновационные стратегии ИБ на практике мы почти не встречаем — количество компаний, которые думали о радикальных изменениях, сократилось более чем в 4 раза (с 23 до 5%).

Тип действующей стратегии ИБ



С изменением горизонта стратегического планирования и выбора типа стратегии, мы наблюдаем качественное изменение в выборе руководителем ИБ способа обоснования топ-менеджменту необходимого целевого состояния ИБ. В дополнение к классическим методам (повышение уровня зрелости, список критериев готовности, достижение целей ИБ) топ-менеджмент все чаще хочет видеть понятные метрики в стратегии развития ИБ — «покрытие» внешних ресурсов средствами защиты, снижение MTTD[5], MTTR[6], времени простоя из-за киберинцидентов и т.д. Практика формирования стратегического вектора и расстановки приоритетов за счет определения недопустимых событий пока слабо распространена и встречается единично.

[4] Согласно ГОСТ Р 54147-2010. Стратегический и инновационный менеджмент. Термины и определения:

- Инновационная стратегия строится вокруг новых, «прорывных» продуктов или решений. Новизна стратегии охватывает все основные составляющие: масштаб, облик и цели.
- Стратегия обновления является промежуточной между инновационной стратегией и стратегией постоянного совершенствования.
- Стратегия постепенного совершенствования предполагает постепенные небольшие изменения масштаба, облика и цели: выполнение в основном прежних операций, но в больших объемах и с незначительными изменениями используемых процессов.

[5] Mean time to detect — среднее время, которое проходит между моментом возникновения инцидента и его обнаруженем командой реагирования.

[6] Mean time to repair — среднее время восстановления/стабилизации.

С 2024 года мы также фиксируем рост интереса к направлению непрерывности бизнеса, увеличение спроса на выстраивание процессов и стратегий киберустойчивости — такие проекты стали чаще появляться в стратегиях развития ИБ. Серии громких инцидентов с вирусами-шифровальщиками сформировали среди руководителей крупных компаний спрос на независимое подтверждение собственной киберустойчивости — настольные тестирования и киберучения.

БЮДЖЕТЫ ИБ

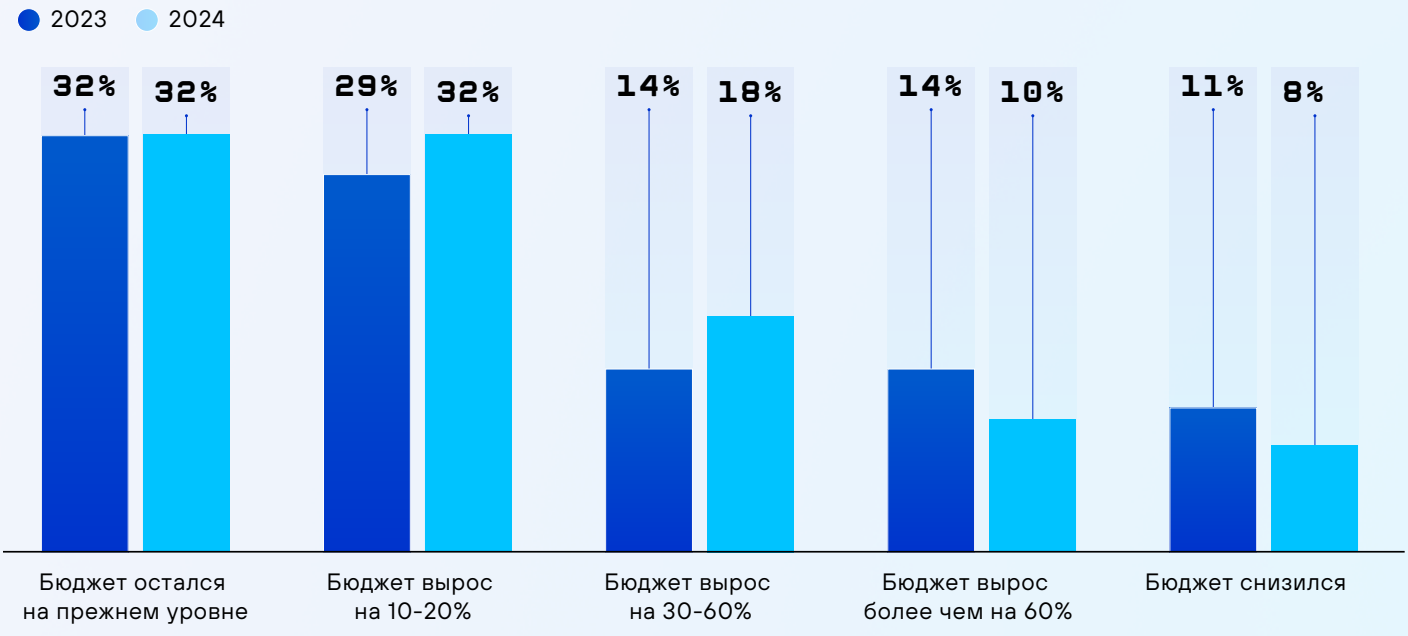
Бюджет ИБ в 2024 году рос умеренно ввиду экономической неопределенности. Крупные компании продолжали инвестировать в ИБ, повышая эффективность уже существующих мер, а тренды бюджетирования начали смещаться в направлении развития систем мониторинга и реагирования (Detect & Respond). Подход к планированию стал более осознанным и системным, а ИБ-стратегии синхронизируются с бизнес-целями.

В лидерах отраслей, на которые пришелся рост бюджета в 2024 году, **— финансовый сектор (25%), промышленность (22%) и ИТ (15%).**

Средний бюджет на кибербезопасность в 2024 году сохранил динамику 2023 года: у трети опрошенных компаний бюджет остался на прежнем уровне, у 60% бюджет вырос минимум на 10%.

Бюджеты на кибербезопасность небольших компаний в основном остались на прежнем уровне и были проиндексированы на уровень инфляции. Рост бюджета более 30% отмечен только в крупном enterprise с численностью сотрудников от 1000 человек.

Изменение бюджета на ИБ



Накопительные данные за два года подсветили тренд на «расслоение» между сферами SMB и крупным бизнесом. Заметное отличие в объемах выделяемого бюджета на ИБ между крупными и малыми компаниями в том числе подтверждают отчеты World Economic Forum по перспективам глобальной кибербезопасности на международном рынке и рынке РФ.

Многие компании до сих пор не могут перейти от принципа ограничения бюджета на уровне предыдущих финансовых периодов («деньги выделяют как в прошлом году») к обоснованию формирования «бюджета от потребностей»

По нашему опыту проектов по разработке стратегий развития ИБ, больше шансов на выделение дополнительного бюджета наблюдается у CISO, которые используют при планировании инициатив и утверждении бюджета систему координат, понятную бизнесу. Наиболее популярными остаются оценка рисков, повышение оценки зрелости и метрики эффективности. Концепт недопустимых событий как способ «разговора с бизнесом на одном языке» пока встречается единично. Наиболее убедительными при обосновании бюджета остаются кейсы с инцидентами у конкурентов, которые привели к существенным финансовым и репутационным потерям, и результаты показательных тестирований на проникновение (внешний пентест).

Накопленные данные за два года подтвердили интересную гипотезу — влияние величины бюджета на стиль подчинения службы ИБ: ИБ в подчинении ИТ-подразделения или службы безопасности ограничена в увеличении выделяемого бюджета, и в основном вопрос решается по остаточному принципу. Стагнация или стабильность бюджета с таким типом подчинения отмечались почти в 20% таких компаний. Значительно бюджет вырос в компаниях именно с прямым, «классическим» подчинением.

Динамика выделения бюджета на ИБ в зависимости от стиля подчинения

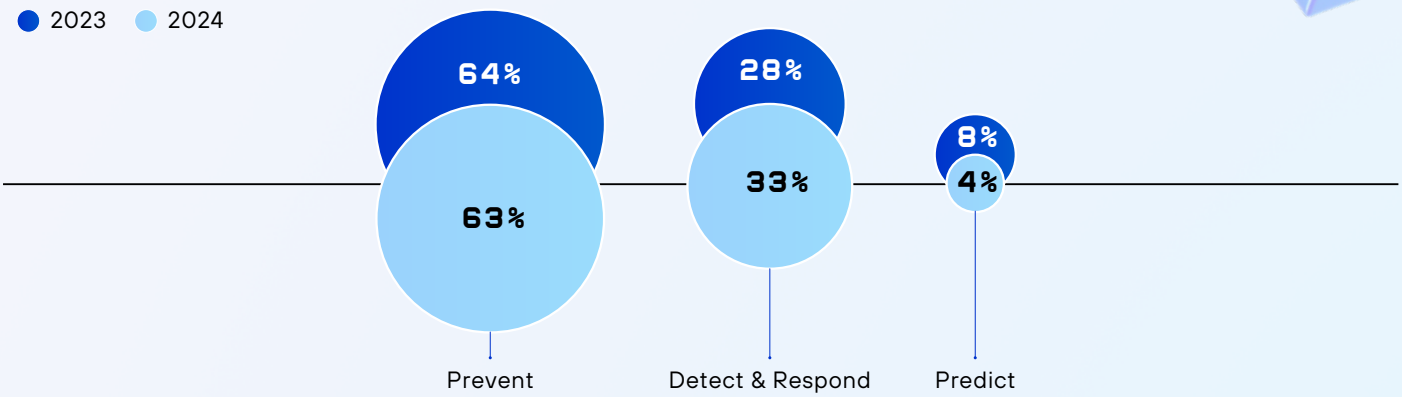
	Бюджет вырос на 10-20%	Бюджет вырос на 30-60%	Бюджет вырос более чем на 60%	Бюджет остался на прежнем уровне	Бюджет снизился
ИБ независима, подчинена напрямую исполнительному органу	26%	10%	6%	14%	3%
ИБ отсутствует / функции выполняются ИТ	0%	0%	1%	0%	0%
ИБ подчинена ИТ	3%	3%	1%	9%	2%
ИБ подчинена СБ	2%	4%	1%	9%	2%
Другой вариант подчинения	1%	1%	1%	0%	1%

Еще один фактор, значительно повлиявший на рост бюджета, — исполнение требований регуляторов (в частности, импортозамещение) и усиление ответственности за несоблюдение нормативных требований. С введением оборотных штрафов за утечку персональных данных мы прогнозируем изменение этих показателей в 2025 году.

Ключевой фактор успешной защиты и увеличения бюджета ИБ заключается в независимости ИБ и прямом диалоге ИБ с руководством компании

С конца 2023 года сохраняется акцент на распределение бюджета на функции «предотвращение» (Prevent) и «оперативное выявление угроз» (Detect & Respond). При этом увеличение бюджетирования функции Detect & Respond («обнаружение и реагирование») объясняется тем, что компании, которые с 2022 года начали трансформировать свою инфраструктуру, начинают смещать акцент в сторону ее интеграции с системами мониторинга, используя экспертные сервисы (SOC, киберучения и т.п.). Меры «предотвращение» (Prevent) по-прежнему показывают высокую долю бюджетирования, поскольку компании продолжают мигрировать на отечественные решения, например сетевую безопасность (NGFW).

Фокус бюджетирования на ИБ в 2024 году



Наибольший рост вложений в превентивные меры наблюдается в сферах промышленности и финансовом секторе — они строго зарегулированы законодательно, но процесс импортозамещения еще на завершен, а возникающие риски могут нести серьезные последствия для государства ввиду критичности инфраструктуры.

Изменения в перераспределении бюджета показывают поступательный рост зрелости ИБ в компаниях: от преимущественно превентивного подхода к более комплексной киберустойчивой модели, включающей в том числе проактивные сервисы и восстановление

Помимо типовых мер ИБ, бюджетируемых из года в год, некоторые компании стали включать в свои дорожные карты развития ИБ инновационные и трендовые направления (киберстрахование, машинное обучение в сфере ИБ), но на практике такие проекты единичны.

ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ, ИСПОЛЬЗОВАНИЕ СЕРВИСОВ И АВТОМАТИЗАЦИЯ

В современной теории управления рассматриваются различные концепции построения организационной структуры компании: функциональный подход, ситуационный метод и процессно-ориентированная модель, как наиболее современная модель управления. Управление на основе процессов входит в перечень инструментов большинства стандартов по системе менеджмента и обеспечивает более эффективное использование ресурсов и разрушает барьеры между подразделениями.

УПРАВЛЕНИЕ ПО ПРОЦЕССАМ

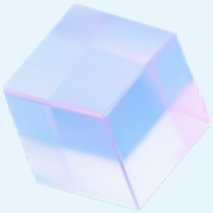
Рассмотрим процессно-ориентированную модель в контексте ИБ более подробно.

Вопрос внедрения общекорпоративного процессного управления на уровне компании не рассматривается или практики отсутствуют примерно у 24% опрошенных компаний. В основном российские компании находятся на уровнях «описанный» (37%) и «контролируемый» (39%). На этих уровнях практики применяются либо только для отдельных, ключевых бизнес-процессов, либо бизнес-процессы регламентированы и, в целом, и для большинства установлены детальные контрольные процедуры.

Уровни зрелости «интегрированный» и «проактивно управляемый» встречаются единично, так как большинство компаний останавливаются на уровне контролируемых процессов — это позволяет им решать текущие задачи без необходимости в столь глубокой трансформации.

