JET SECURITY TEAM

ИССЛЕДОВАНИЕ

СТРАТЕГИИ И РЕШЕНИЯ РУКОВОДИТЕЛЕЙ СЛУЖБ ИБ КОМПАНИЙ В 2023 ГОДУ

Инфосистемы Джет
JET.SU

АВТОРЫ

АЛЕКСАНДР МОРКОВЧИН

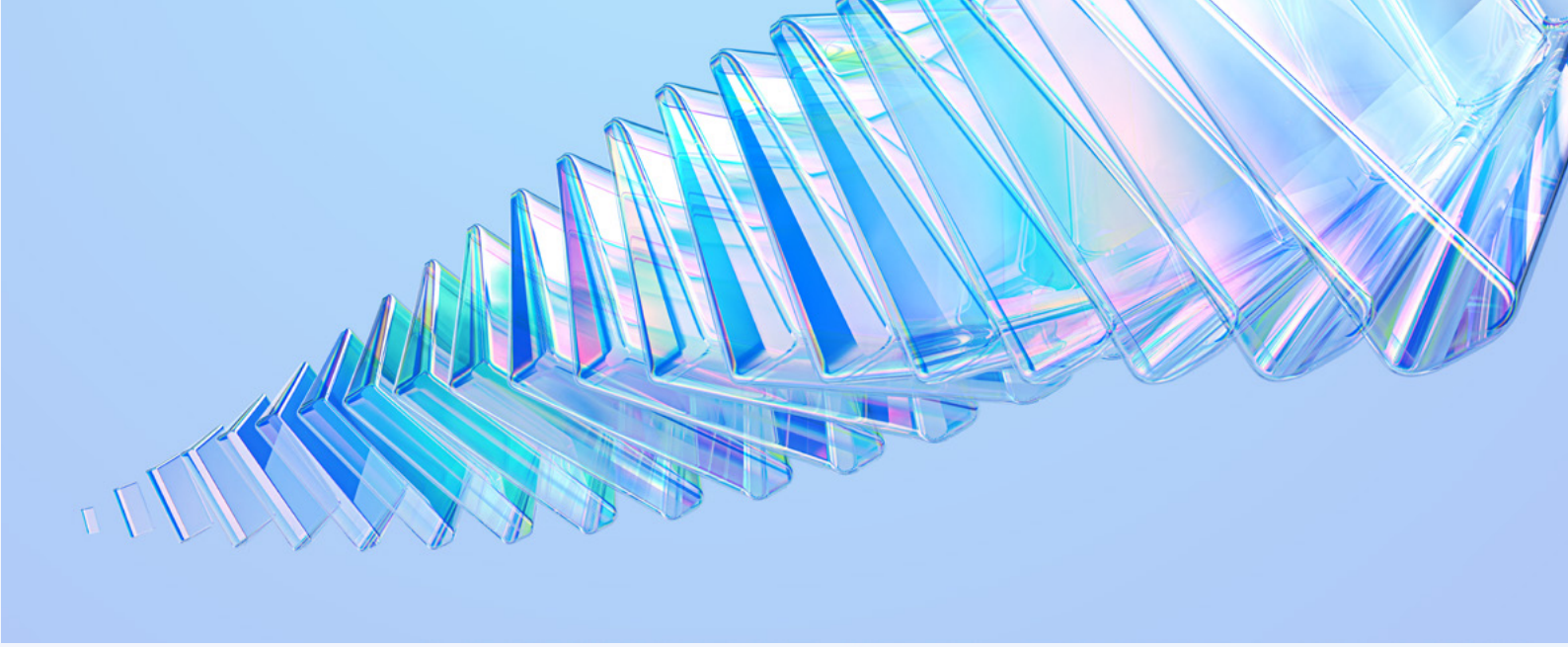
Руководитель группы департамента консалтинга центра информационной безопасности, «Инфосистемы Джет»

ЕЛЕНА АГЕЕВА

Ведущий консультант по информационной безопасности, «Инфосистемы Джет»

АСКАР МУСАЕВ

Консультант по информационной безопасности, «Инфосистемы Джет»



КЛЮЧЕВЫЕ ВЫВОДЫ

ДО 2-3 ЛЕТ

сузился горизонт планирования в ИБ. В 2023 году компании стали чаще выбирать краткосрочное планирование с непрерывным мониторингом результатов.

46%

компаний используют устаревшую модель защиты «Замок и ров», которая фокусируется только на внешнем периметре.

НА 10-20%

вырос бюджет на ИБ в 2023 году. Значительный рост (30–60%) показали компании финансового, топливно-энергетического, а также ИТ-сектора.

ТРЕТЬ

опрошенных не использует управление рисками для обоснования бюджета. 24% респондентов считают риски формально и 16% — «подгоняют» под свое видение.

64%

CISO выделяют большую часть бюджета на внедрение и модернизацию превентивных мер защиты.

В 48%

компаний отдел ИБ состоит из 5 и более работников, бизнес постепенно уходит от модели «один специалист-мультиинструменталист в штате».

ВВЕДЕНИЕ

2022–2023 годы стали переломными для руководителей служб информационной безопасности (CISO). Обострение геополитической ситуации и множество других (в том числе непрогнозируемых) факторов спровоцировали развитие российского рынка ИБ и потребовали формирования новых подходов к управлению кибербезопасностью. Наша команда провела исследование, чтобы понять, как CISO смотрели на изменение функции ИБ в 2023 году, с какими проблемами они сталкивались и насколько оказались готовы к преодолению кризисных ситуаций.

В исследовании собраны мнения CISO из 90 российских компаний, принадлежащих к разным сферам бизнеса. Мы задали респондентам вопросы по ключевым направлениям развития функции ИБ:

- Стратегический менеджмент (постановка и корректировка целей, формирование и защита бюджета на ИБ)
- Организация службы ИБ, поиск и развитие персонала
- Оценка собственной эффективности и составление отчетов для руководства
- Поддержание киберустойчивости и обеспечение непрерывности бизнеса
- Поддержание культуры 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. Эта 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). Вопросы были заданы в следующих областях:

- Общая информация о компании и подразделениях ИБ и ИТ
- Управление ИБ: стратегический и операционный менеджмент, бюджетирование, взаимодействие со

смежными подразделениями, подходы к выстраиванию процессов управления ИБ

- Направления защиты: киберустойчивость, управление инцидентами ИБ, повышение осведомленности персонала в сфере ИБ

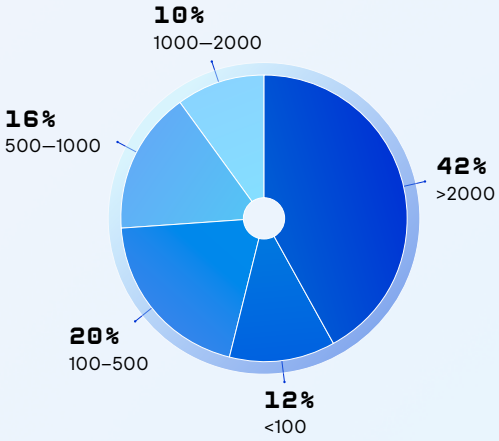
Краткая информация об участниках опроса

Сфера деятельности

В опросе приняли участие представители финансового, промышленного и топливно-энергетического сектора, ИТ-компании, организации из сферы здравоохранения, транспорта и ритейла.

Количество работников

Опрос проводился преимущественно в крупных компаниях с штатом от 500 работников (68%). Небольшие компании (до 500 работников, обычно в сфере ИТ) составили 32% выборки.

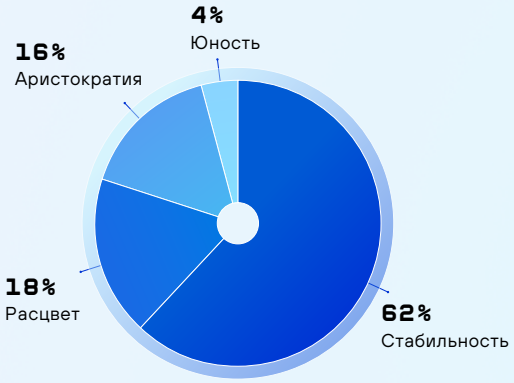


Тип компаний

Большинство опрошенных компаний является предприятиями холдингов (18% головных компаний и 54% дочерних). Отдельные и самостоятельные организации составляют 28% выборки.

Модель жизненного цикла

Подавляющее большинство компаний (62%) находится на стадии «Стабильность» по модели жизненного цикла Ицхака Адизеса — то есть чувствует себя на рынке достаточно уверенно.



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.

