

Июнь 2025

Инвестиции в информационную безопасность в России





Оглавление

Глобальные тренды	3
Инвестиции в ИБ в России	4
Подходы к управлению бюджетами ИБ в России	6
Управление инвестициями в ИБ	6
Целеполагание при инвестировании в ИБ	6
Определение объема инвестиций в ИБ	8
Выводы	9

Глобальные тренды

Информационная безопасность (ИБ) является критически важным элементом современного бизнеса в условиях стремительной цифровизации, роста киберугроз и перехода к облачным технологиям. По данным компании Gartner, глобальные расходы на ИБ и управление рисками выросли с \$150,4 млрд в 2021 году до прогнозируемых \$212 млрд в 2025 году¹, демонстрируя среднегодовой темп роста (CAGR) в 9–15%. Основные драйверы роста включают в себя увеличение числа кибератак, в том числе с применением вредоносного ПО (в особенности программ-вымогателей, ransomware), различных техник социальной инженерии (в особенности фишинга), а также необходимость защиты данных при удаленной работе, внедрении технологии Интернета вещей (IoT/IIoT) и искусственного интеллекта (ИИ).

> \$212 млрд

Объем мировых затрат на информационную безопасность в 2025 году (прогноз)

Расходы на ИБ варьируются в зависимости от уровня экономического развития и цифровой зрелости экономики государства. В развитых странах, таких как США, странах Европы и крупнейших экономиках Азии, наблюдаются более высокие бюджеты и темпы роста, тогда как в развивающихся странах, таких как Бразилия, Аргентина и ЮАР, рынок ИБ растет медленнее, но демонстрирует значительный потенциал.

Таблица 1.² Расходы на ИБ в зависимости от региона

	2024 \$ млрд	2025 \$ млрд	Доля мирового рынка в 2025 г.	Рост рынка	
США	82,4	88,25	42%	7.11%	CAGR, 2025-2029
Европа	63,9	69,5	33%	11.8%	YoY, 2024/2025
Япония	8,3	9,7	5%	16.9%	CAGR, 2024-2028
Китай	8,4	9,7	5%	15.5%	CAGR, 2024-2028
Латинская Америка	8,35	9,01	4%	7.89%	CAGR, 2025-2029
Ближний Восток и Северная Африка	2,89	3,3	2%	12,7%	YoY, 2024/2025

¹ "Forecast: Information Security, Worldwide, 2022-2028, 2024 Update.", Gartner, 2024

²

"Information Security Spending: What Does the Future Hold?", Gartner, 2024

"Worldwide Security Spending Guide", IDC, 2025

Cybersecurity - United States, Statista, 2025

"Gartner Security & Risk Management Summit", Gartner, 2025

Инвестиции в ИБ в России

По данным Центра Стратегических Разработок (ЦСР), в 2023 году объем российского рынка информационной безопасности составил 248,5 млрд рублей, что на 28,5% больше по сравнению с предыдущим годом³. ЦСР прогнозирует, что в 2025 году объем российского рынка составит 369 млрд рублей (~2.2% мирового рынка), а к 2028 году вырастет до 715 млрд рублей при среднегодовом темпе роста 23,6%. Российский рынок информационной безопасности демонстрирует устойчивый высокий рост, обусловленный как внутренними органическими потребностями, так и внешними вызовами.

Стоит отметить, что приведенные выше цифры включают только расходы на приобретение программного обеспечения, оборудования и услуг. Кроме того, существуют и внутренние затраты компаний на обеспечение информационной безопасности — прежде всего, расходы на персонал, включая зарплаты и непрерывное обучение специалистов по информационной безопасности. По общемировой практике данные расходы варьируются в широких пределах, достигая существенных 39% от всех трат на информационную безопасность⁴.

Приведенные выше цифры дают общее представление о состоянии отрасли со стороны рынка (компаний-производителей (вендоров), предоставляющих ПО, оборудование и услуги информационной безопасности). Однако эти данные не раскрывают механизм формирования бюджетов заказчиков (прямых инвестиций в ИБ), не объясняют, какие именно факторы и управленческие роли влияют на рост или сокращение расходов на информационную безопасность внутри организаций.

Для уточнения этих аспектов ЦСР провёл опрос среди крупных предприятий и государственных организаций, с целью выявить, как именно формируются бюджеты на ИБ, кто принимает ключевые решения, какие внутренние приоритеты и внешние требования определяют изменение расходов в ту или иную сторону.

Опрос, проведенный в рамках данного исследования, показал, что в 2025 году бюджет крупной организации на обеспечение информационной безопасности составляет в среднем более 294 млн рублей в год при росте в 29% в сравнении с 2024 годом⁵.

> 294 млн рублей

Средние ежегодные инвестиции крупной российской компании в ИБ в 2025 году

+ 29%

Средний рост инвестиций крупной российской компании в ИБ в 2025 году

³ «Прогноз развития рынка кибербезопасности в Российской Федерации на 2024-2028 годы», ЦСР, 2024

⁴ «Compensation and Budget for CISOs in Large Enterprises», IANS + Artico, 2025

⁵ В исследовании учитывались бюджеты на информационную безопасность, не включая затраты на оплату труда, обучение и повышение квалификации персонала.

Средний годовой бюджет на информационную безопасность крупных организаций варьируется от 102 млн рублей в государственном секторе до более 500 млн рублей в финансовом и ИТ-секторе, что отражает различия в уровне цифровизации бизнеса, зрелости процессов безопасности и соответствующих регуляторных требованиях.