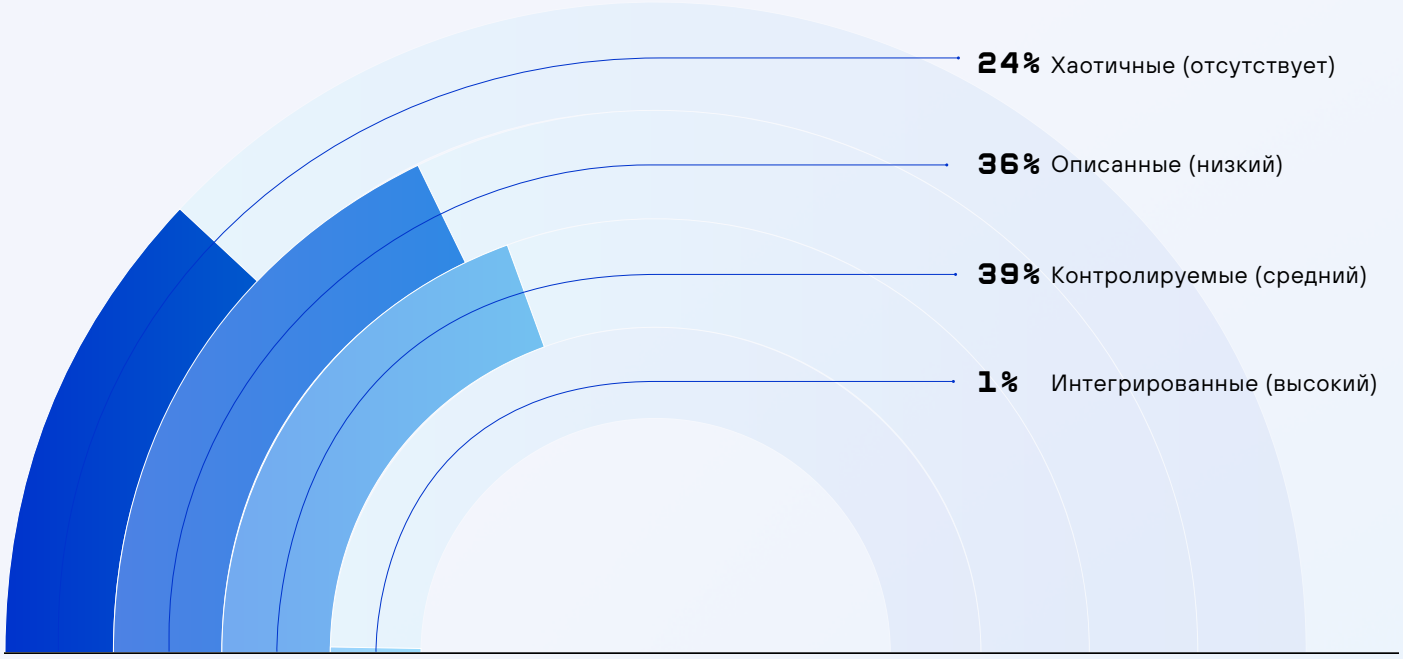
Чтобы подчеркнуть взаимосвязь между общим уровнем развития процессного подхода в организации и его применением в подразделении ИБ, мы использовали упрощенную шкалу оценки зрелости ABPMP Russia[7], состоящую из пяти последовательных этапов повышения качества процессов:

- Хаотичные (отсутствует)
- Описанные (низкий)
- Контролируемые (средний)
- Интегрированные (высокий)
- Проактивно управляемые (передовой)



[7] https://abpmp.org.ru/project/maturity/

Зрелость процессного управления на уровне компании



Если компания уже имеет опыт внедрения практик управления общекорпоративными процессами, то это создает благоприятную почву и для их применения в сфере ИБ. Так, в компаниях с уровнем зрелости «описанный», «контролируемый» и «интегрированный» уже 55% руководителей служб ИБ либо уже внедрили методы процессного управления в ИБ, либо в процессе перехода.

Зрелость процессного управления в компании напрямую влияет на успех внедрения практик процессного управления в подразделении ИБ, образуя практически линейную зависимость

Как зрелость общекорпоративного процессного управления влияет на внедрение практик процессного управления в подразделении ИБ

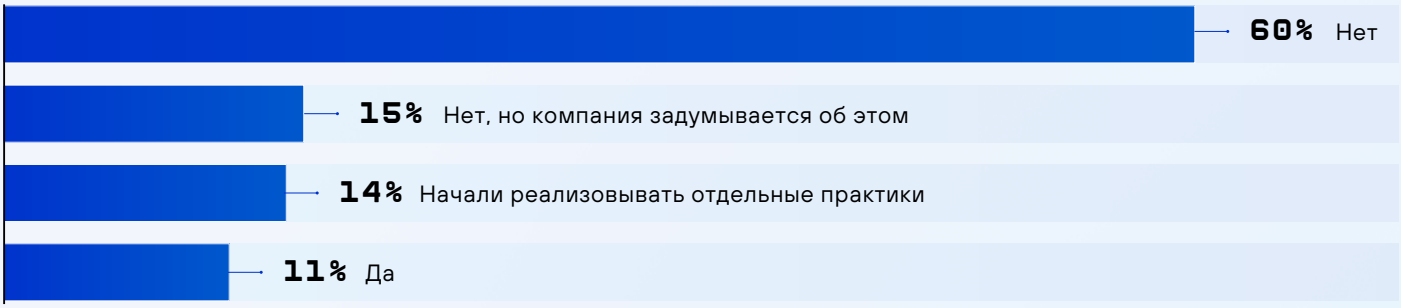
Осуществляется ли управление ИБ при помощи процессного подхода? / Уровень развития процессного подхода в компании	Нет	Нет, но компания задумывается об этом	Да, в процессе перехода на данную модель	Да
Хаотичные (отсутствует)	19%	2%	3%	0%
Описанные (низкий)	5%	8%	18%	5%
Контролируемые (средний)	0%	8%	11%	20%
Интегрированные (высокий)	0%	0%	0%	1%

СЕРВИСНАЯ МОДЕЛЬ ИБ

В рамках выбора подхода, который будет обеспечивать высокие требования бизнеса к надежности, управляемости и прозрачности ИБ, крупные компании выбирают более сложные сервисные или гибридные модели управления ИБ. Сервисная модель предполагает, что задачи ИБ организуются как набор услуг, которые предоставляются внутренним «поставщиком» (подразделением ИБ) заказчикам с фиксированным SLA.

Кибериндустрия только делает первые шаги в этом направлении: всего 14% компаний внедрили сервисный подход, 11% реализуют отдельные практики — определение базовых и опциональных сервисов, проработка системы тарификации, выбор инструмента управления сервисами, проработка методологической базы сервисной модели.

Используется ли в компании сервисный подход для обеспечения ИБ?

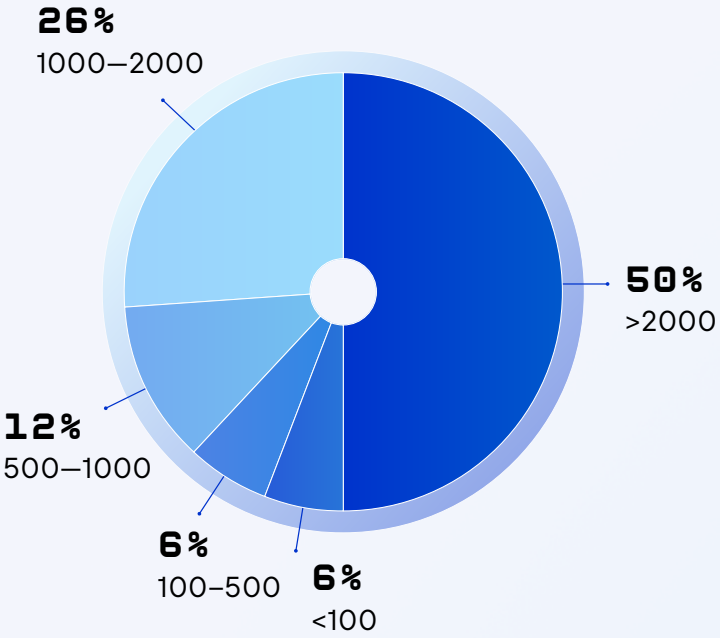


Самая популярная «модель потребления» сервисов — централизация экспертизы и ресурсов ИБ на базе головной компании, которая предоставляет услуги дочерним обществам. Такая модель характерна для крупных компаний с большим количеством юридических лиц: она помогает справиться с масштабом, предоставляя единый набор стандартных услуг для всех бизнес-единиц, способствует оптимизации расходов и легко масштабируется при покупке новых активов. Только 3% компаний (в основном крупные ИТ-компании), которые уже реализовали сервисный подход, не являются частью холдинга и экосистемы.

Менее популярная модель — когда потребителями услуг ИБ являются внутренние подразделения компании. В этом случае важным инструментом является OLA (Operational Level Agreement), который описывает взаимодействие между подразделением и определяет конкретные условия предоставления услуг ИБ. Наличие OLA было отмечено только в финансовой отрасли (около 25% опрошенных) и единично — в крупных ИТ-компаниях.

«Пионерами» внедрения сервисной модели являются крупные компании финансовой отрасли, промышленности, ТЭК и ИТ со штатом более 2000 человек.

Масштаб компаний, в которых внедряется сервисная модель или реализуются отдельные ее практики



ИСПОЛЬЗОВАНИЕ MSSP И ИИ

Отдельно стоит рассмотреть практику использования компаниями услуг по модели Managed Security Service Provider (MSSP). Сложность найма специалистов, трудоемкость разворачивания и сопровождения on-prem-решений становятся катализатором интереса к MSSP-сервисам, особенно для сегмента SMB (малый и средний бизнес). Так, в компаниях с числом работников от 100 до 500 и от 500 до 1000 более 55% используют внешние сервисы.

Сервисы, наиболее часто используемые российскими компаниями:

- Защита от DDoS-атак
- Сервис центра мониторинга и реагирования на инциденты ИБ
- Поддержка средств защиты информации
- Сервис фильтрации трафика уровня веб-приложений
- Сервис антифишинга

Также набирают популярность сервисы Digital Risk Protection и Continuous Penetration Testing.

Несмотря на распространенное мнение о том, что интеллектуальные алгоритмы и нейросети активно внедряются для совершенствования систем кибербезопасности, повышения эффективности и автоматизации, респонденты не смогли отметить ни один сценарий, где ИИ бы применялся системно для решения операционных задач. В основном руководители ИБ используют большие языковые модели и их отдельные модули (GPT agents) в качестве виртуальных помощников, для поиска информации или обучения.

Осторожнее всего к использованию внешних услуг относятся компании промышленного сектора — **более 60% компаний данного сектора не используют и не планируют подключать MSSP-сервисы**

ОРГАНИЗАЦИЯ СЛУЖБЫ ИБ

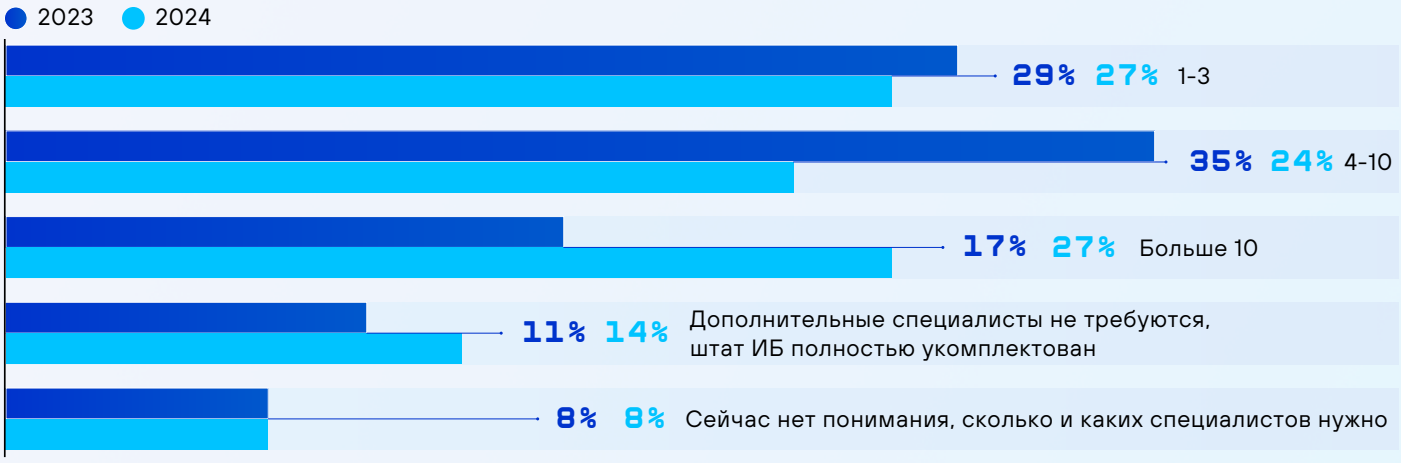
ПОИСК КАДРОВ

По оценкам Министерства цифрового развития, связи и массовых коммуникаций РФ, ИТ-отрасли в России не хватает около 500–700 тысяч работников ИТ[8]. Дефицит специалистов в сфере ИБ, по информации отдельных исследований[9], в 2023 году в России достиг 50 тысяч человек, в 2024 году он оценивался в 100 тысяч[10] и больше.

Спрос на работников ИБ среди опрошенных нами компаний остается стабильно высоким: нуждаются в дополнительном штате 78% компаний.

Растущий «аппетит» в отношении кадров наблюдается преимущественно среди крупных компаний (Large Enterprise), где ищут более 10 специалистов ИБ. В таких компаниях штат уже укомплектован опытными специалистами и его продолжают расширять. В основном от одного до трех специалистов ищут компании сегмента SMB (Small-Medium Business) с фокусом на эксперта-мультиинструменталиста.

Число дополнительных ИБ-специалистов, необходимых компании для полноценного покрытия операционных задач и развития функции ИБ



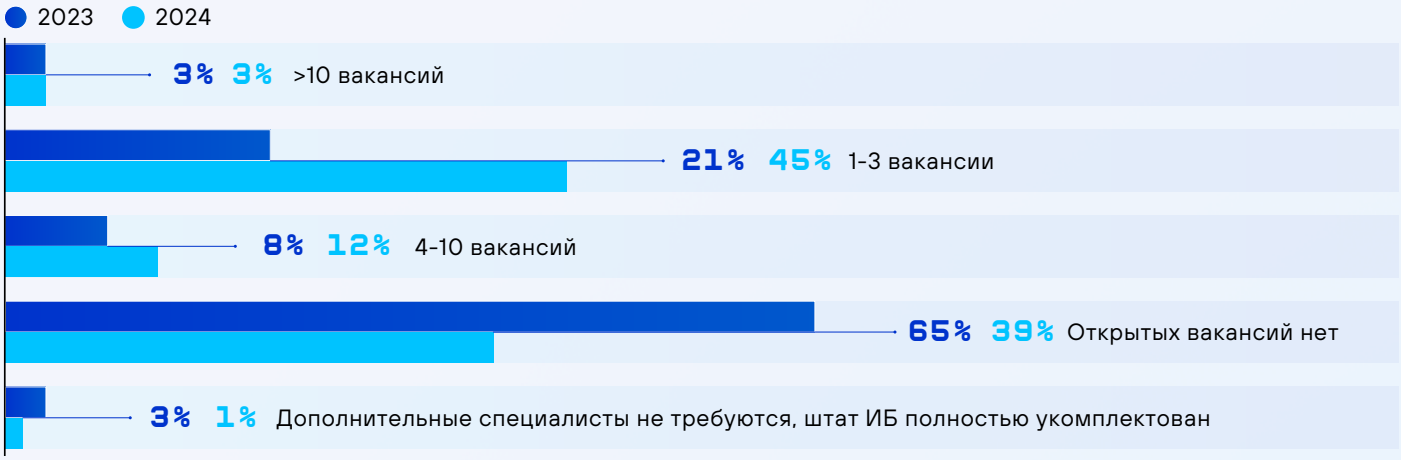
[8] «Ведомости». Глава Минцифры оценил дефицит кадров в ИТ-отрасли в 500 000 – 700 000 человек: https://www.vedomosti.ru/economics/news/2023/08/16/990480-glava-mintsifri-otsenil-defitsit-kadrov-it-otrasli

[9] Рынок труда в информационной безопасности в России в 2024 – 2027 гг.: прогнозы, проблемы и перспективы: https://www.ptsecurity.com/ru-ru/research/analytics/preview/rynok-truda-v-informacczionnoj-bezopasnosti-v-rossii-v-2024-2027-gg-prognozy-problemy-i-perspektivy/?utm_source=pt&utm_medium=article&utm_campaign=issledovanie-czsr-severo-zapad-i-pt&utm_content=news

[10] https://www.fontanka.ru/2024/10/17/74219291/

С начала 2024 года мы наблюдаем динамику изменения числа открытых вакансий, особенно в сегменте крупного бизнеса. За 2024 год число открытых вакансий по ИБ среди опрошенных нами компаний выросло на 30% по сравнению с аналогичным периодом прошлого года: так, в 2024 году в 60% компаний была открыта хотя бы одна вакансия специалиста ИБ. ста ИБ.