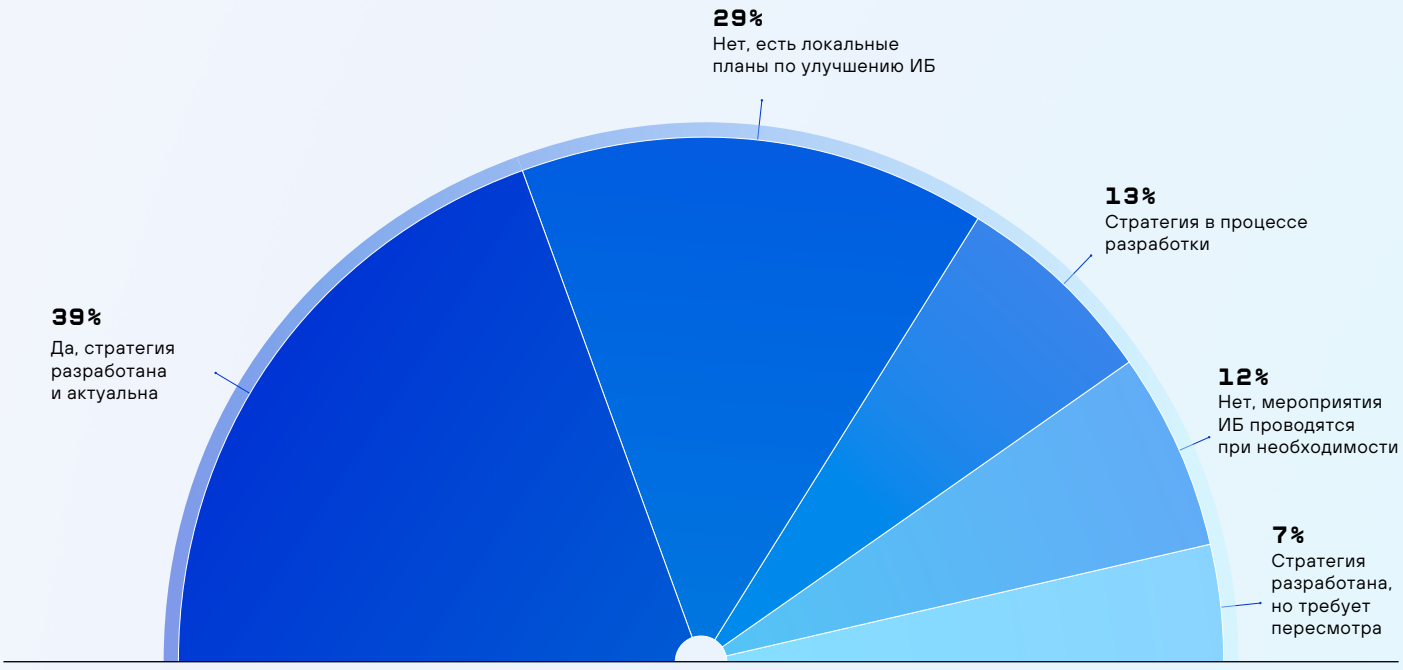
В исследование не включены результаты опроса компаний, находящихся на стадиях «Зарождение», «Младенчество» и «Высокая активность»: они ориентированы на быстрое и устойчивое развитие самого бизнеса, а не на безопасность. Также мы не опрашивали компании на стадиях бюрократизации и смерти.

СТРАТЕГИЧЕСКИЙ МЕНЕДЖМЕНТ

Ключевые задачи руководителя службы ИБ — выбор направления и способов развития функции ИБ, а также выработка стратегии, которая обеспечит это развитие. В 2023 году появилась необходимость сместить фокус на результативность и операционную эффективность подразделения («эффективнее используем то, что есть»). Это вынудило многие компании скорректировать долгосрочные планы развития: спрос на разработку стратегий ИБ вырос почти вдвое.

Ситуационный менеджмент как управленческий инструмент в большинстве случаев показал свою неэффективность — работа с последствиями, а не с причинами, и непоследовательность при планировании приводят к неоптимальным решениям. Такой вывод сделали 59% респондентов: они скорректировали свои долгосрочные планы в 2022–2023 годах или формировали их на момент опроса. В 41% компаний разработаны планы развития отдельных направлений или проекты реализуются по мере возникновения проблем.

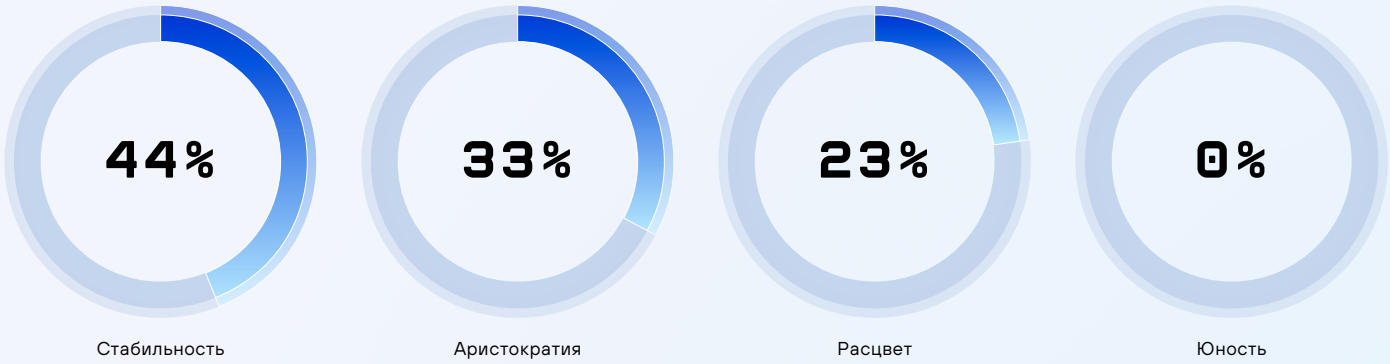
Наличие стратегии ИБ в компании



При этом потребность в разработке стратегии ИБ, как правило, возникала у компаний, достаточно уверенно чувствующих себя на рынке и стоящих на определенном этапе жизненного цикла (по модели Ицхака Адизеса)[1].

Обычно компании задумываются о стратегическом планировании на этапе расцвета (23% опрошенных), вместе с развитием общекорпоративного процесса стратегического менеджмента и уходом от ситуационного планирования. Бизнес большинства компаний (более 70%), имеющих стратегию ИБ, находится на стадии «плато» — стабильности. Ярко выраженная несистемность мероприятий ИБ характерна для компаний на стадиях «Младенчество» — «Юность».

Зависимость наличия стратегии ИБ от стадии жизненного цикла компании



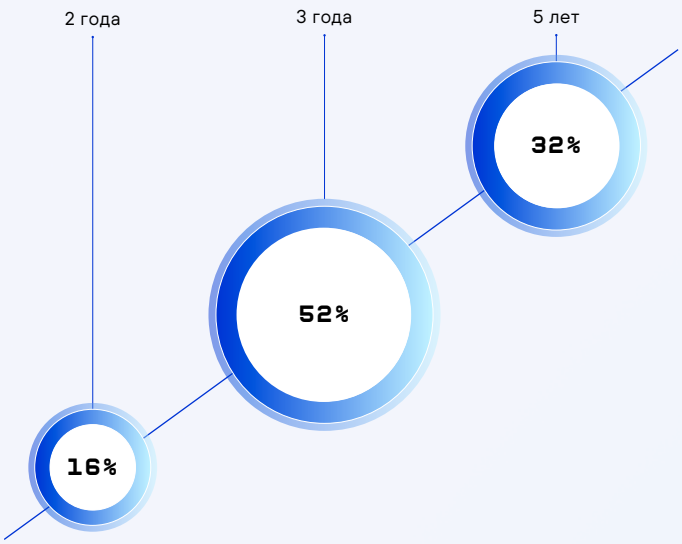
Прогнозирование даже на год вперед для многих CISO сегодня является сложной задачей. Начиная с 2021 года мы наблюдаем сужение горизонта стратегического планирования в ИБ до 2–3 лет. Принимая во внимание:

- ограничения в технологических и кадровых ресурсах,
- неопределенность политической ситуации,
- ускорение темпов развития ИТ и развития методов атаки,

компании чаще выбирали модель планирования короткими временными отрезками до года с непрерывным мониторингом ситуации. Так, половина опрошенных (52%) перешла с долгосрочного на среднесрочное планирование, только 32% формируют планы на 5 лет вперед.

[1] Описание модели приведено в разделе «Вводная часть».

Горизонт стратегического планирования в ИБ

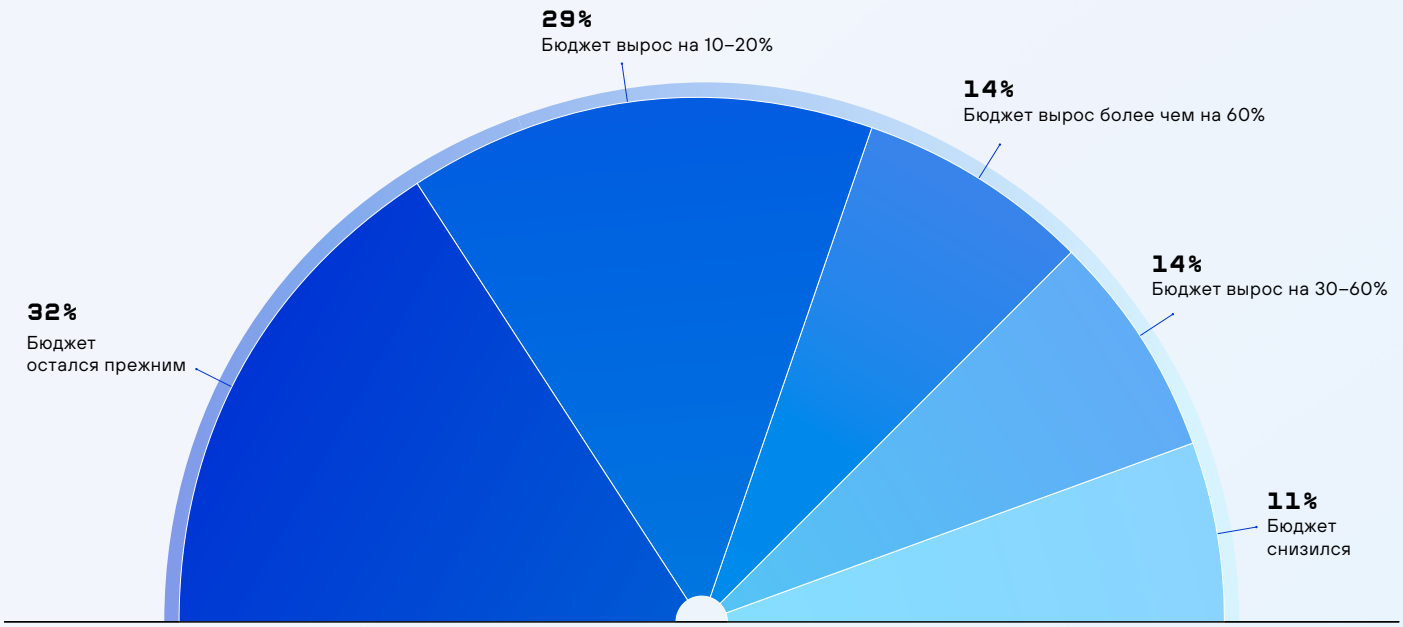


Тип действующей стратегии ИБ

Современный стратегический менеджмент в ИБ можно назвать осторожным. В условиях нестабильности компании склоняются к проверенным подходам к защите и базовым защитным мерам, стараются избегать дополнительных расходов на инновационные идеи — реализацию Zero Trust, киберстрахование и т. п. Так, более 61% респондентов, учитывая положительный опыт прошлых стратегических периодов, идут по пути обновления уже существующей стратегии, включающему корректировку целей и приоритетов. Только 23% опрошенных меняли стратегии кардинально. В основном такие стратегии являлись следствием старта ИТ-трансформации или выделения службы ИБ в отдельную сервисную компанию.

Средний бюджет на кибербезопасность в 2023 году демонстрировал умеренный рост. Треть опрошенных отметили увеличение бюджета на 10–20%, еще у трети он остался прежним. Значительный рост бюджета (30–60%) показали компании финансового и топливно-энергетического сектора, а также ИТ-компании.

Изменение бюджета на ИБ относительно прошлого года/лет



Большую часть бюджета руководители направляли на внедрение и модернизацию превентивных мер (межсетевые экраны, WAF, мультифакторная аутентификация, сегментация, антивирусная защита и т. п.). Примерно 30% компаний выделяли средства на обнаружение и реагирование, 8% — на проактивное обнаружение угроз (киберразведка).

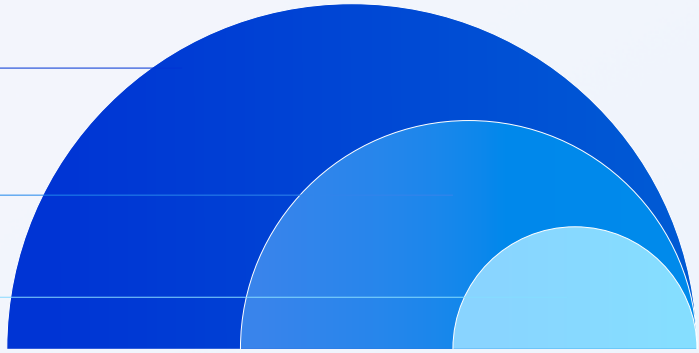
2023 год подсветил растущую необходимость для компаний активно анализировать и контролировать информацию за пределами внутренних сетей и обеспечивать системный контроль защищенности постоянно модернизируемой ИТ-инфраструктуры. Финансирование этого направления выросло на 20% по сравнению с 2022 годом.

Наиболее финансируемый сегмент ИБ в компании

64%
Prevent

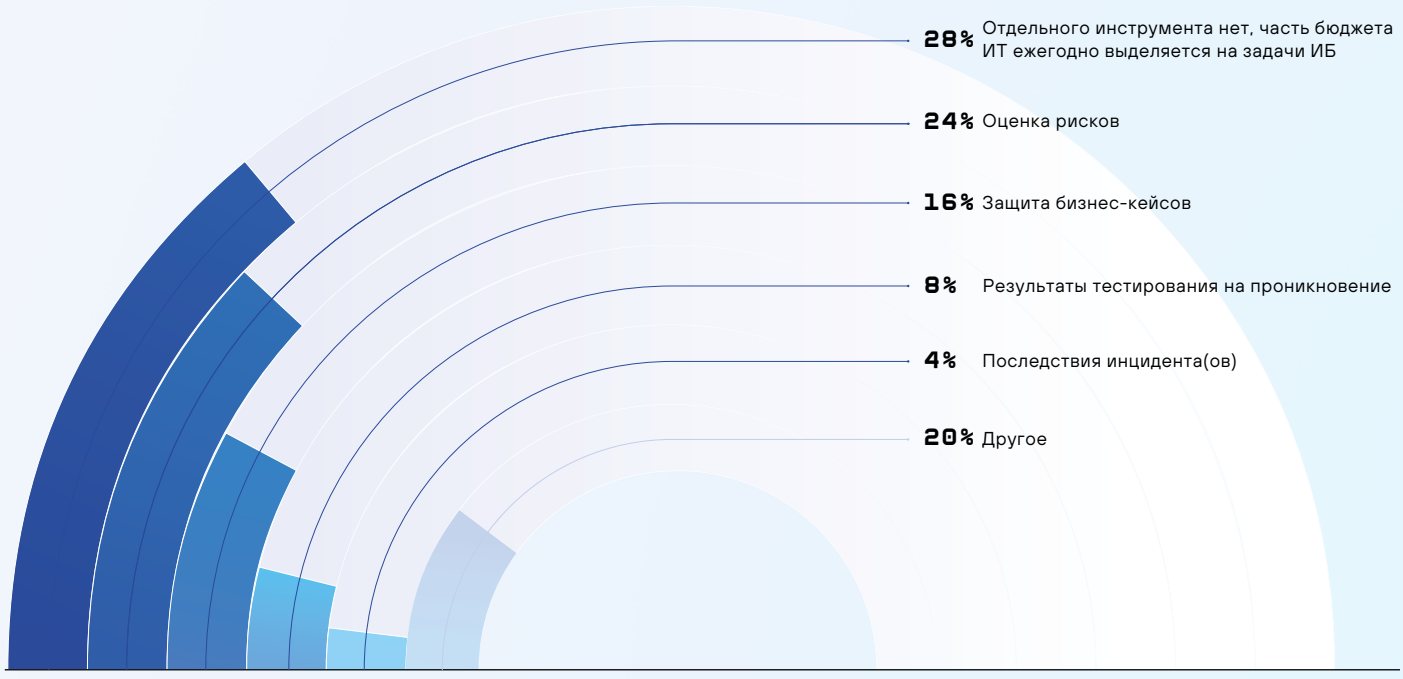
28%
Detect & Respond

8%
Predict



Консервативный подход к планированию отмечают 30% компаний: постоянные расходы незначительно корректируются с учетом инфляции и курса валют. Чуть больше 20% компаний используют для обоснования инициатив риск-ориентированный подход. 16% обосновывают бюджет через защиту бизнес-кейсов или пилотирование решений. Такой подход отмечается в зрелых компаниях со сложной системой защиты инициатив, когда деньги не выделяют «под честное слово». При этом, по словам респондентов, ключевыми драйверами увеличения бюджета стали рост числа регуляторных требований и инициативы по усилению ответственности за их невыполнение.

Основной инструмент обоснования бюджета на ИБ



Управление рисками как инструмент обоснования бюджета не так популярно — во многом из-за незрелости риск-ориентированного подхода на корпоративном уровне. Почти треть респондентов считают риски формально (24%) или «подгоняют» их под свое видение результата (16%).

Большинство компаний используют для определения уровня рисков качественные шкалы (высокий – средний – низкий), и только 12% считают риск в денежном выражении. Большая часть респондентов, использующих количественный метод оценки, относится к финансовой и топливно-энергетической сферам.

Метод оценки рисков ИБ

ОРГАНИЗАЦИЯ СЛУЖБЫ ИБ, ПОИСК И РАЗВИТИЕ ПЕРСОНАЛА

ФОРМИРОВАНИЕ ШТАТА ОТДЕЛА, ПОИСК ПЕРСОНАЛА

Устойчивое развитие функции ИБ в компании напрямую зависит от достаточного количества компетентных ИБ-специалистов. В этой части исследования мы обращали внимание на величину штата ИБ в разных отраслях, изучали потребность в дополнительных специалистах, причины сложности найма и развития персонала.

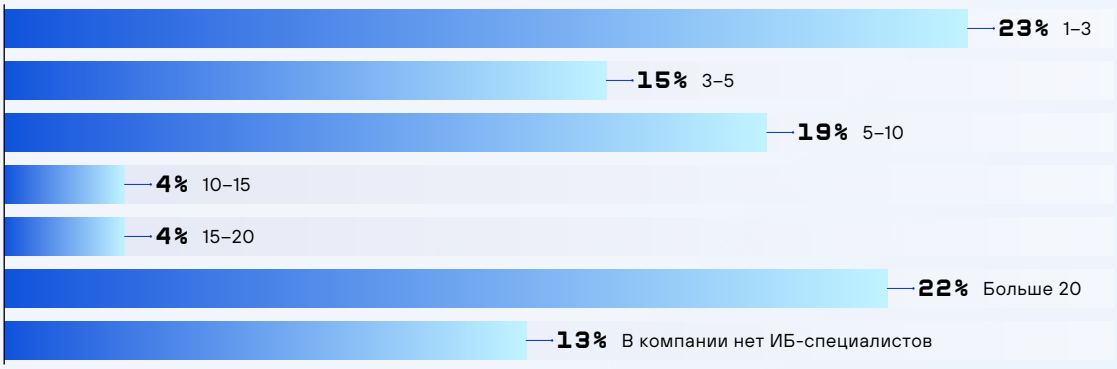
С момента публикации нашего исследования, посвященного особенностям организации служб ИБ в 2019–2021 годах[2], средний штат отдела ИБ заметно вырос. Особенно сильный рост — примерно в два раза — отмечается в финансовом секторе, ритейле и промышленности. Изменение внешнего контекста, крупные кибератаки и утечки, законодательные инициативы — все это повлияло на восприятие ИБ бизнесом. В 2023 году компании постепенно ушли от модели одного специалиста-мультиинструменталиста и начали активно формировать штат отделов ИБ. Это сказывается на рынке труда: спрос явно превышает предложение, дефицит кадров отмечают многие аналитические издания.