Число вакансий специалистов ИБ, открытых за 2023–2024 годы

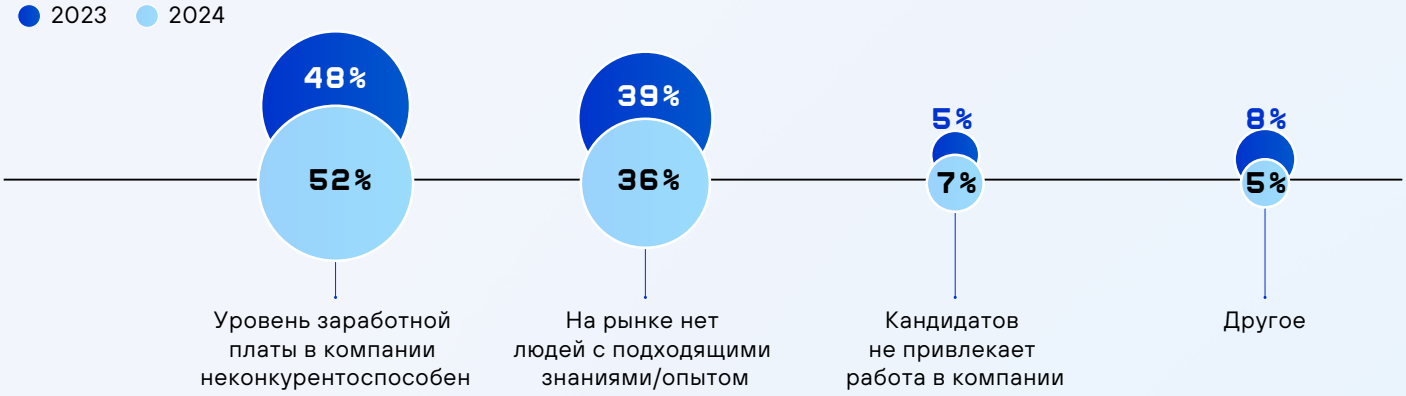


Большинство опрошенных руководителей ищут от одного до трех специалистов в штат, что обусловлено сложностями с обоснованием и открытием новых вакансий. Предпочтение при поиске отдается кандидатам, способным взяться сразу за несколько направлений ИБ: с 2023 года количество компаний, которые ищут универсальных специалистов, увеличилось на 18%, что составило почти половину опрошенных (52%). Также ощутимо вырос спрос на руководителей ИБ (CISO) и специалистов в области безопасной разработки.

ИБ-специалисты, которых чаще всего ищут

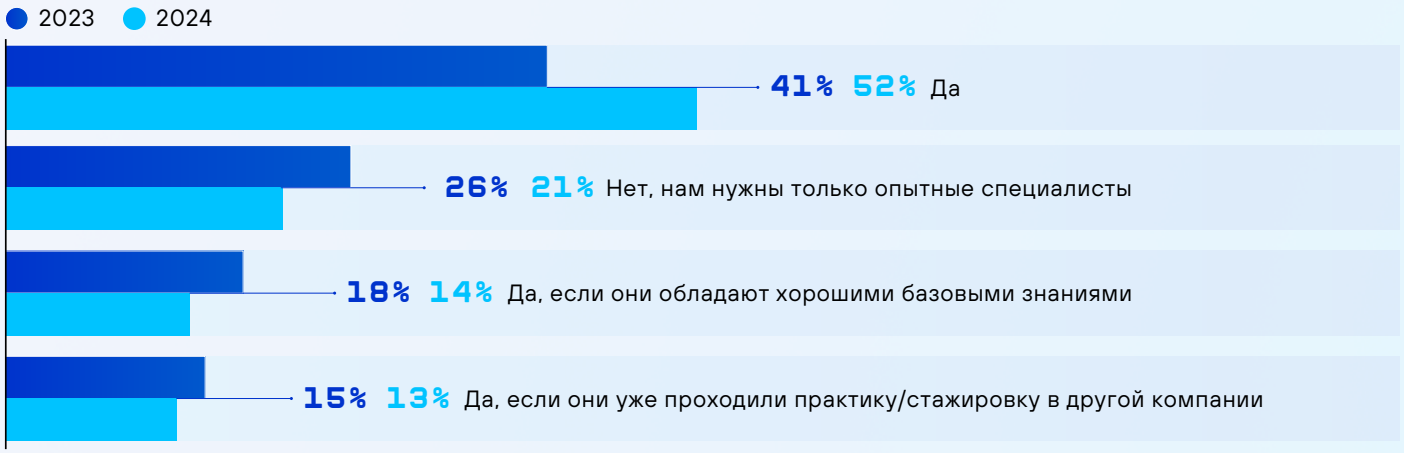
Средний срок закрытия позиций остался на уровне 2023 года: три-четыре месяца — для специалиста и шесть-семь месяцев — для руководителей в сфере ИБ. Одной из ключевых причин затягивания процесса подбора кадров являются высокий уровень конкуренции в борьбе за кандидатов. По данным индекса HH.ru, это приводит к «перегреву» рынка труда: кандидаты имеют высокие зарплатные ожидания, которые не могут быть удовлетворены небольшими компаниями. Так, неконкурентоспособный уровень зарплаты (52%) и отсутствие специалистов с подходящими знаниями и опытом (36%) были названы основными проблемами при поиске специалистов в штат.

Причина сложности найма новых ИБ-специалистов



Нехватка кадров и высокая конкуренция на рынке труда стимулируют работодателей все чаще инвестировать в будущие таланты — 52% компаний уверенно ответили «Да» на вопрос о готовности найма студентов, что на 11% выше показателя 2023 года. Высокая готовность брать в штат студентов наблюдается у тех же компаний, которые испытают наибольший кадровый голод: в компаниях финансовой отрасли, промышленности и ИТ. На практике мы действительно наблюдаем большой спрос на студентов — нередко они уже со 2–3-го курса совмещают работу и учебу.

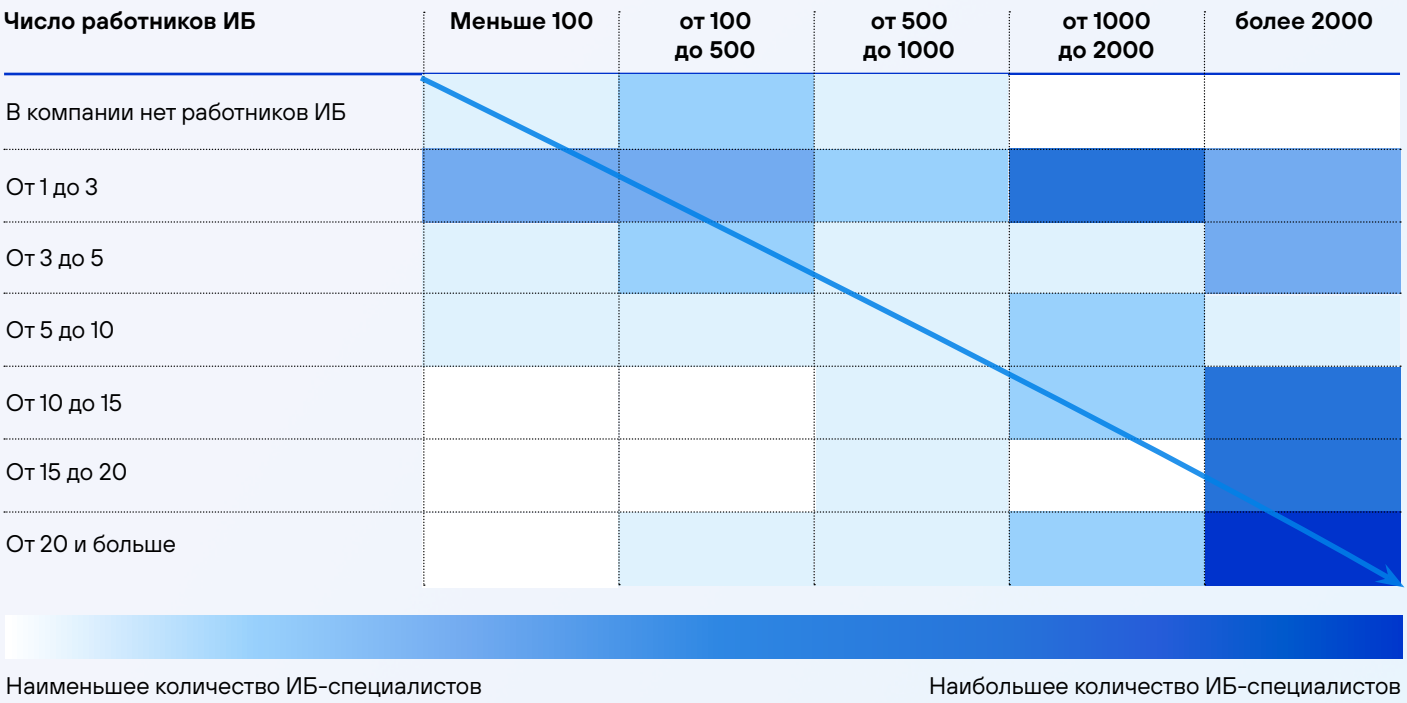
Готовность брать в штат выпускников по ИБ-специальностям



ФОРМИРОВАНИЕ КОМАНД ПО ИБ

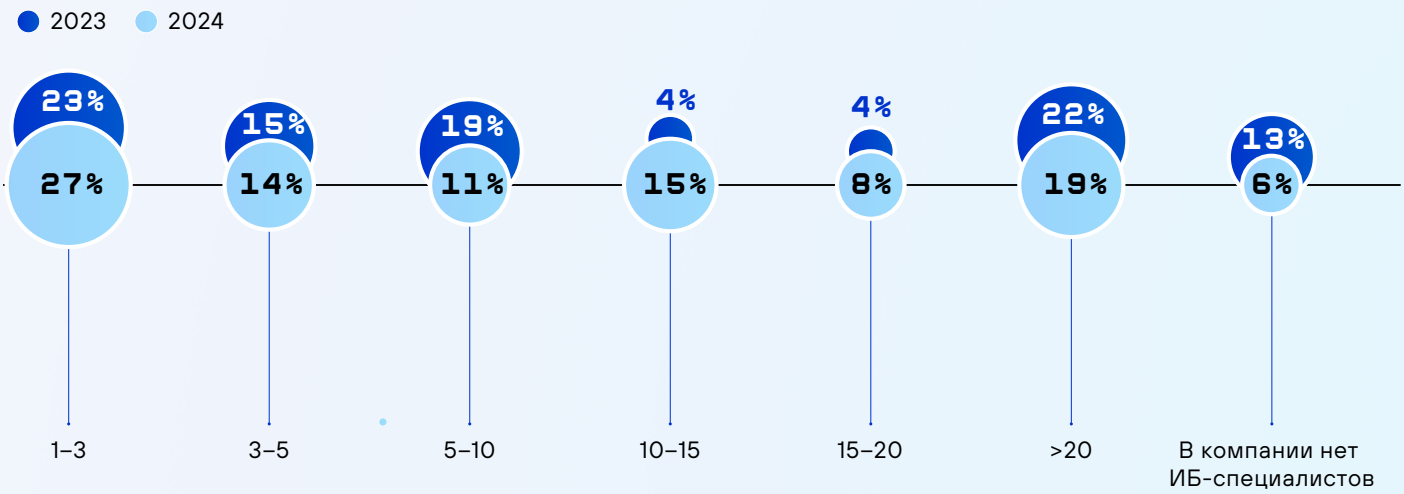
Накопительные данные опроса за два года еще раз подтверждают практически линейную зависимость между численностью команды ИБ и общим количеством работников в компании. При этом одиночных специалистов без команды становится все меньше.

Зависимость размера команды ИБ от общей численности работников компании



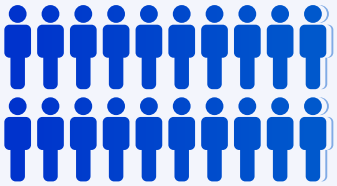
Увеличение числа законодательных требований, рост и усложнение ИТ-инфраструктуры, реальный пережитый опыт восстановления после атак повлияли на формирование подразделений, отвечающих за ИБ. Количество компаний, в которых работники ИБ отсутствуют, значительно уменьшилось по сравнению с 2023 годом — такие компании составляют всего 6% от всей выборки.

Среднее число ИБ-специалистов в отдельных компаниях



Среднее число ИБ-специалистов по отраслям практически не изменилось за 2024 год, исключением стали компании в сфере транспорта (рост с одного-трех до трех-пяти специалистов). Полное отсутствие штата ИБ встречалось редко — единичные случаи в ритейле, топливно-энергетическом комплексе, промышленности и здравоохранении.