Среднее число ИБ-специалистов в разных сферах бизнеса

[2] https://jet.su/upload/content/Osobennosti%20organizaczii%20sluzhb%20ib%20v%20raznykh%20sferakh%20biznesa.pdf

В 48% компаний в отдел ИБ уже входят пять и больше работников. Компании со штатом до трех специалистов составили четверть выборки, и их процент снижается. Только в 13% компаний специалисты ИБ отсутствуют, а поддержку процессов ИБ осуществляют работники ИТ-подразделений.

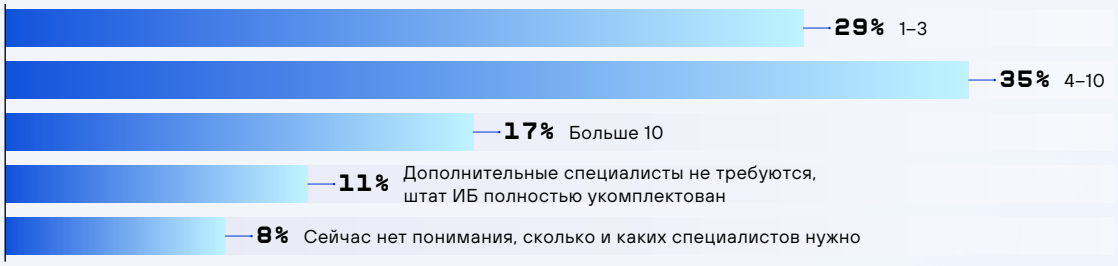
Среднее число ИБ-специалистов в отдельных компаниях



Масштаб компании, стадия ее развития и размер штата ИБ соотносятся почти линейно. Чем крупнее компания, тем больше функций ИБ в ней реализуется и тем больше времени и персонала нужно на выполнение операционных задач. Так, 10 и больше ИБ-специалистов в штате было отмечено в компаниях Large-Enterprise (более 2000 работников.)

Нехватку ИБ-специалистов и трудности с их наймом (особенно на руководящие позиции) отметили большинство опрошенных руководителей (92%). Импортозамещение существующих решений и перестройка процессов ИБ требуют ресурсов: в среднем медианное значение — четыре сотрудника. Больше 10 работников, в основном, требуется респондентам, имеющим достаточный уровень зрелости и ресурсы для выстраивания собственного SOC. Наибольший дефицит профильных кадров испытывают представители финансового, промышленного и топливно-энергетического секторов.

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

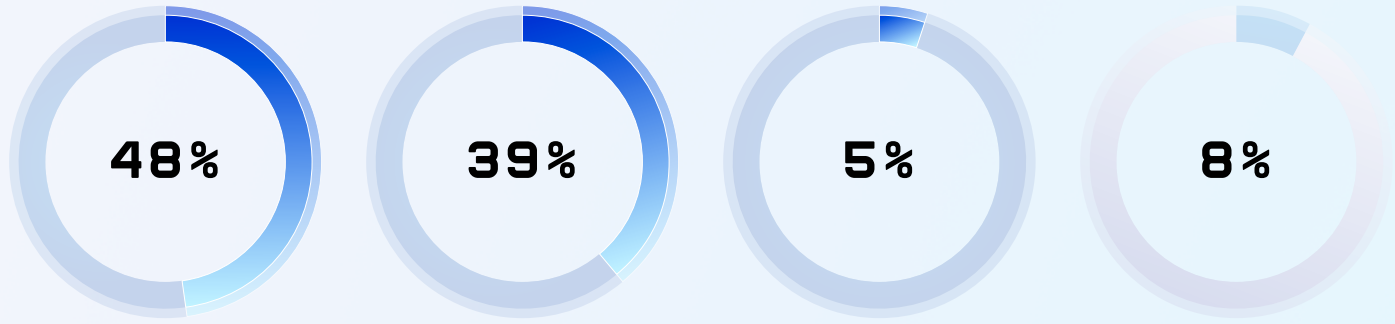


Каждый третий опрошенный отметил затягивание поиска квалифицированных специалистов. Среднее время закрытия вакансий составило 3-4 месяца для специалиста и 6-7 месяцев — для руководителя службы ИБ. Основные причины состоят в следующем:

- высокие зарплатные ожидания кандидатов и неконкурентоспособное предложение на зачастую «перегретом»[3] рынке труда (48%);
- отсутствие в свободном поиске компетентных специалистов, которые сразу могут закрыть потребности компании (39%).

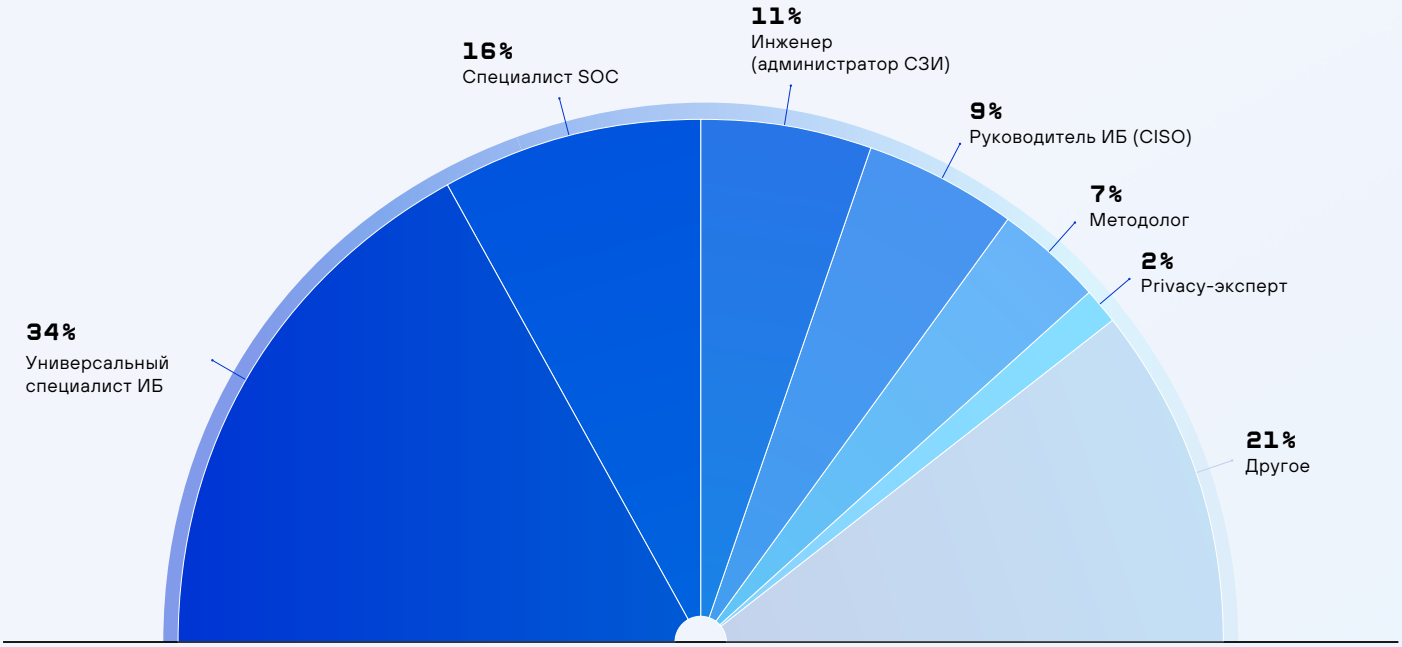
Наибольшим спросом пользуются «универсальные» специалисты, способные закрыть большую часть направлений ИБ в компании (34%). Во многом это обусловлено малым количеством открытых вакансий.

Причина сложности найма новых ИБ-специалистов



[3] Доходы работников растут быстрее их опыта и квалификации.

ИБ-специалист, которого сложнее всего найти в принципе или на текущий момент

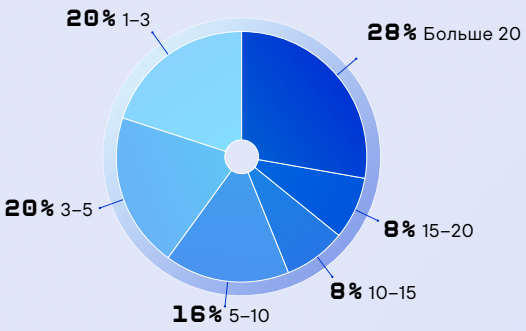


Возможность брать в штат выпускников по ИБ-специальностям

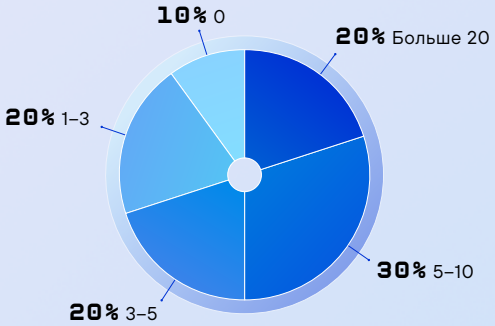
Дефицит квалифицированных кадров побуждает компании активно привлекать выпускников вузов, обладающих базовыми знаниями в нужных областях. Большая часть опрошенных (74%) готова трудоустраивать выпускников профильных направлений. 33% респондентов отмечают, что, помимо образования, кандидаты должны иметь хорошие базовые знания или пройти практику/стажировку в другой компании.

РАЗМЕР ШТАТА ИБ В РАЗНЫХ СФЕРАХ БИЗНЕСА

Финансовый сектор

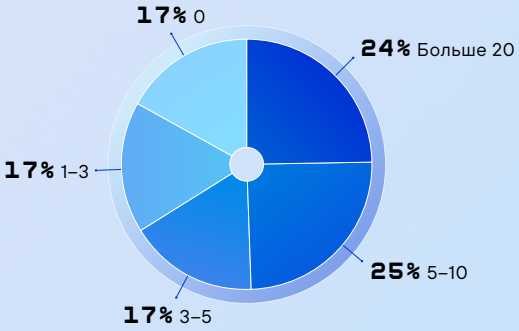


Топливно-энергетический комплекс

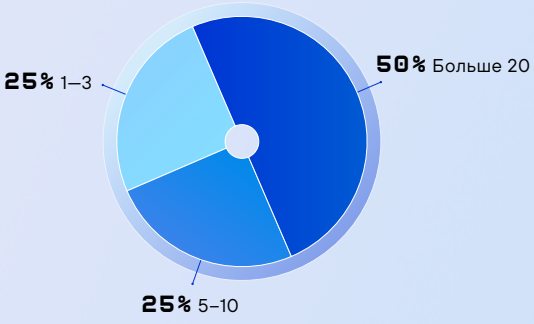


Ритейл

Промышленность

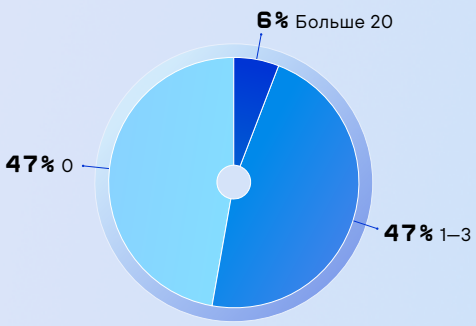


ИТ

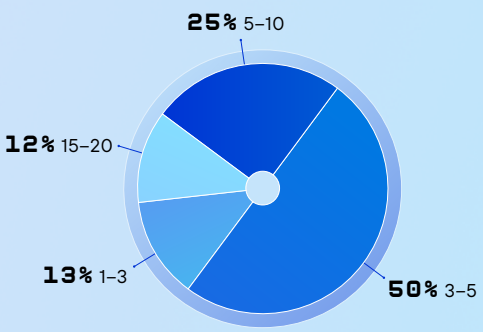


Здравоохранение

Транспорт



Другое



СТРУКТУРНАЯ ПОДЧИНЕННОСТЬ

Эффективность развития ИБ в компании во многом определяется ее структурной подчиненностью. Подчинение блоку ИТ или СБ часто приводит к восприятию ИБ как второстепенной функции, конфликту интересов и формированию бюджета на ИБ по остаточному принципу.

Изменения в законодательстве, принятые в 2022 году, способствовали пересмотру подчиненности функции ИБ и стали драйвером обоснования ее вывода на прямой уровень руководства. Однако мы не наблюдали кардинальной картины «переподчинения». В большинстве компаний (38%) подразделение ИБ независимо: ситуация была такой же в 2021-2022 годах. Второй большой блок — подчинение службы ИБ блоку ИТ (28%).

Подчинение высшему руководству в наибольшей степени характерно для финансового сектора. Подчинение блоку ИТ чаще всего наблюдается в ТЭК, транспортной и промышленной отрасли.

Подчиненность подразделения ИБ

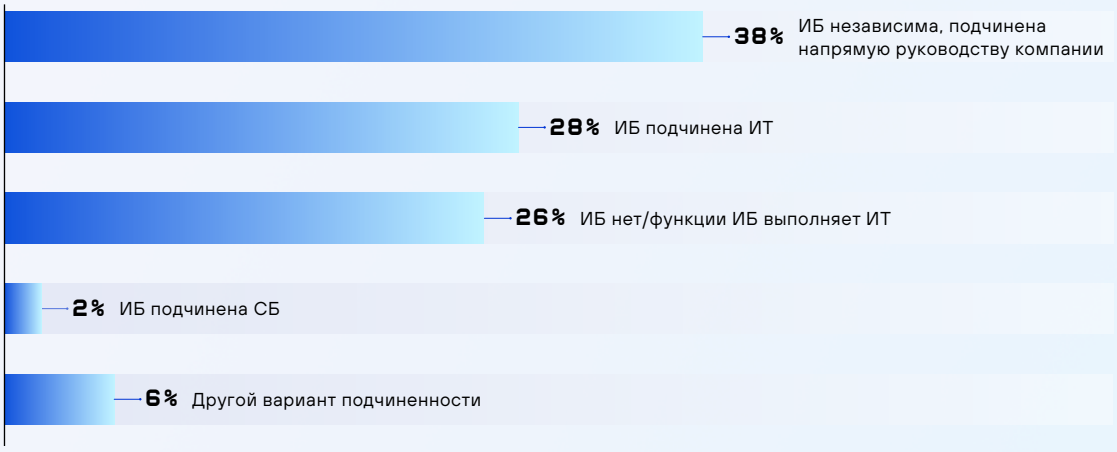


Таблица. 2. Зависимость между сферой деятельности компании и подчиненностью ИБ

	ИТ	Здравоохранение	Другое (сфера услуг, девелопмент, торговля и т.п.)	Промышленность	Ритейл	Топливно-энергетический комплекс	Транспорт	Финансовый сектор
ИБ независима, подчинена напрямую руководству компании	2%	2%	2%	4%		2%	2%	22%
ИБ подчинена ИТ	2%		2%	4%		4%	12%	4%
ИБ подчинена СБ							2%	
ИБ нет/функции ИБ выполняет ИТ				6%	2%	2%	16%	
Другой вариант подчиненности						3%		5%

ОЦЕНКА ЭФФЕКТИВНОСТИ ФОРМИРОВАНИЕ ОТЧЕТНОСТИ ДЛЯ РУКОВОДСТВА

Подготовка отчетности по результатам работы службы ИБ помогает:

- Обосновать принятые решения
- Обеспечить прозрачность и доверие к работе подразделения
- Отследить прогресс и информировать руководство о результатах отдельных инициатив

Управленческую отчетность для высшего руководства (C-level) формирует большинство компаний (72%). Только в трети компаний отчетности нет или она остается на уровне подразделения. При этом уровень зрелости процессов ИБ не является определяющим фактором: отчетность отмечалась во всех компаниях с разным уровнем зрелости, начиная с повторяемого и заканчивая управляемым.

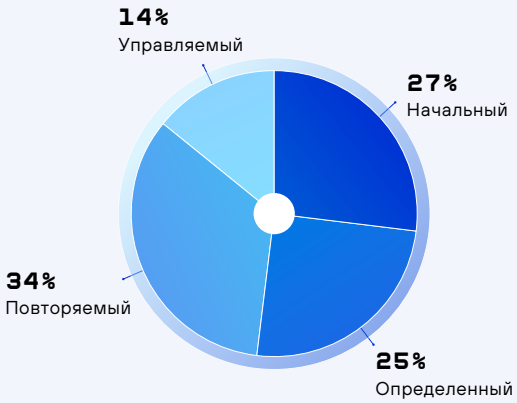
На начальном уровне (27% опрошенных) выполняются единичные процессы, специализированных средств защиты нет или очень мало.

На повторяемом уровне (34% опрошенных) используются минимально необходимые средства защиты. Процессы ИБ повторяемы и планируются, но не соответствуют лучшим практикам. Управление процессами не построено.

На определенном уровне (25% опрошенных) у компании достаточно ресурсов для оперативного управления процессами ИБ, разработана программа развития ИБ на несколько лет, процессы стандартизированы и надежны, документация разработана и регулярно обновляется.

На управляемом уровне (14% опрошенных) эффективность процессов постоянно измеряется с помощью метрик. Связь между ИБ и бизнесом налажена, процессы ИБ контролируются, управление процессами автоматизировано.

Уровень зрелости процессов ИБ в компании

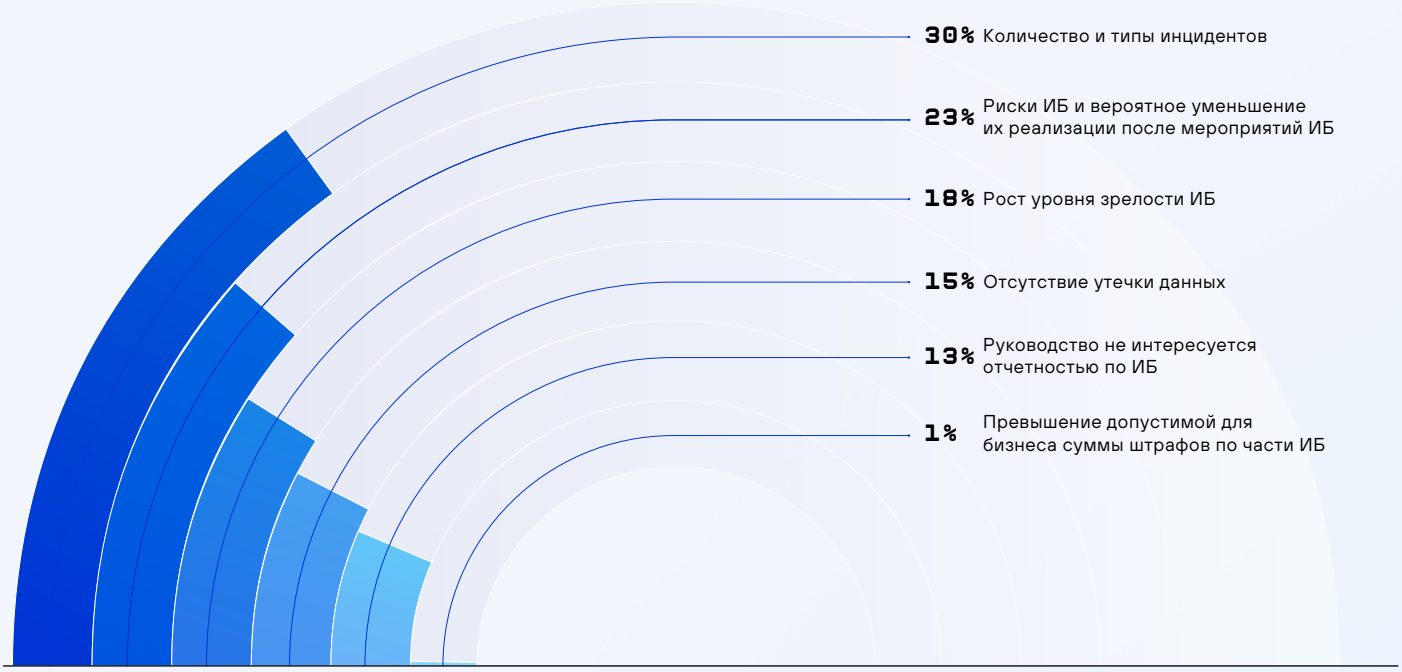


Адресаты отчетности по результатам работы службы ИБ

Периодичность подготовки отчетов зависит от размера и структуры компании, корпоративных правил и предпочтений руководства. В общем случае (больше 40% опрошенных) отчеты предоставляются раз в квартал. Треть респондентов готовит аналитику ежегодно, еще 20% формируют отчеты по запросу или от случая к случаю.