Среднее число ИБ-специалистов в разных сферах бизнеса (2024)



>20

Финансовый сектор и ИТ

5–10

Топливно-энергетический комплекс, промышленность, здравоохранение

10–15

Ритейл

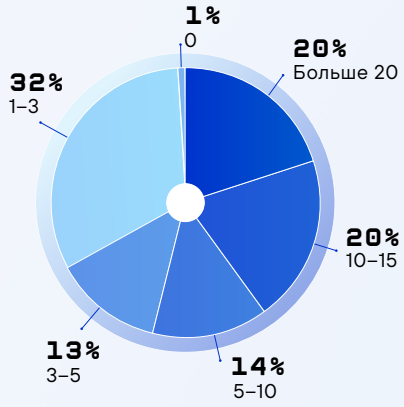
Прирост средней численности кадров

3–5
Транспорт

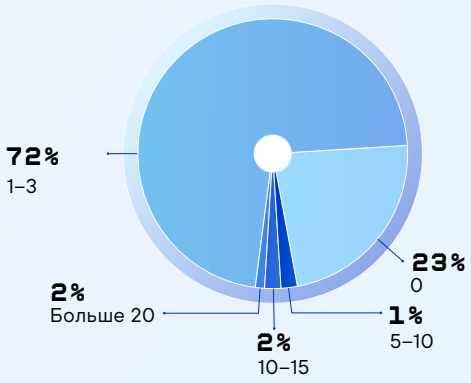
5–10
Другое

Размер штата ИБ в разных сферах бизнеса

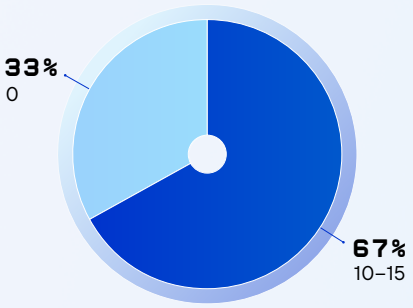
Финансовый сектор



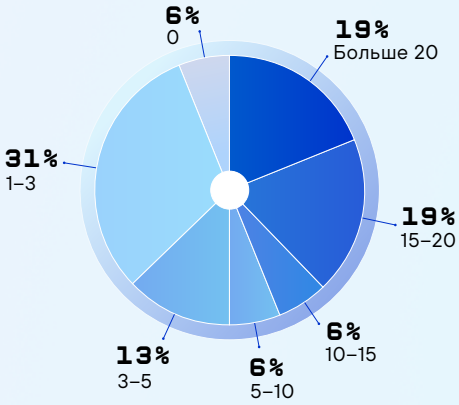
Топливно-энергетический комплекс



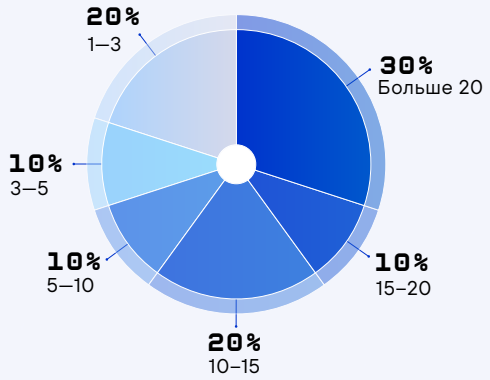
Ритейл



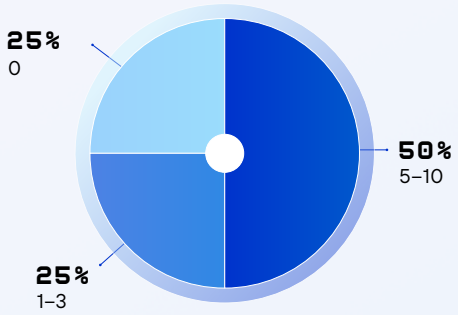
Промышленность



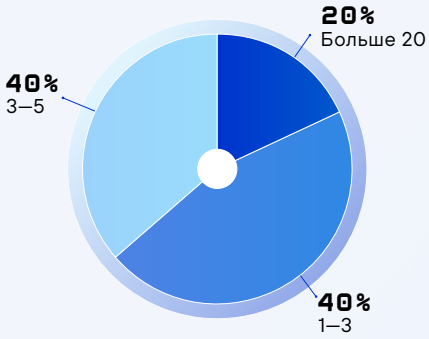
ИТ



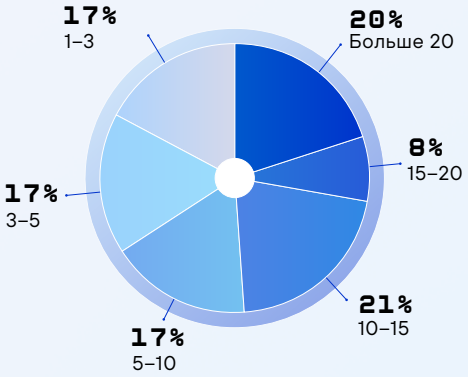
Здравоохранение



Транспорт



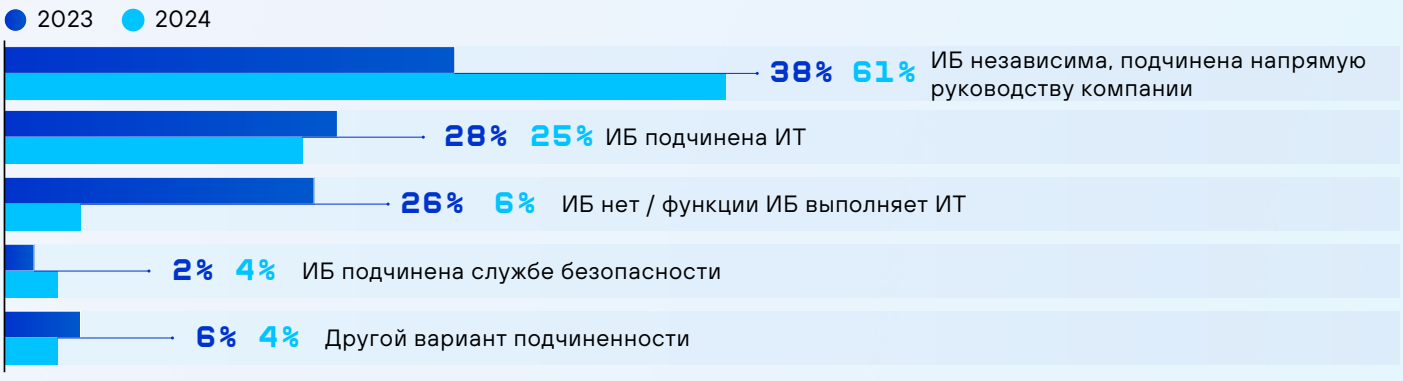
Другое



СТРУКТУРНАЯ ПОДЧИНЕННОСТЬ ПОДРАЗДЕЛЕНИЯ ИБ

В 2024 году независимость ИБ от других структурных подразделений стала самым распространенным вариантом подчинения — она отмечена более чем в половине опрошенных компаний (61%). Высокий процент обусловлен в том числе выборкой опрошенных компаний — почти 20% только начинают выстраивать собственную ИБ (являются новым дочерним обществом крупного холдинга или технологической компанией) и со старта выбирают наиболее оптимальную и эффективную модель.

Подчиненность подразделения ИБ



Характер подчинения службы ИБ в той или иной отрасли практически не изменился за 2023–2024 годы. Подчинение напрямую руководству компании все так же характерно для компаний финансового сектора и для государственных учреждений. Подчинение ИБ функции ИТ чаще всего наблюдается в сфере промышленности и транспорта.

Зависимость между сферой деятельности компании и подчиненностью ИБ (накопительный срез за 2023 и 2024 годы)

	Финансовый сектор	Промышленность	Ритейл	Топливно-энергетический комплекс	Транспорт	ИТ	Государственные учреждения	Другое[11]
ИБ независима, подчинена напрямую руководству компании	27%	8%	2%	2%	2%	6%	4%	11%
ИБ подчинена ИТ	4%	6%		3%	8%	2%		1%
ИБ нет / функции ИБ выполняет ИТ	1%	2%	1%		3%			
ИБ подчинена СБ		1%		2%	1%			
Другой вариант подчинения	1%			1%				1%

[11] В данную категорию были отнесены компании из сферы здравоохранения, науки и образования, телекома, СМИ и иные коммерческие компании (сфера услуг, девелопмент, HoReCa и др.), что связано с малым количеством организаций из этих отраслей в выборке.

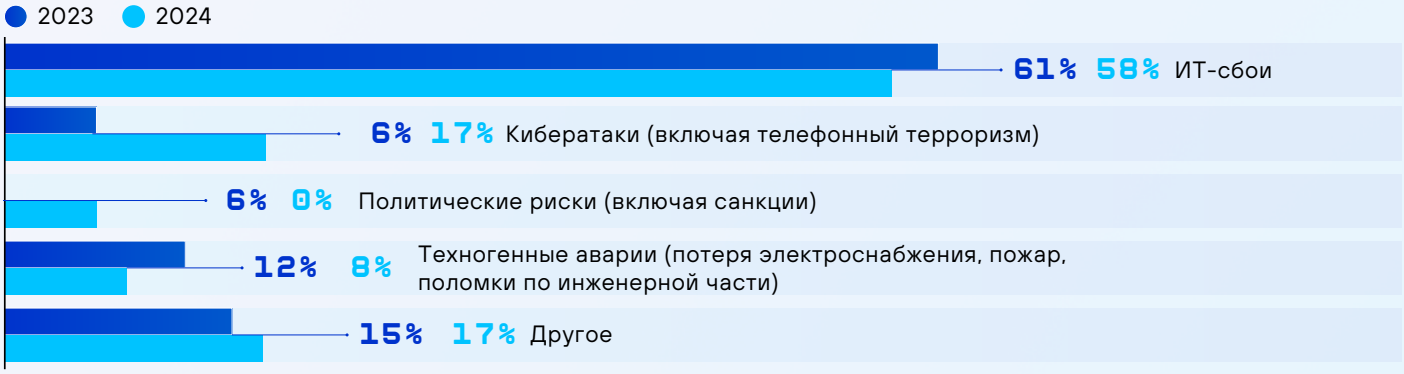
КИБЕРУСТОЙЧИВОСТЬ

Киберустойчивость как концепция развития кибербезопасности заставляет организации сосредотачивать свои усилия не только на защите, но и на реагировании на инциденты, а также на восстановлении после кибератак. Устойчивая архитектура защитных мер, харденинг, практики кризисного реагирования и непрерывности бизнеса — все это ключевые компоненты киберустойчивости, которые мы рассмотрим в этом разделе.

Киберустойчивость смещает акцент противодействия компании киберугрозам с вопроса «может ли такое произойти с нами?» на вопрос «что мы будем делать, если такое произойдет с нами?», в рамках которого ключевую роль играют процессы восстановления бизнеса.

В 2024 году увеличилась доля компаний, считающих кибератаки основным риском прерывания бизнеса.

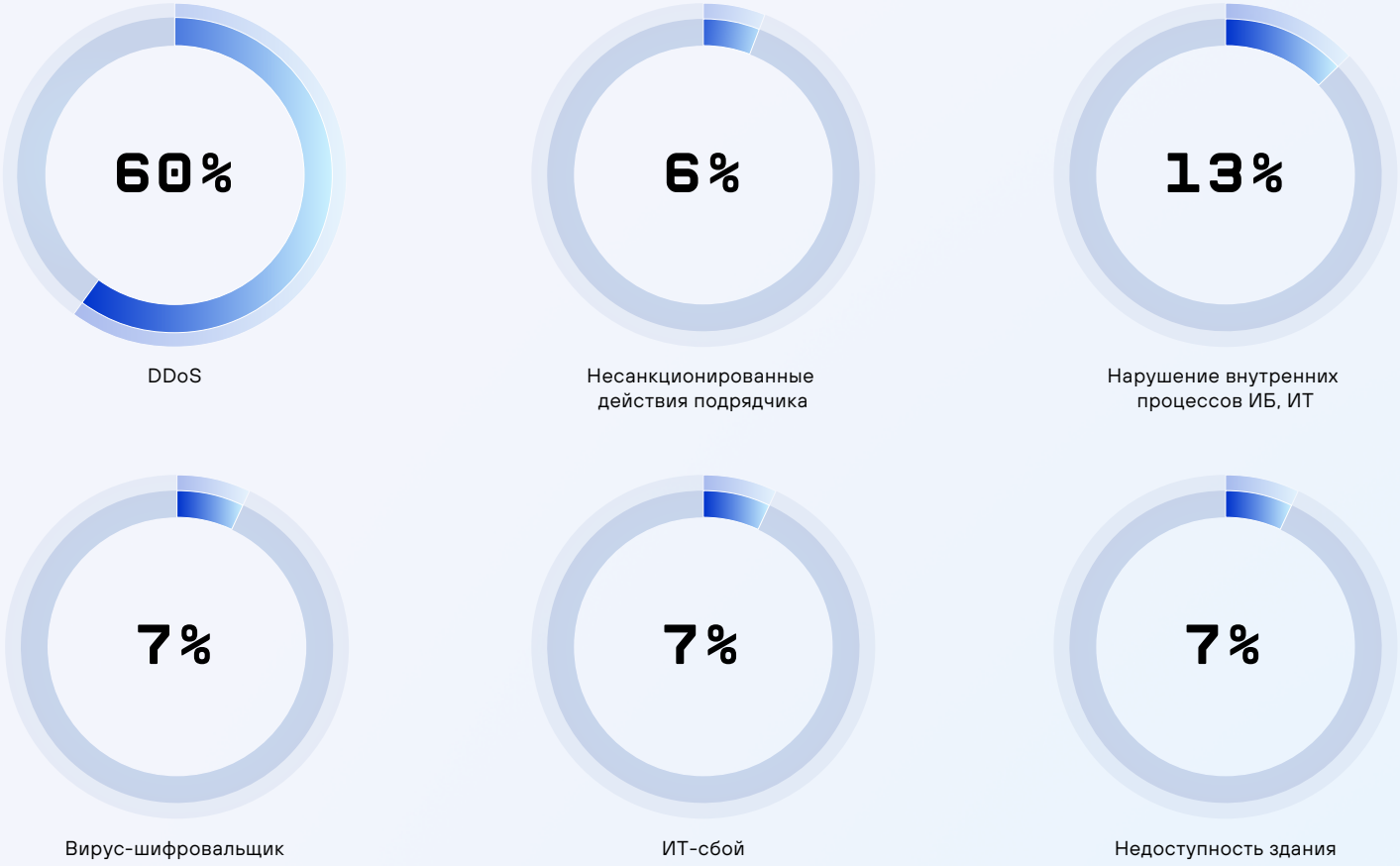
Каких рисков прерывания бизнеса больше всего опасается компания?