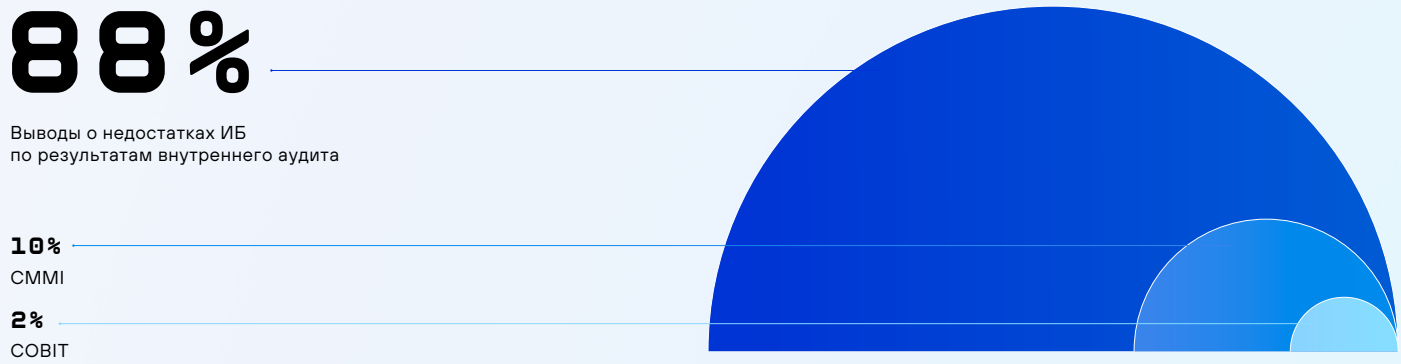
Чаще всего на уровень менеджмента поднимается информация о количестве и типах инцидентов за отчетный период (30%), динамике обработки рисков ИБ (23%) и росте уровня зрелости процессов ИБ (18%). Меньше всего руководство интересуется данными об утечках и штрафах за невыполнение требований регуляторов: их величина некритична для ведения бизнеса.

Показатель, наиболее интересующий руководство компании



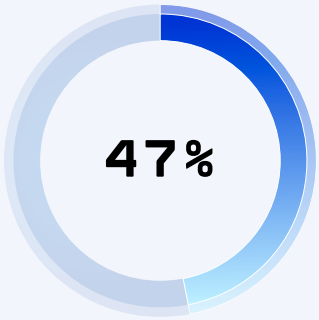
В качестве инструмента оценки эффективности реализуемых мер по ИБ подавляющее большинство компаний использует подход к оценке выполнения набора внутренних контролей (требований) по результатам систематического внутреннего аудита. 10% респондентов используют общеизвестную методику CMMI, позволяющую качественно оценить уровень зрелости процессов.

Инструмент для измерения уровня зрелости ИБ в компании

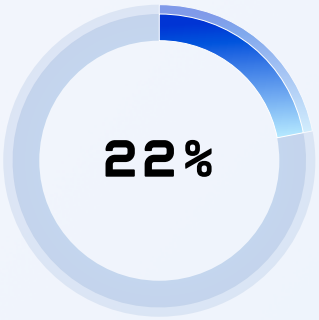


Интегрированный подход к оценке эффективности ИБ на основе метрик в большинстве российских компаний используется фрагментарно: чаще всего метрики разрабатываются для отдельных процессов ИБ (15%), но процесс их сбора не является системным. Несмотря на значимость метрик для оценки эффективности и управления ИБ, большинство компаний (более 40%) их до сих пор не применяет, что ограничивает их способность к контролю отдельных областей ИБ. Только 7% компаний автоматизировали процесс сбора и используют инструменты визуализации метрик (дашборды).

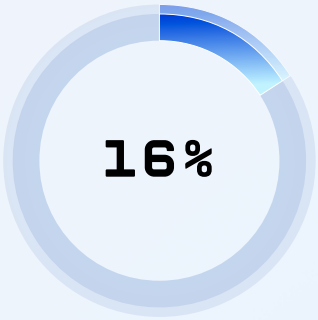
Наличие в компании метрик для отслеживания эффективности ИБ



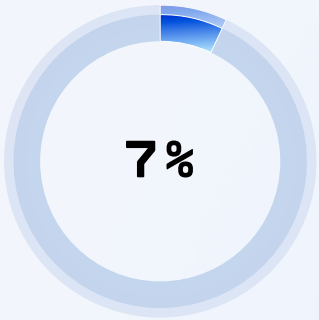
Нет



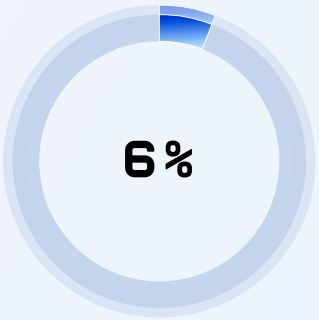
Есть система метрик, по которой мы принимаем решение и отчитываемся



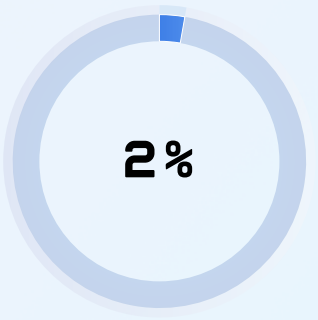
Есть единичные метрики по процессам ИБ (не для всех процессов ИБ)



Сбор метрик автоматизирован, есть инструменты визуализации (дашборды)



Есть метрики, но процесс не системен (метрики ни на что не влияют)



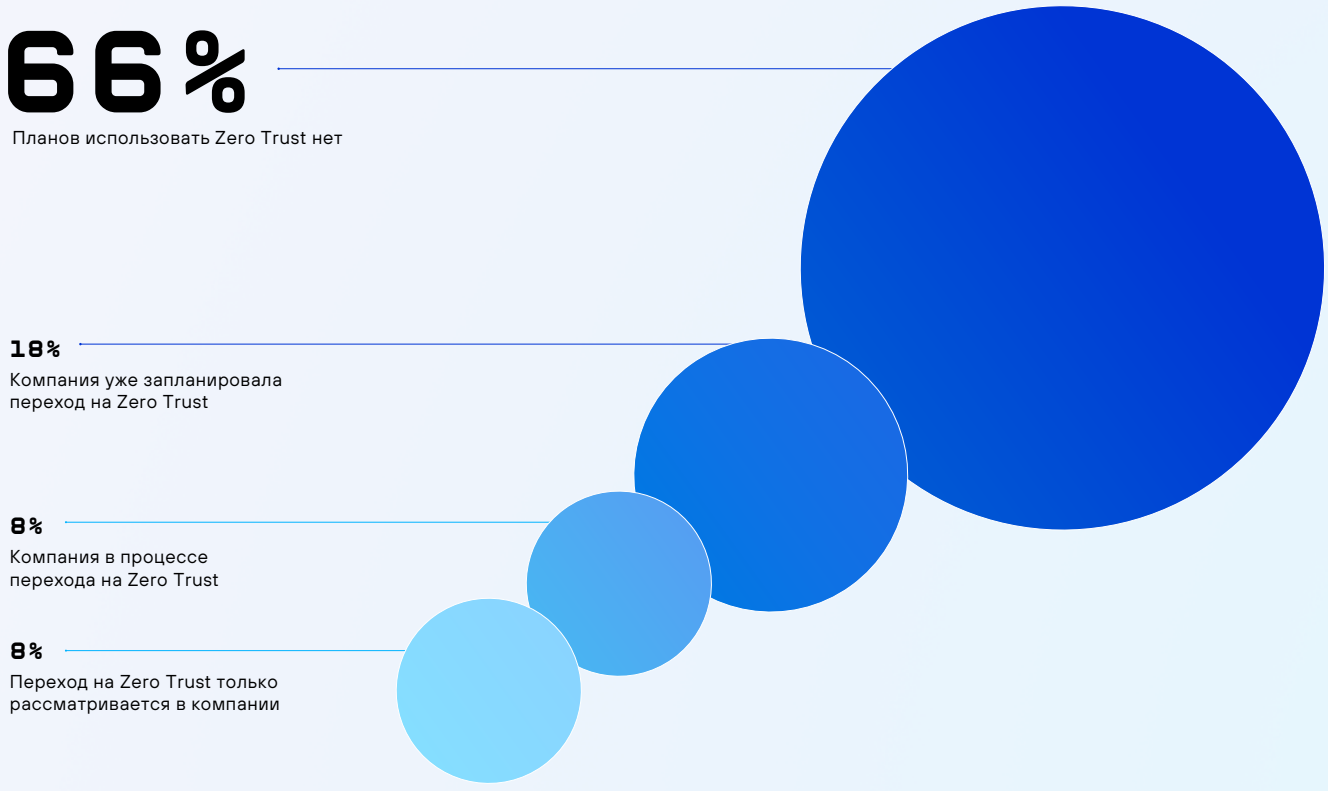
Другое

ПОДДЕРЖАНИЕ КИБЕРУСТОЙЧИВОСТИ

Киберустойчивость компании определяется тем, насколько быстро и без значимых потерь она может справиться с кибератакой, продолжая эффективно вести бизнес. Грамотно выстроенная архитектура ИБ помогает отражать атаки, а управление непрерывностью бизнеса — восстановиться до наступления критичных последствий.