Изменение обусловлено ландшафтом киберугроз: более 40% компаний простаивали из-за инцидентов, большинство из которых составили классические угрозы ИБ: атаки вирусов-шифровальщиков, атаки на эксплуатацию доверия и DDoS.

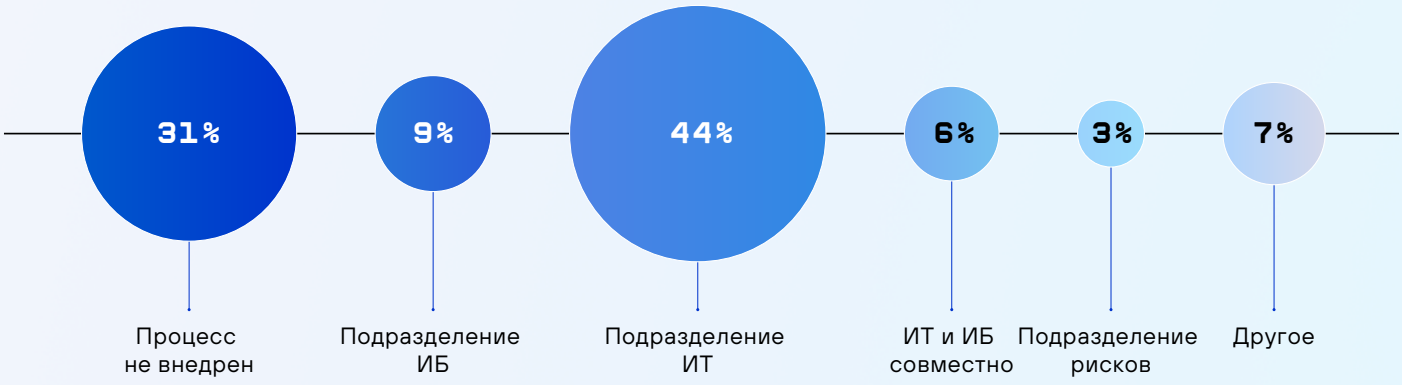
Согласно опросу, причины инцидентов, повлекших остановку бизнеса, следующие:

Причины инцидентов, повлекших остановку бизнеса



Ответом на это может быть применение практик непрерывности бизнеса, которые частично или полностью внедрены более чем в 60% компаний, но все еще остаются незрелыми. В 40% компаний не определено целевое время восстановления, а в 56% нет разработанного плана реагирования на кризис, что снижает эффективность процесса реагирования в случае реализации инцидента. Подразделения ИТ остаются традиционным владельцем практик непрерывности.

Какое подразделение в компании ответственно за обеспечение непрерывности бизнеса

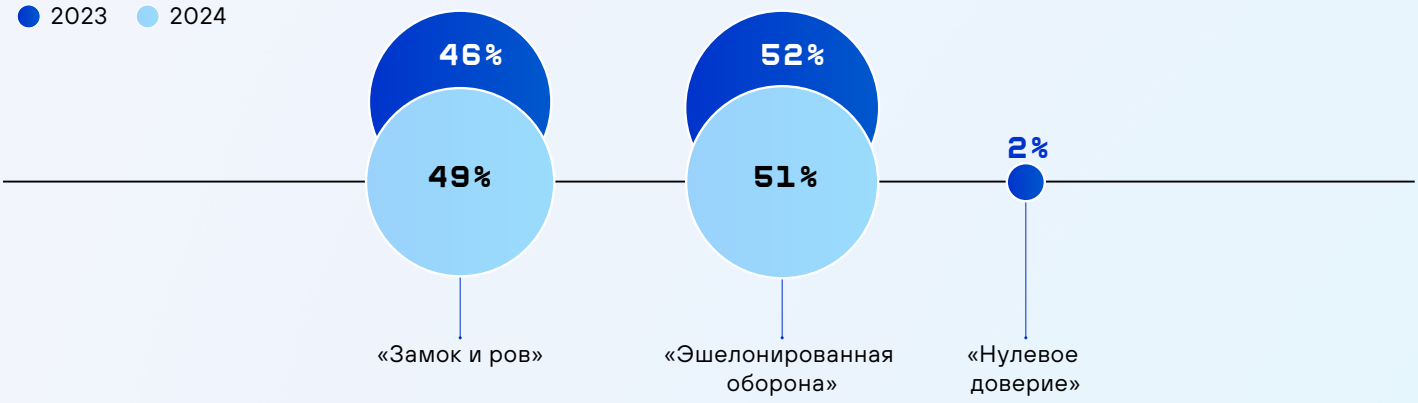


При этом мы не наблюдаем синергии между ИТ и ИБ в таких вопросах, что является зоной, требующей улучшений в рамках киберустойчивости.

Инциденты кибербезопасности в крупных компаниях, таких как СДЭК[12], «Верный»[13] и других, заставляют задумываться над вопросом «сможем ли мы сами восстановиться?». Это формирует запрос на независимую оценку действующих в компаниях планов. Так, спрос на услуги тестирования Disaster recovery и Business continuity планов увеличился более чем на 30%, а самым частым тестируемым сценарием был выбран сценарий успешной атаки вируса-шифровальщика. В рамках таких тестирований особое внимание уделяется проверке кризисного реагирования и вовлеченности ключевых лиц, принимающих решения, в процесс управления кризисом в формате настольного тестирования (tabletop exercise).

Правильная архитектура кибербезопасности является фундаментальным компонентом киберустойчивости. Она определяет, как компания обеспечивает защиту, функционирует во время и восстанавливается после кибератак.
По результатам опроса ситуация в отечественных компаниях остается неизменной. Организации отдают предпочтения устаревшей модели «Замок и ров»[14] и модели «Эшелонированная оборона»[15]:

Используемая архитектурная модель ИБ



[12] https://www.vedomosti.ru/business/articles/2024/05/28/1039828-prichinoi-sboya-v-rabote-sdek-mog-stat-virus-shifrovalschik

[13] https://www.kommersant.ru/doc/6744686

[14] Основной принцип модели — сосредоточить усилия преимущественно на защите периметра сети.

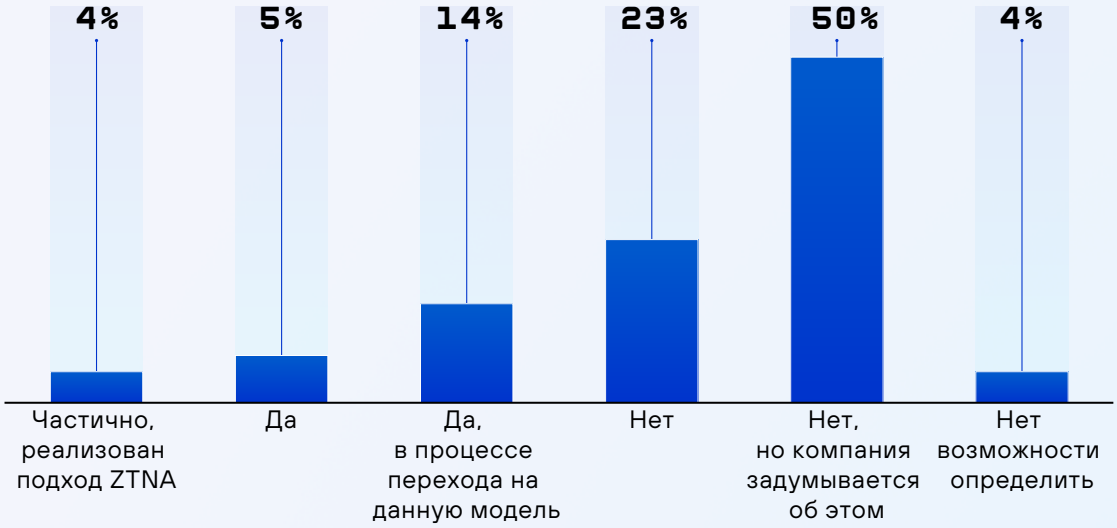
[15] В отличие от модели «Замок и ров» акцент делается на создании нескольких слоев безопасности, которые дополняют друг друга.

Опыт 2024 года показывает недостаточную эффективность стратегии «укрепляем существующие рубежи» для достижения киберустойчивости. Решением могла бы стать концепция Zero Trust, но на сегодняшний день лишь один принцип модели может быть полноценно реализован: доступ к сети с нулевым доверием (Zero Trust Network Access, ZTNA), а компаний, рассматривающих Zero trust как целевую архитектурную модель, мало.

В сложившихся обстоятельствах компании все чаще проектируют гибридные (переходные) архитектуры, добавляя к статичным эшелонам защиты практики ZT и киберустойчивости.

Zero Trust опирается на механизмы динамического управления доступом к данным и приложениям. Это требует сбора и анализа больших объемов данных, необходимых для принятия решения. Современные приложения не поддерживают динамических политик доступа, это потребовало бы их полной переработки (Zero Trust Enabled App). Для сбора контекстных данных о пользователях, их устройствах, инфраструктуре, приложениях и т.д. (Zero Trust Metrics & Orchestration) отсутствуют полноценные аналоги / решения только развиваются: EMM, UEBA, CASB, NAC и др. Доступ к сети с нулевым доверием (Zero Trust Access), напротив, уже реализуем, и многие компании рассматривают эту технологию как трендовую

Планируется ли переход на модель Zero Trust



К ключевым практикам киберустойчивости можно отнести Secure by Design — подход, при котором безопасность закладывается на этапе проектирования, а также построение устойчивой и безопасной ИТ-инфраструктуры, способной противостоять современным угрозам. Кроме того, важную роль играет харденинг, повышающий защищенность организации за счет правильных настроек безопасности, который позволяет замедлить или остановить злоумышленника при его попытках продвижения внутри инфраструктуры. Эти меры в совокупности помогают компании увеличить время, необходимое злоумышленнику для успешной атаки (TTA[16]), и сократить время реагирования и локализации инцидентов (TTR[17]).

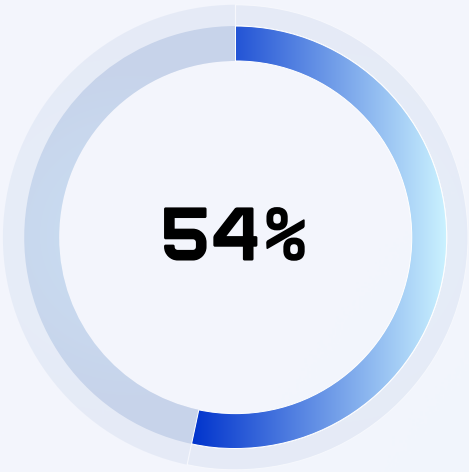
[16] TTA (time to attack) — время от получения первоначального доступа до начала выполнения вредоносных действий.

[17] TTR (time to respond) — время до завершения реагирования.

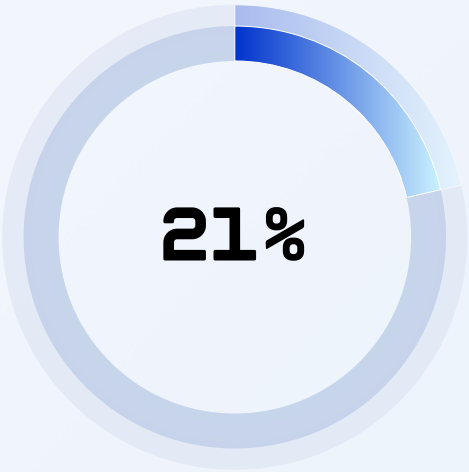
Лидером по использованию харденинга привычно выступает финансовая отрасль. Это объясняется в том числе высокой зарегулированностью, например, наличием требований по конфигурированию в стандарте PCI DSS. В целом же на практике процесс харденинга отсутствует более чем в половине компаний.

Харденинг — эффективный способ дополнительного усиления защиты технических и программных средств путем их настройки. В усиление защиты входит отключение неиспользуемых функций, изменение настроек по умолчанию и внесение изменений, повышающих защищенность систем (изменение прав доступа, включение и настройка дополнительных встроенных механизмов защиты)

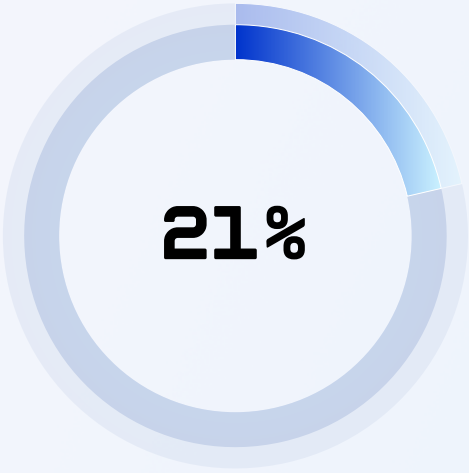
Существует ли в компании практика настройки компонентов ИТ-инфраструктуры в соответствии с лучшими практиками по безопасности?



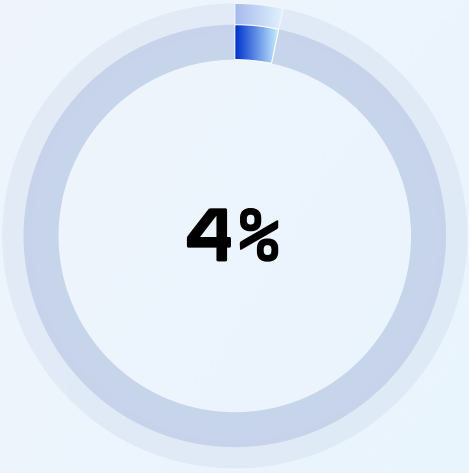
Нет, мероприятия по безопасной настройке не проводятся



Да, утверждены стандарты конфигурирования, аудиты не проводятся



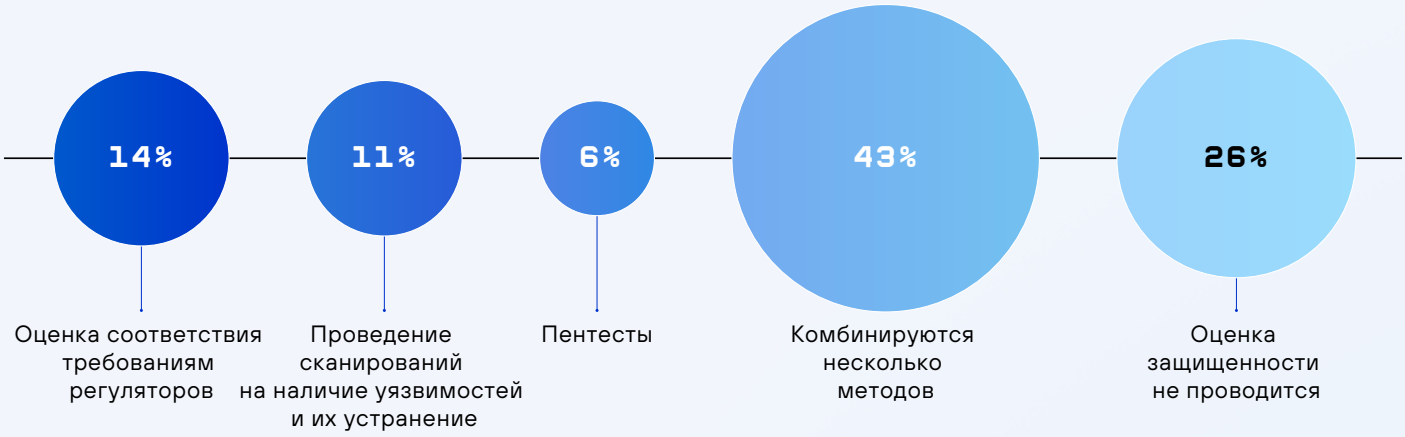
Да, утверждены стандарты конфигурирования и проводятся регулярные аудиты



Другое

Для проверки киберустойчивости важно реализовать систематические практические проверки, желательно применяя симуляции атак вместо зачастую формальных внутренних аудитов. Около трети компаний до сих пор не используют какие-либо методы оценки защищенности, самый популярный ответ: комбинирование нескольких методов.

Какие методы оценки защищенности используются в компании?

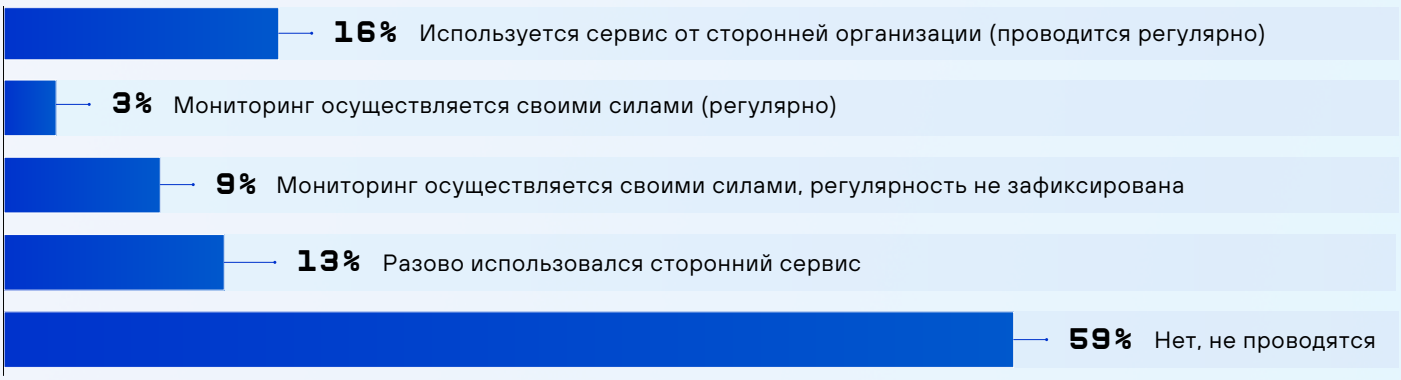


Единичные компании уже инициируют в том числе программы Bug Bounty, однако практика еще не стала массовой, потому что для ее успешного внедрения нужен высокий уровень зрелости компании в вопросах кибербезопасности. Не все организации готовы к этому: нужно иметь четкие процессы, ресурсы для анализа найденных уязвимостей и возможность оперативно их устранять.

Bug Bounty — это программа, в которой компании вознаграждают специалистов за выявление уязвимостей и ошибок в их программном обеспечении, продуктах или инфраструктуре

Помимо выстраивания киберустойчивой внутренней инфраструктуры ключевой практикой киберустойчивости является проактивное управление защищенностью за пределами корпоративной сети. Одной из таких практик является мониторинг даркнета с целью выявления потенциальных угроз, утечек данных или информации, связанной с кибератаками. Мы фиксируем рост интереса к киберразведке и другим методам защиты вне ИТ-периметра: около 15% компаний уже используют такие сервисы для защиты своих активов, 13% пилотировали сервис.

Проводятся ли в компании работы по мониторингу теневых ресурсов?

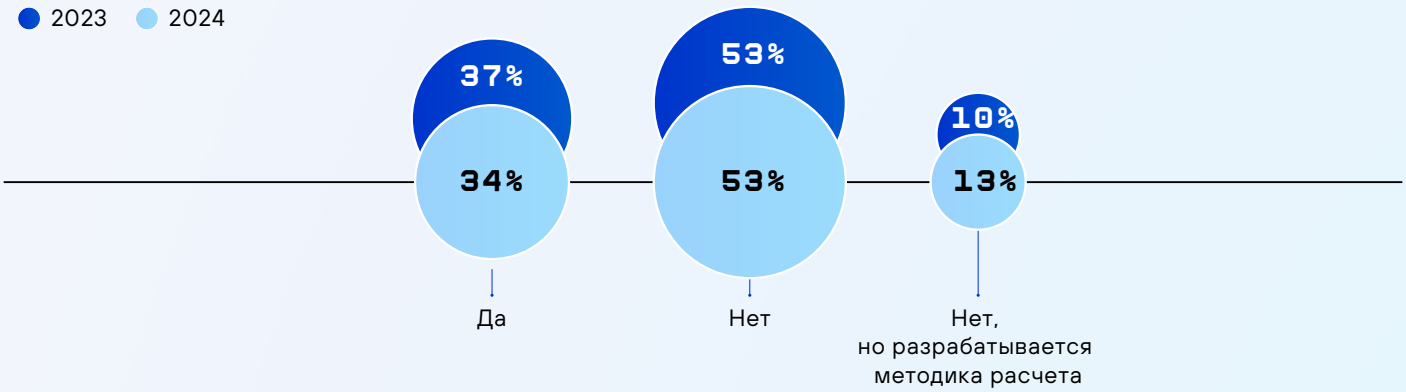


УПРАВЛЕНИЕ РИСКАМИ

Чтобы представить топ-менеджменту кибербезопасность как стратегическое направление, которое напрямую влияет на бизнес-показатели и способствует сохранению конкурентоспособности, необходим выбор подходящей системы оценки рисков. Правильная модель, учитывающая зрелость риск-ориентированного подхода в компании, доступность исторических данных, цели оценки, помогает расставить приоритеты руководителю службы ИБ и позволяет менеджменту принимать более обоснованные решения.

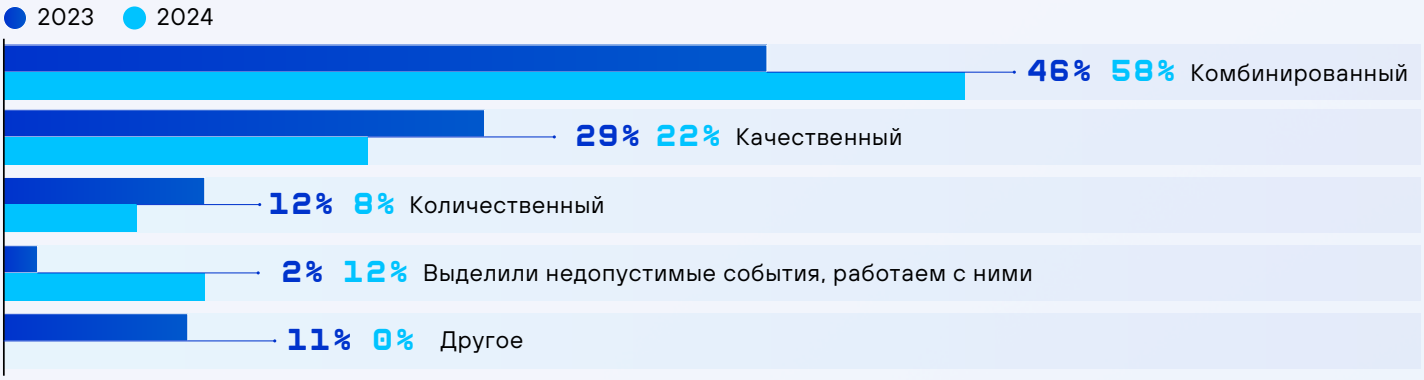
Среди множества подходов наиболее показательными для менеджмента являются экономические аргументы, демонстрирующие реальную цену бездействия. Однако количественный метод является сложным, требует навыков расчета прямых и косвенных потерь от инцидентов, поэтому используется руководителями ИБ крайне редко (8% опрошенных). Только 34% компаний считает ущерб от инцидентов в деньгах, еще 13% разрабатывают методику расчета такого ущерба — данные практически не изменились с 2023 года. Отрасли, где чаще всего считают риски в деньгах, — финансовые компании, ритейл и крупная промышленность.

Проводится ли расчет ущерба от инцидентов в деньгах?



В основном руководители ИБ отдают предпочтение качественным шкалам (высокий — средний — низкий) или комбинированным методам, которые сохраняют популярность с 2023 года.

Метод оценки рисков ИБ

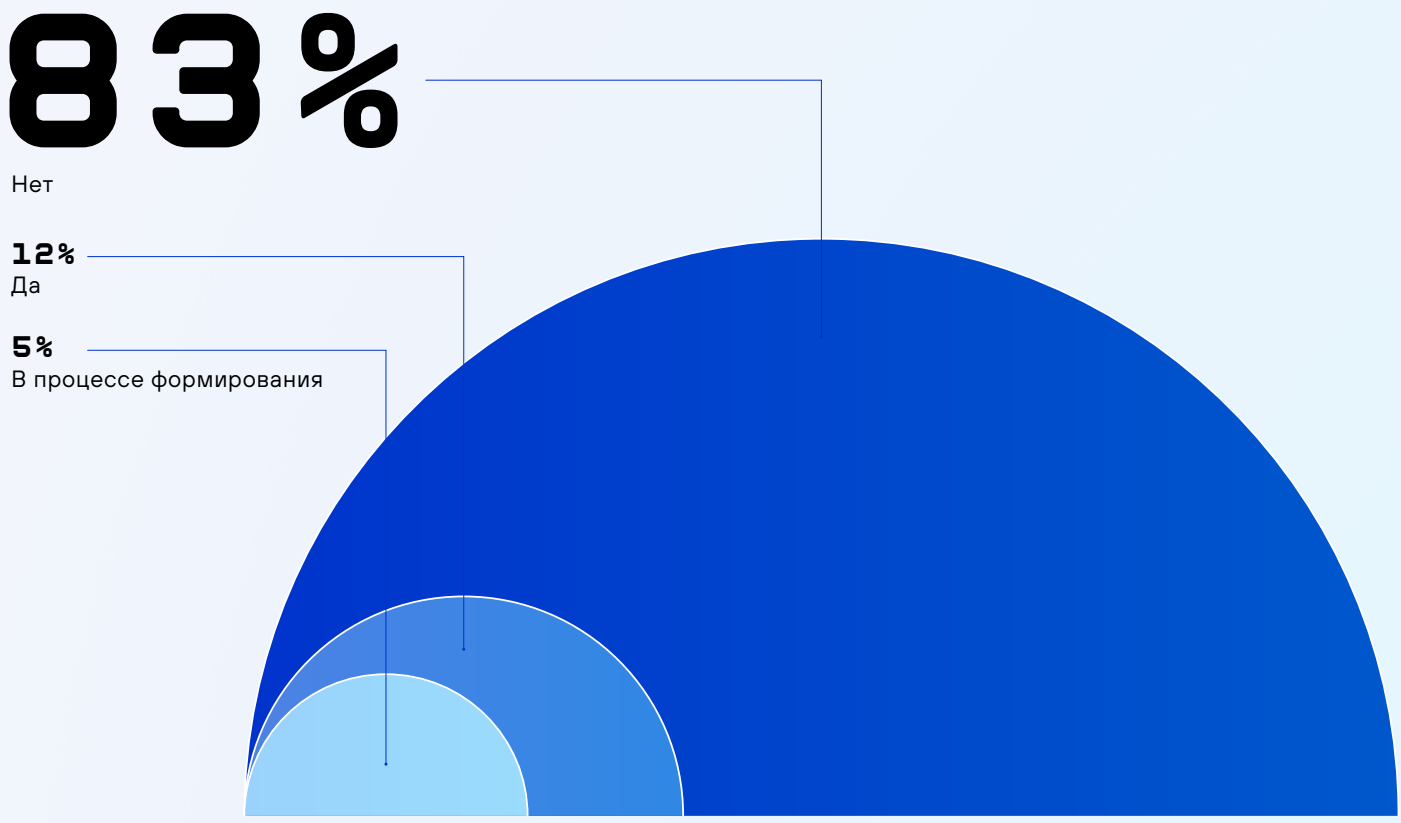


Мы наблюдаем тенденцию к упрощению процесса оценки: использование вместо традиционных матриц рисков более бинарных методов — сценарный анализ или определение недопустимых событий (НС).

Среди опрошенных руководителей ИБ 12% уже определили перечень недопустимых событий, еще 5% планируют это сделать в ближайшее время.