Большинство респондентов предпочитает классические модели построения архитектуры ИБ: модель защиты периметра «Замок и ров» — 46%, модель эшелонированной обороны — 52%[4]. В 2023 году CISO чаще всего следовали стратегии «Укрепляем существующие рубежи». Модель Zero Trust пока непопулярна: ее используют только 2% опрошенных. Однако тренд перехода на модель нулевого доверия начал уверенно прослеживаться в прошедшем году в виде реализации ее отдельных принципов.

Возможность перехода на модель Zero Trust



[4] С моделями кибербезопасности можно подробно ознакомиться в нашем ролике: https://youtu.be/ZYO0rgc11j4?feature=shared

«Никогда не доверяй, всегда проверяй» — самый известный принцип модели нулевого доверия. Согласно этому принципу, уровень доверия не зависит от источника запроса или типа данных, к которым мы обращаемся. По умолчанию все пользователи являются недоверенными и не могут получить доступ без тщательной проверки.

В ходе анализа мы выявили четкую зависимость выбранной модели от текущего уровня зрелости ИБ. Компании с начальным уровнем оценки по CMMI чаще используют модель «Замок и ров» (фокусировка на защите периметра), модель эшелонированной обороны применяют компании с уровнем зрелости «Повторяемый» и выше. Выбор модели построения архитектуры ИБ практически не зависит от сферы деятельности компании: мы не выявили характерные модели для той или иной отрасли.

Таблица. 3. Зависимость выбора модели архитектуры ИБ от уровня зрелости ИБ в компании

Уровень зрелости CMMI / Модель построения архитектуры ИБ	Castle-and-Moat	Defense in Depth	Zero Trust
Начальный	32%	6%	
Повторяемый	12%	22%	
Определенный	2%	10%	2%
Управляемый		14%	

Все опрошенные руководители отметили незначительный рост числа атак в 2023 году: количество переросло в качество, увеличились сложность и разнообразие применяемых методов. Лидирующими по частоте остаются DDoS-атаки и фишинг: они уверенно занимают первые места с 2022 года.

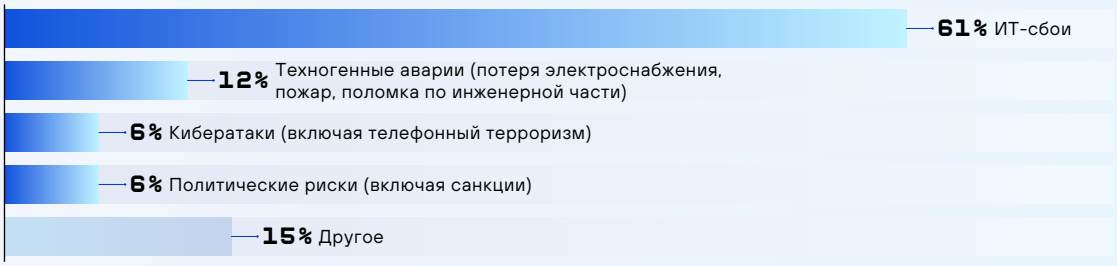
Наиболее актуальные для компании виды атак

Чтобы компания даже во время кибератак продолжала эффективно работать и выполнять обязательства перед клиентами и партнерами, необходим выстроенный процесс управления непрерывностью бизнеса. Однако для многих респондентов этот процесс связан только с ИТ-сбоями, и его выстраиванием занимаются в основном ИТ-специалисты.

При оценке рисков прерывания деятельности фокус также остается смещенным в сторону ИТ: несмотря на рост числа киберугроз, большинство руководителей считают ИТ-сбой главной угрозой.

Подразделение компании, ответственное за обеспечение непрерывности бизнеса

Наиболее критичные для компании риски непрерывности бизнеса

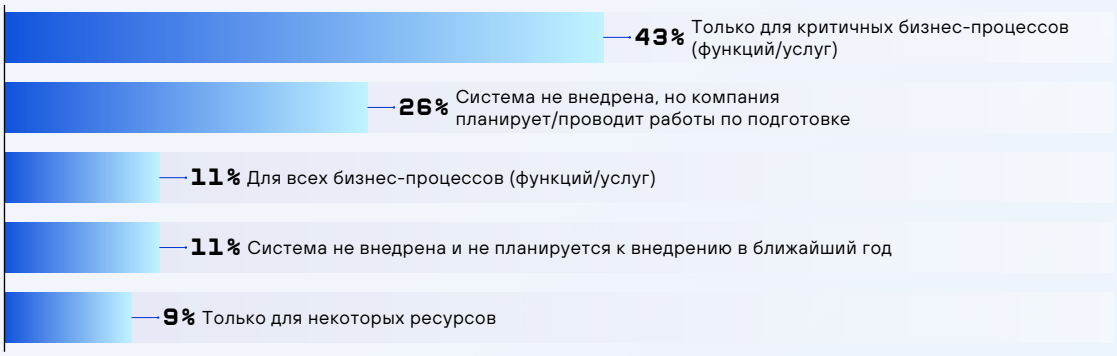


Применение аспектов непрерывности для функций ИБ, восстановление распределенных СЗИ, наличие общего с ИТ-блоком SLA на восстановление — единичные случаи в больших холдинговых компаниях, имеющих зрелый общекорпоративный процесс управления непрерывностью бизнеса.

Сам процесс управления непрерывностью бизнеса почти в 40% компаний до сих пор находится на уровне «У нас есть

система резервного копирования, в случае сбоя восстановимся как-нибудь». Такая выжидающая позиция приводит к серьезным проблемам, если атака оказывается успешной. Большинство компаний (55%) не имеет готового плана действий на кризисный случай. Это подтверждается и зафиксированными инцидентами, приводившими к остановке бизнес-процессов: 42% респондентов, оказавшихся в такой ситуации, не смогли восстановиться в целевое время.

Область действия системы управления непрерывностью бизнеса в компании



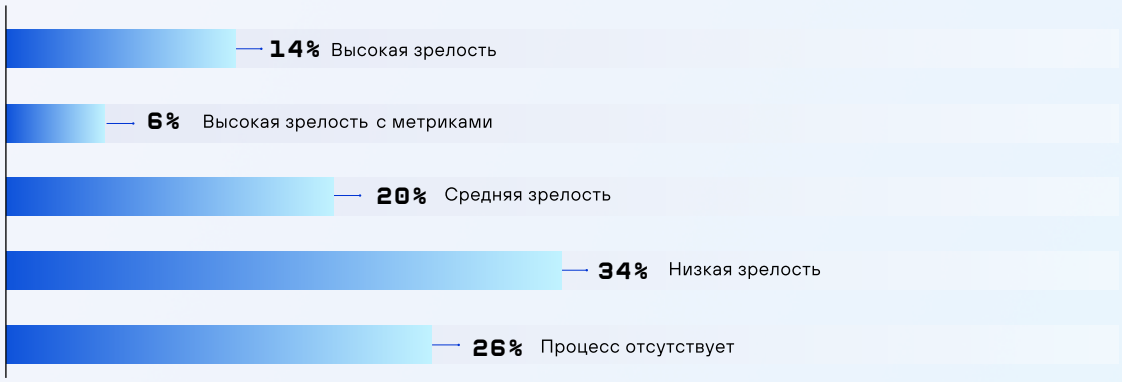
ПОДДЕРЖАНИЕ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Массовое обучение работников компании базовым правилам цифровой гигиены, систематические фишинговые эмуляции, подведение пользователей к осознанному взаимодействию с конфиденциальной информацией — основы культуры кибербезопасности.

Согласно результатам опроса, наиболее распространенным типом атак являются фишинговые атаки на работников (34% респондентов), а человеческий фактор — основная причина успешного взлома инфраструктуры злоумышленниками (53% респондентов).

Несмотря на это, большинство опрошенных компаний придерживаются консервативных моделей обучения, а сам процесс повышения осведомленности отсутствует или имеет низкий уровень зрелости[5] (60%).