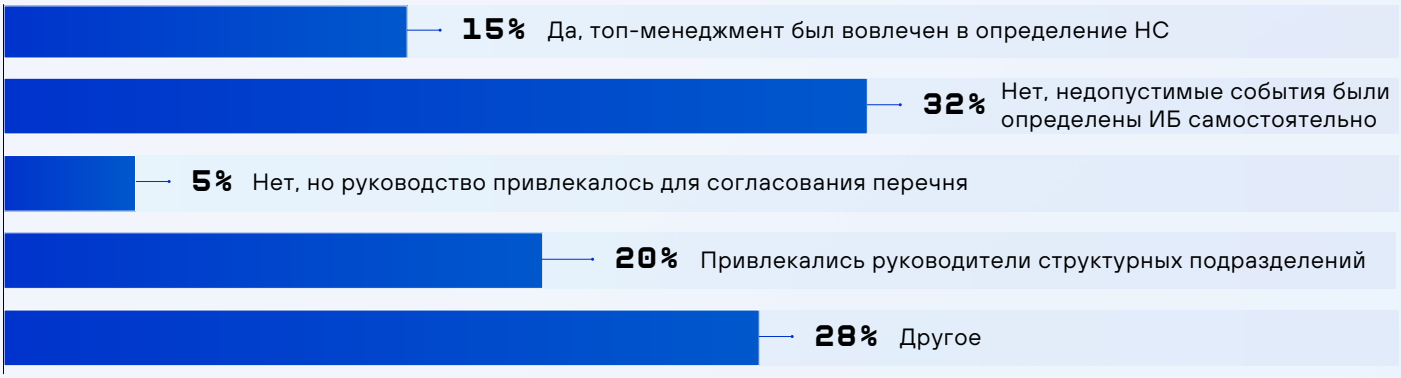
Смещение фокуса на недопустимые события ИБ с 2022 года вызвано рядом законодательных инициатив, таких как Указ Президента РФ №250 от 01.05.2022. С 2023 года от экспертного сообщества также появились реестры типовых недопустимых событий, а также информационные порталы с методической поддержкой

Компании, которые определили для себя недопустимые события



Методика определения недопустимых событий в качестве начального этапа предполагает проведение серий интервью с руководителями компании, чтобы заручиться их поддержкой. Однако только 15% опрошенных нами руководителей ИБ вовлекали топ-менеджмент в определение НС — в основном недопустимые события определялись самостоятельно (32%) с последующим согласованием или только с привлечением руководителей структурных подразделений (20%).

Привлекалось ли руководство компании для определения недопустимых событий?



Еще одной тенденцией стало повышение интереса к страхованию как методу управления киберрисками, сам же рынок страхования от киберрисков в России слабо развит по сравнению с объемом мирового рынка киберстрахования, достигающего, по разным источникам, от $15 млрд до $20 млрд. Только 1% опрошенных нами компаний имели страховой полис для защиты от кибератак и утечек со страховым покрытием не более 5 млн рублей. Большая часть опрошенных не считает такое страхование целесообразным.

Помимо управления собственными рисками, с конца 2023 года на первый план выходит важность управления рисками третьих сторон. В 17% расследованных нами инцидентов в 2024 году мы фиксировали подозрение на компрометацию поставщиков услуг: в основном атакующие использовали взломанные учетные записи компаний малого и среднего бизнеса, оказывающих сервис жертве.

Мы провели сравнительный анализ данных, полученных в ходе исследования риска эксплуатации доверия (2022–2023), с данными аудитов и опросов российских компаний в 2024 году.

Анализ показывает, что компании начали проводить более серьезную оценку безопасности подрядчиков на этапе заключения договоров и регулярно пересматривают их статус. Все большую популярность набирают сервисы анализа поверхности атак своих подрядчиков, позволяющие выявлять уязвимые места еще до того, как они станут целями злоумышленников.

Оцениваете ли вы уровень риска ИБ поставщиков до начала взаимодействия?	2024 год	2022-2023 годы
Проводим свой/независимый аудит для критичных поставщиков	36%	17%
Проводим только проверку по линии СБ	48%	68%
Третьи лица заполняют анкету с вопросами по ИБ	16%	15%

Кроме того, компании внедряют политики взаимодействия с подрядчиками, закрепляющие процедуры по минимизации рисков, уходя от «размазанных» по документам общих правил передачи информации.

Формализован ли процесс безопасного взаимодействия с поставщиками?	2024 год	2022-2023 годы
Есть отдельный документ, детализирующий меры безопасности при работе с поставщиками	48%	19%
Есть требования только по безопасной передаче информации поставщикам	42%	71%
Нет или в процессе разработки	10%	10%

ОЦЕНКА СВОЕГО УРОВНЯ ИБ И ОТЧЕТНОСТЬ

Оценка уровня ИБ компании и регулярная отчетность помогают корректировать курс развития кибербезопасности, а также обеспечивают прямой диалог с бизнесом, отражая динамику развития функции ИБ (стала ли компания защищеннее, эффективно ли тратится бюджет и пр.).

Отчетность является обязательным атрибутом для всех компаний, достигших минимального уровня зрелости процессов ИБ — «повторяемого»[18]. Практически все компании предоставляют отчетность ИБ на уровень руководства компании C-level. В целом показатель по подготовке и отправке отчетности в сравнении с 2023 годом изменился незначительно: в 2023 году 80% компаний формировали отчетность, в 2024 году — 85%.

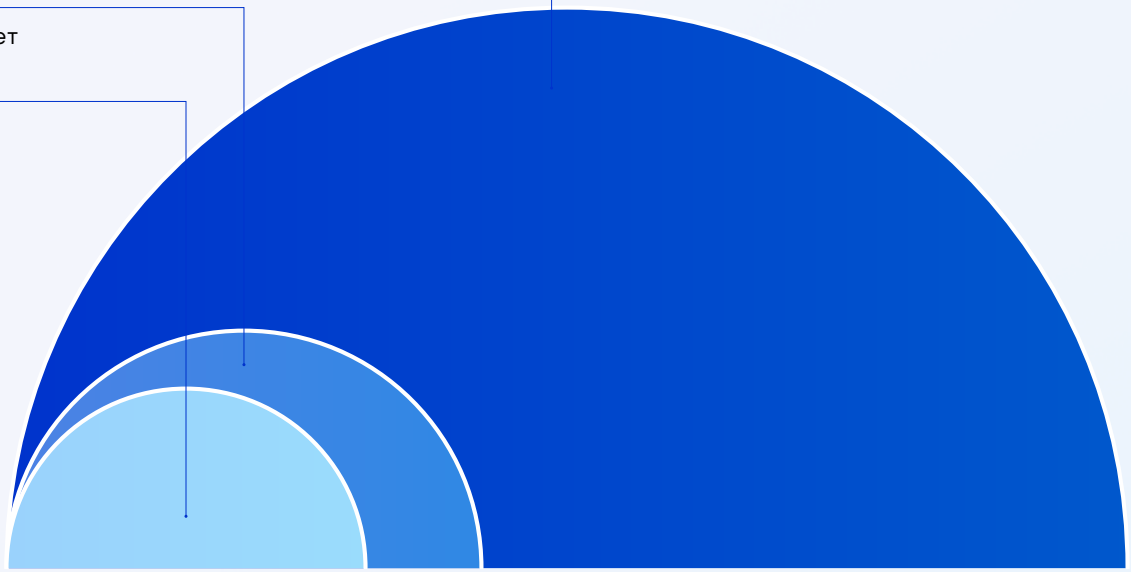
[18] В соответствии с моделью совершенствования процессов CMMI (Capability Maturity Model Integration).

Адресаты отчетности по результатам работы службы ИБ

78%
Руководство компании (C-level)

14%
Отчетность отсутствует

8%
Остается на уровне подразделения, руководству выше не передается



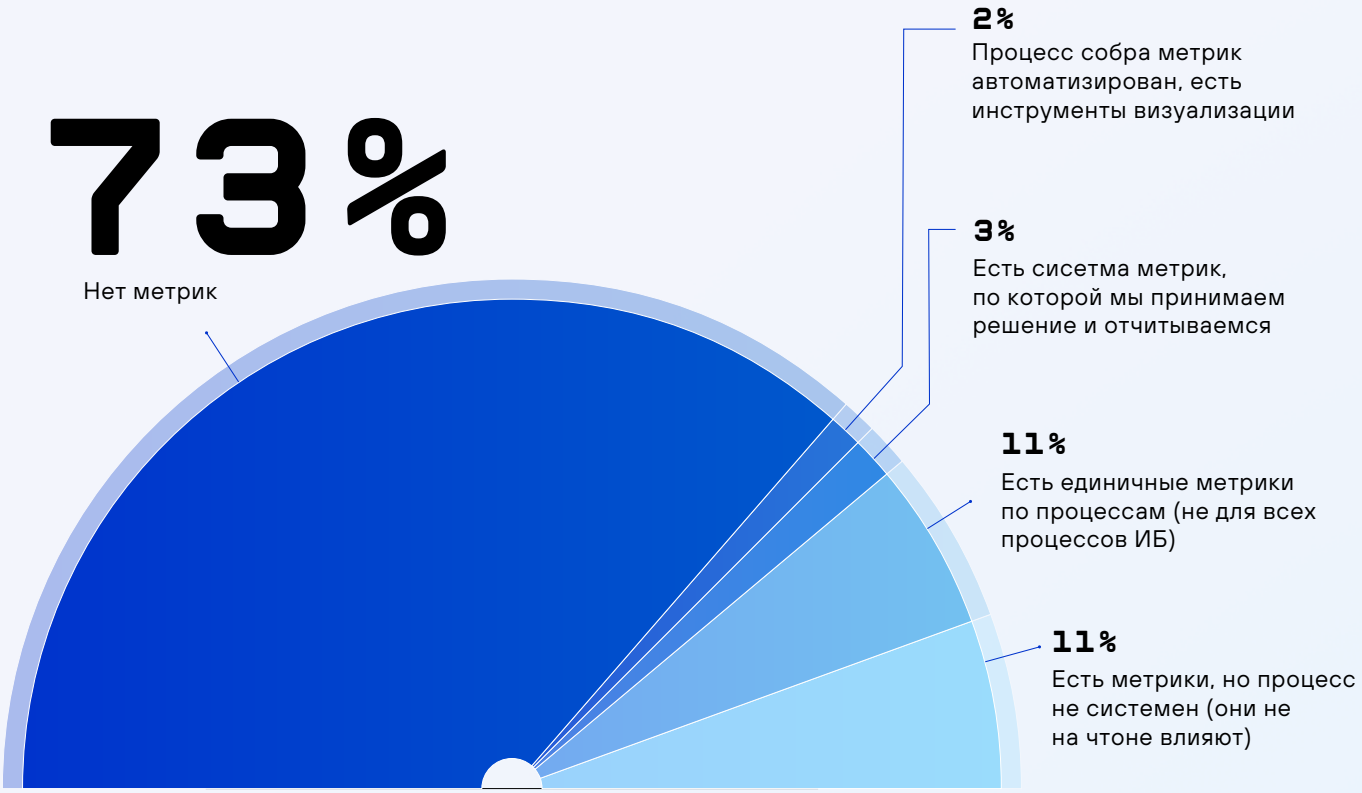
Периодичность подготовки отчетности ИБ для руководства сохраняет тренд 2023 года: в основном отчетность формируется и предоставляется руководству ежеквартально, часть компаний делает это раз в год либо при наступлении инцидента или по запросу.

Отчетность ИБ для руководства чаще предоставляется либо в виде короткой сводки основных данных, либо в формате нескольких слайдов с ключевой статистикой, метриками и информацией в составе общей отчетной презентации, которая наглядно показывает текущий статус ИБ в компании. По нашему опыту, в компаниях с развитой аналитической культурой, где бизнес активно использует BI-системы, ИБ также может иметь отдельные дашборды в таких системах, что удобно с точки зрения отслеживания динамики развития, однако такая практика до сих пор встречается редко.

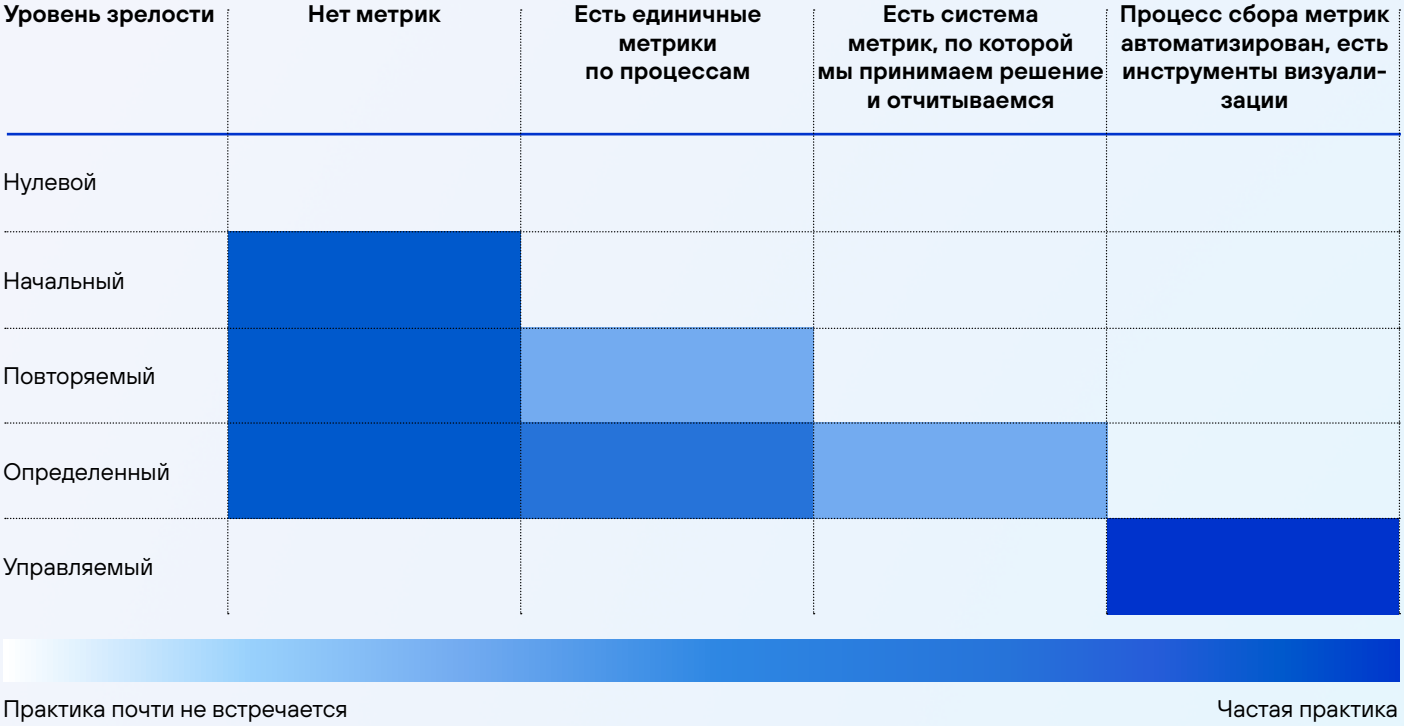
Все больше компаний начинают уходить от демонстрации в отчетности локальных успехов и результатов устранения недостатков из отчетов по результатам аудитов в сторону сбора метрик,пусть и без выстроенного системного процесса. И хотя количество таких компаний до сих пор невелико (у 73% компаний нет метрик для отслеживания эффективности ИБ), мы отмечаем тренд на постепенное изменение ситуации в лучшую сторону.