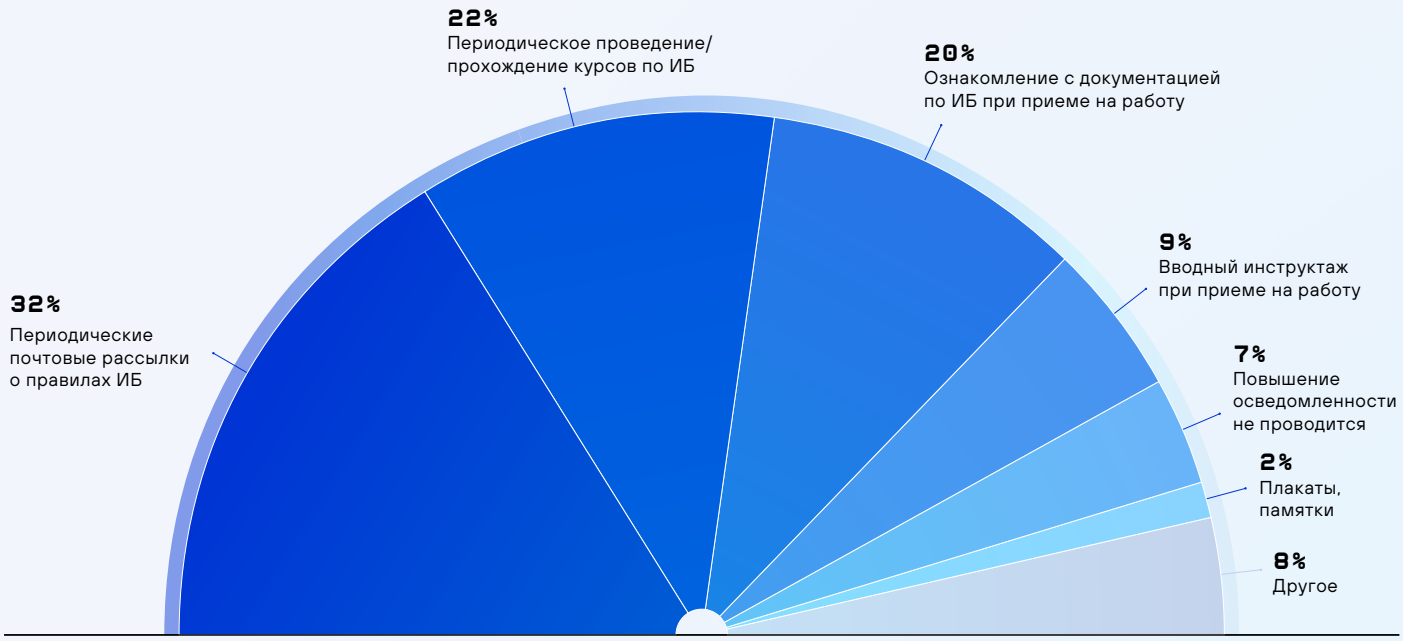
Оценка уровня процесса повышения осведомленности



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

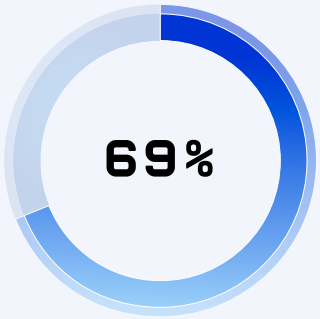
В компаниях, имеющих процесс повышения осведомленности, самыми распространенными мероприятиями являются периодические почтовые рассылки о правилах ИБ (32%). На втором месте — периодическое прохождение работниками специализированных курсов по темам ИБ (22%). В большинстве случаев процесс повышения осведомленности консервативен. Только малая часть компаний использует для донесения важности правил ИБ текущие возможности рынка, разные форматы обучающих материалов и творческий подход (интерактивные электронные курсы, видеоролики, скринсейверы, памятки, плакаты и т. д.).

Способы повышения осведомленности работников в области ИБ

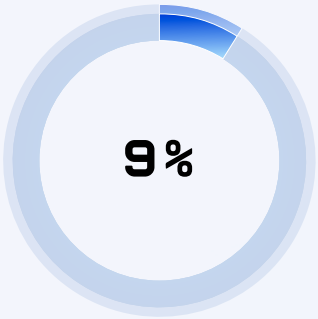


Учебные фишинговые рассылки для практической оценки подготовленности работников к атаке методом социальной инженерии проводят 31% респондентов (в 7% случаев это разовые мероприятия). Можно сказать, что они постепенно становятся стандартом для формирования корпоративной киберкультуры.

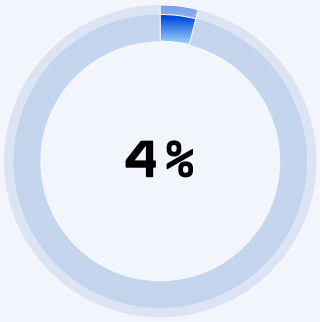
Частота проведения эмуляций фишинговых атак



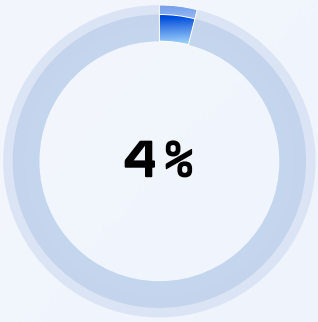
Не проводятся



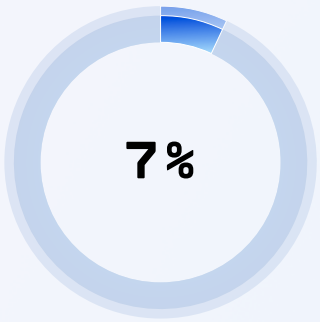
Ежегодно



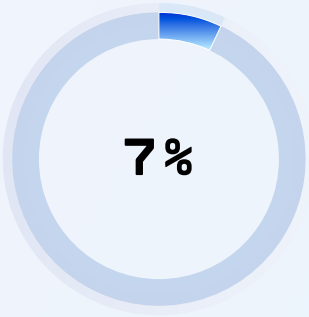
Ежеквартально



Ежемесячно



Проводились разово



Другое

ВМЕСТО ЗАКЛЮЧЕНИЯ: НА ЧТО ОБРАТИТЬ ВНИМАНИЕ CISO?

В 2023 году российские компании столкнулись со значительными вызовами — усилением угроз, изменением характера и методов проведения кибератак. На основе наших прогнозов на 2024 год мы предлагаем CISO сосредоточиться на следующих ключевых направлениях ИБ.

УТОЧНИТЕ ПРИОРИТЕТЫ БИЗНЕСА

В круг особого внимания должны входить интересы руководства и области высокого риска — критически важные процессы и ресурсы. С изменением внешних факторов фокус часто смещается. Пообщайтесь с руководством: уточните приоритеты в области ИБ, актуальность и достаточность текущей отчетности (какие метрики/срезы нужны для принятия решений и отслеживания результативности ИБ).

ИСПОЛЬЗУЙТЕ ВОЗМОЖНОСТИ ТЕКУЩЕЙ ИНФРАСТРУКТУРЫ

Для реализации базовой гигиены ИБ не всегда требуется целый парк средств защиты — часто достаточно полностью использовать потенциал существующей ИТ-архитектуры. Ошибки в настройке приложений и сервисов сложно «перекрыть» даже с помощью СЗИ. Установка безопасных настроек ИТ-ландшафта и сетевого оборудования поможет защититься от горизонтального перемещения атакующих в инфраструктуре.

РАЗВИВАЙТЕ КУЛЬТУРУ КИБЕРБЕЗОПАСНОСТИ

Фишинговые атаки прочно входят в ТОП-3 способов получения доступа к инфраструктуре. С 2023 года мы наблюдаем широкое использование искусственного интеллекта для проведения атак такого рода. Инвестируйте в культуру кибербезопасности: сделайте учебные фишинговые рассылки

системными, повышайте доступность знаний по ИБ с помощью разных каналов и форматов (электронные курсы, почтовые рассылки, видеоролики и т. п.), формируйте и поддерживайте позитивный бренд ИБ.

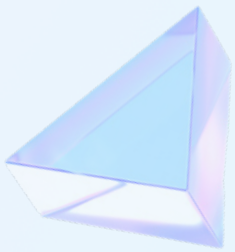
ПОВЫШАЙТЕ КИБЕРУСТОЙЧИВОСТЬ

Реагирование на инциденты ИБ не должно быть изолировано от функций поддержания непрерывности бизнеса. Вам нужно иметь четкое представление о порядке действий в кризисной ситуации. Проверьте актуальность имеющихся планов реагирования на инциденты, резервного копирования данных и тестирования их восстановления. Уточните точки взаимодействия с ИТ в рамках процесса поддержания непрерывности бизнеса. Обновите планы по внешним коммуникациям: они понадобятся, если кризис коснется клиентов компании.

РАЗВИВАЙТЕ КОМПЕТЕНЦИИ КОМАНДЫ РЕАГИРОВАНИЯ

Уделите внимание развитию навыков совместной работы команды реагирования на инциденты. Сервисы киберучений помогут выявить проблемы в коммуникации и пробелы в знаниях. Развивайте «гибкие навыки» команды (убеждение и ведение переговоров).

ОБЕСПЕЧЬТЕ МОНИТОРИНГ ЗА ПРЕДЕЛАМИ ИНФРАСТРУКТУРЫ КОМПАНИИ



Проводите регулярный мониторинг теневых форумов и открытых источников информации на предмет упоминания компании и возможной компрометации принадлежащих ей данных. Системно анализируйте поверхность атаки инфраструктуры компании и ее критичных подрядчиков. Фокус на проактивной безопасности позволит выявлять атаки на ранней стадии.

СФОКУСИРУЙТЕСЬ НА ИНСАЙДЕРАХ

Стабильные продажа клиентских данных в Даркнете и интерес к таким данным со стороны злоумышленников, «вербующих» инсайдеров, вряд ли приведут к уменьшению количества утечек в 2024 году. Ознакомьтесь с рекомендациями по защите от инсайдеров в нашем исследовании «Атаки инсайдеров: угроза внутри периметра». Уделите особое внимание шагам «Рекрутинг» и «Эксфильтрация».

ОБЕЗОПАСЬТЕ ТОЧКИ ВЗАИМОДЕЙСТВИЯ С КЛЮЧЕВЫМИ ПАРТНЕРАМИ

Повысьте прозрачность своей цепочки поставок: проанализируйте, с какими третьими лицами и каким образом взаимодействует компания, какие методы подключения к корпоративной инфраструктуре используются, к каким ресурсам и данным подрядчик сможет получить доступ. По результатам анализа реализуйте защиту компонентов ИТ-инфраструктуры для совместного использования и контролируйте действия критичных подрядчиков.

JET

SECURITY
TEAM

security@jet.su
jetcsirt.su