В основном компании начинают собирать метрики с «определенного» уровня зрелости ИБ, то есть когда имеют достаточные ресурсы для оперативного управления процессами ИБ, программу развития ИБ на несколько лет, разработанную документацию и пр.

Наличие в компании метрик для отслеживания эффективности ИБ



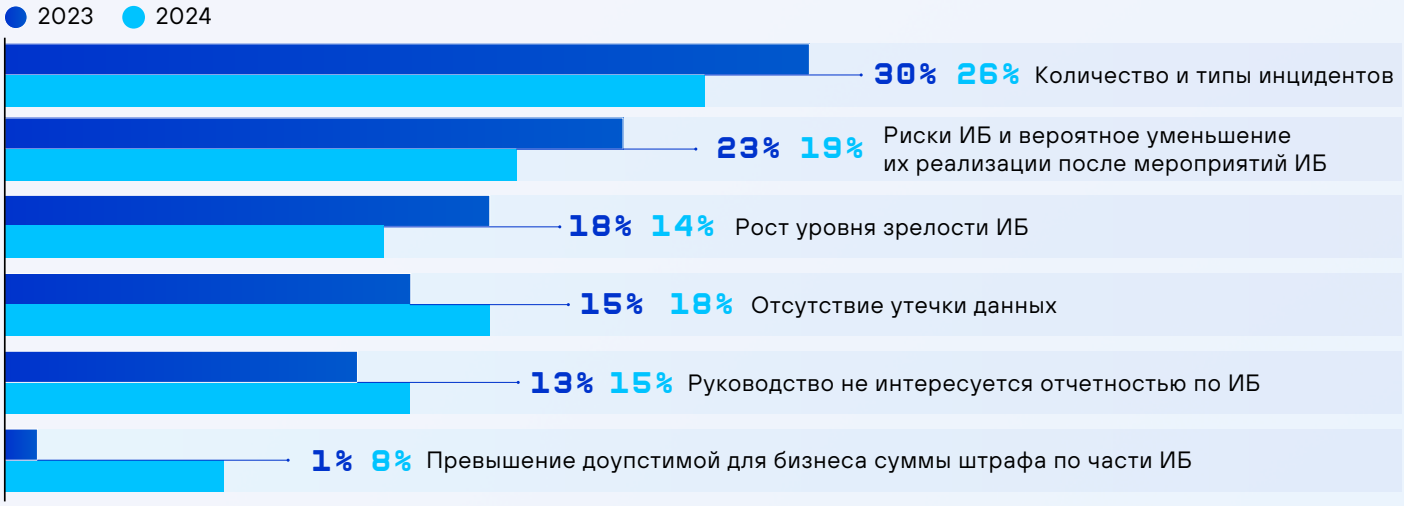
Зависимость между уровнем зрелости компании и выстроенной системой метрик



Интерес к метрикам связан с желанием топ-менеджмента связать успехи руководителей ИБ и бизнес-результаты компании. Руководство хочет видеть метрики, которые позволят оценить эффективность стратегии развития и окупаемость инвестирования в ИБ, понять уровень защищенности компании и потенциальные риски.

В 2024 году руководство компаний аналогично 2023 году также интересовала информация об инцидентах (их количестве и типах), динамике обработки рисков ИБ. Показатели заинтересованности руководства в отсутствии утечек данных и превышения допустимой суммы штрафа выросли в сравнении с прошлым годом, что объясняется усилением регуляторных санкций в случае допущения такого инцидента.

Показатель, наиболее интересующий руководство компании

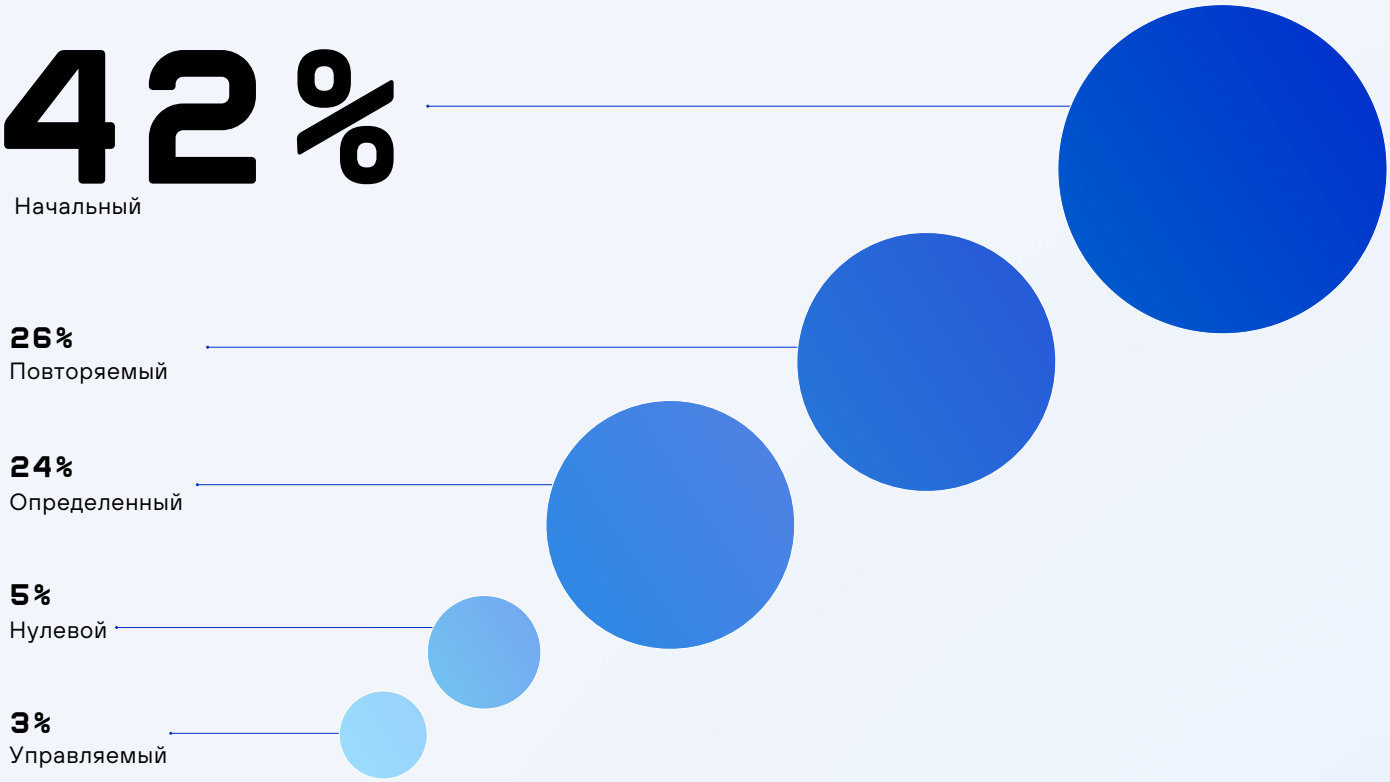


Для понимания того, насколько защищена компания, со стороны руководства стали чаще поступать запросы на helicopter-view-состояния ИБ («быстрые аудиты») с использованием моделей оценки уровня зрелости (CMMI и аналогичные). Такой инструмент в связке с перечнем критичных недостатков позволяет наглядно (хоть и верхнеуровнево) продемонстрировать уровень зрелости и отслеживать его в дальнейшем, выделить области улучшения и предоставить руководству информацию о состоянии ИБ компании в понятном и структурированном виде.

Запрос на проведение «быстрых аудитов» в том числе сформировался в дочерних компаниях крупных холдингов, которые либо только появились, либо существовали долгое время без собственного ИБ. Такие компании начинают постепенно выстраивать ИБ-процессы, и ключевая задача команды ИБ — быстро заложить фундамент для дальнейшего развития ИБ без детального аудита, который избыточно проводить с учетом отсутствия базовых решений и культуры ИБ в целом.

Уровень зрелости процессов ИБ (в соответствии с методикой CMMI) опрошенных нами компаний распределился между «начальным» и «повторяемым». Компании с уровнем «определенный» и выше составляют около трети выборки.

Уровень зрелости процессов ИБ в компаниях



КИБЕРКУЛЬТУРА

Киберкультура играет ключевую роль в обеспечении кибербезопасности, формирует осознанность, ответственность и поведенческие нормы, которые напрямую влияют на киберустойчивость компании в целом.

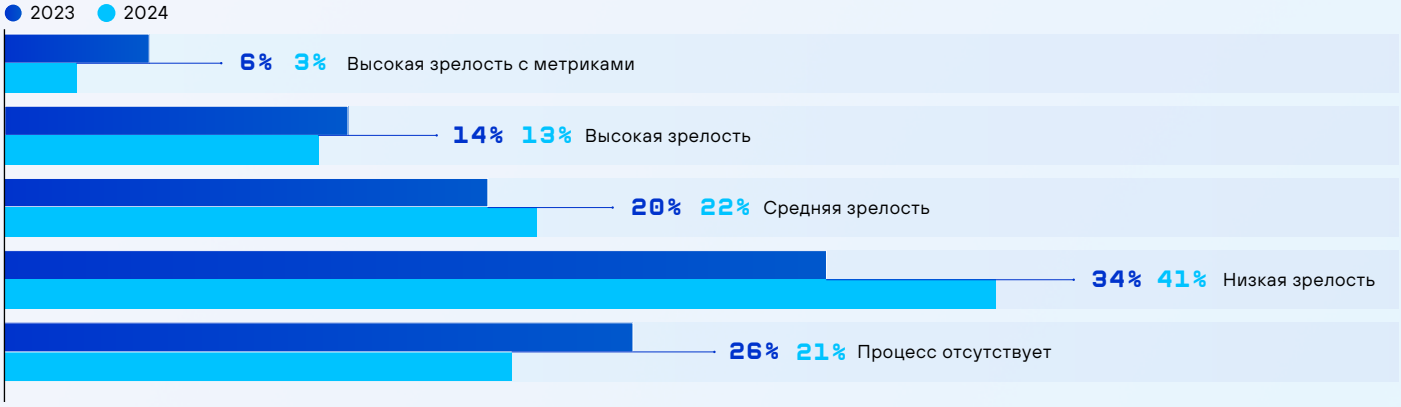
Согласно опросу, в 2024 году человеческий фактор снова стал самой популярной причиной взлома инфраструктуры: инциденты по вине пользователей произошли в четверти опрошенных компаний. При этом компании продолжают полагаться на устаревшие подходы к обучению: инструктажи при приеме на работу, формальные тесты и рассылки. Такие методы часто неэффективны, потому что не вовлекают сотрудников, не содержат живые и близкие человеку примеры и неинтерактивны.

В топ-3 мероприятий по повышению осведомленности вошли как раз такие «традиционные» подходы: периодические почтовые рассылки о правилах ИБ (28%), ознакомление с документацией по ИБ (22%) и прохождение курсов (21%).

Способы повышения осведомленности работников в области ИБ

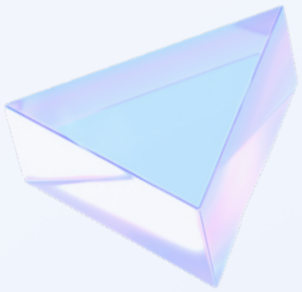
В большинстве компаний уровень зрелости процесса повышения осведомленности либо отсутствует, либо оценивается как низкий (62%) — это значение не изменилось с 2023 года. На таких уровнях обучение, как правило, проводится больше для выполнения требований законодательства — формально, несистемно, без адаптации контента под аудиторию.

Оценка уровня зрелости процесса повышения осведомленности в компаниях[19]

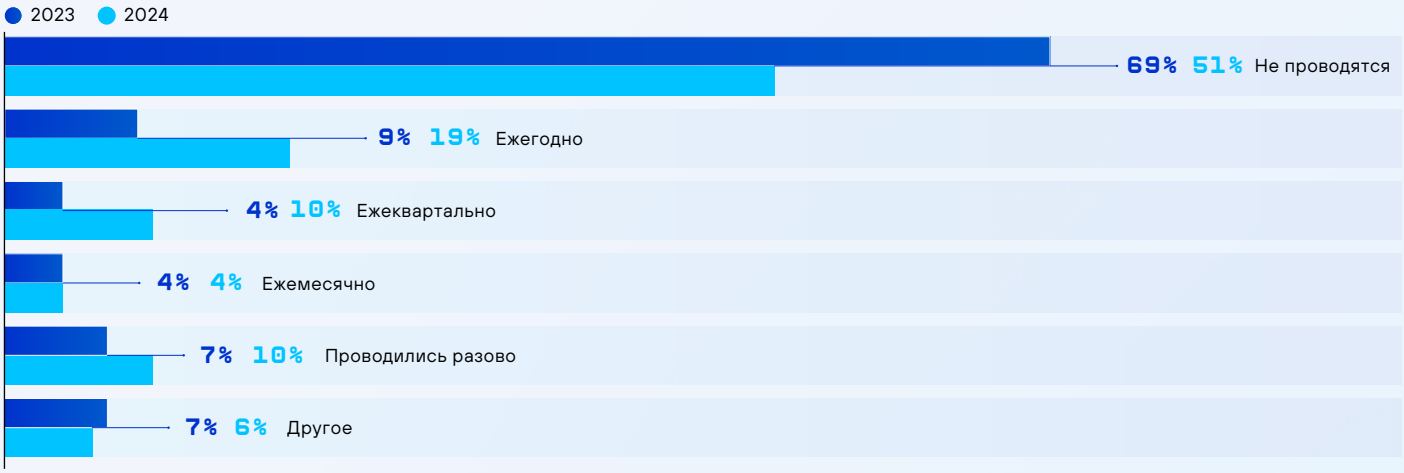


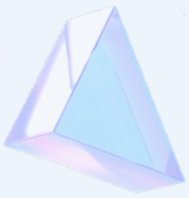
[19] При опросе была использована методика оценки уровня процесса повышения осведомленности в соответствии с SANS

Злоумышленники активно развивают методы фишинговых атак: применяют искусственный интеллект, QR-фишинг, используют личные мессенджеры и социальные сети для deepfake-атак. В 2024 году мы отмечаем рост числа компаний, которые хотя бы раз проводили учебные фишинговые рассылки, чтобы противостоять таким атакам: 49%, что на 18% выше показателя 2023 года. При этом число компаний, которые делают это на системной основе, невелико: чаще всего компании выбирают ежегодный формат проведения учений (19%), что не является эффективным, 15% организаций проводит их чаще одного раза в квартал.



Частота проведения эмуляции фишинговых атак





JET
SECURITY
TEAM

security@jet.su
jetcsirt.su