Диаграмма 1. Средний объем инвестиций крупной организации в ИБ, млн рублей в год

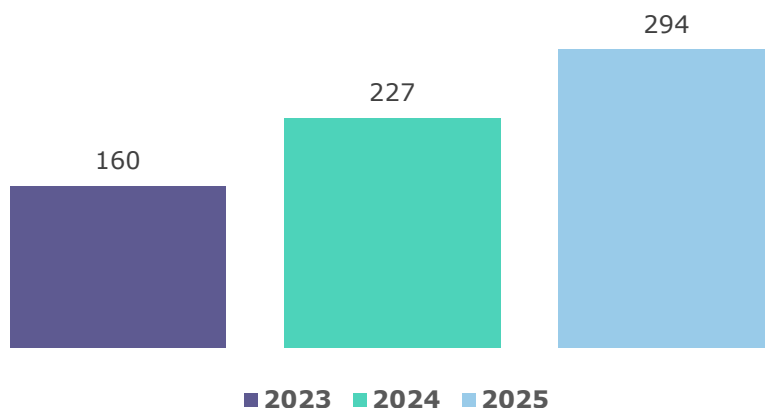
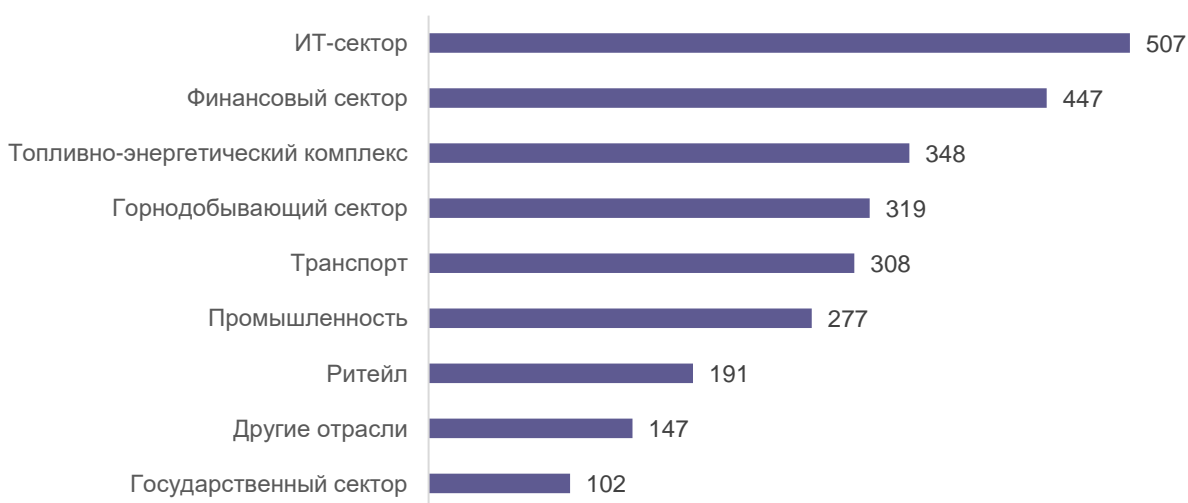


Диаграмма 2. Средние размеры инвестиций в ИБ в 2025 году по отраслям, млн рублей



Российский рынок ИБ развивается в соответствии с глобальными тенденциями, при этом ежегодные инвестиции организаций в информационную безопасность растут быстрее (~29% в год), чем в остальных регионах мира (~13% в год). Это свидетельствует не только о возросшей значимости ИБ для отечественного бизнеса в условиях геополитической нестабильности, но и высоких темпах цифровой трансформации экономики страны. Запрос бизнеса на непрерывное повышение уровня цифровизации предприятий Российской Федерации требует параллельного развития архитектуры безопасности как отдельных организации, так и всего сектора ИТ на уровне государства, с учетом процессов необходимого импортозамещения.

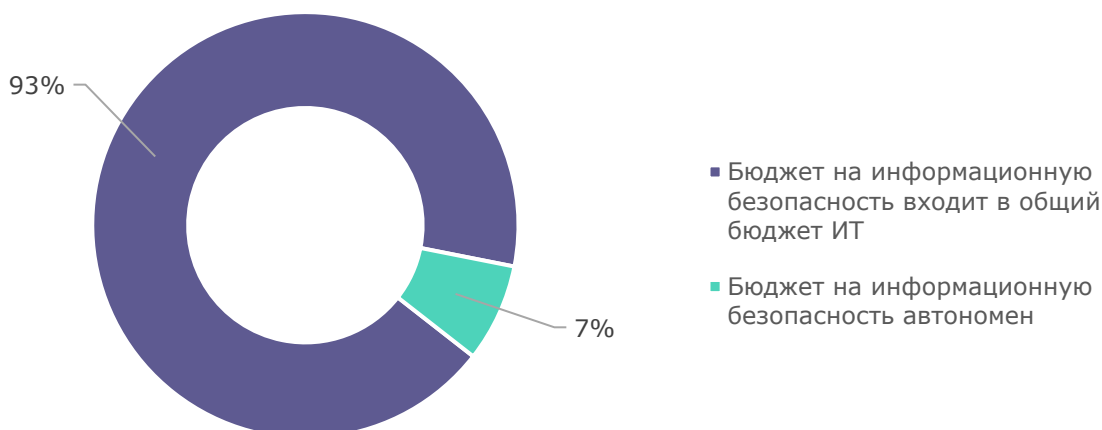


Подходы к управлению бюджетами ИБ в России

Управление инвестициями в ИБ

По данным опроса, в большинстве российских компаний бюджет ИБ интегрирован в общий ИТ-бюджет, отражая подход, при котором кибербезопасность рассматривается как часть общей ИТ-стратегии предприятия и сопутствующих инициатив.

Диаграмма 3. Структурное расположение бюджетов ИБ, % респондентов



Опрос показал, что 93% компаний включают ИБ бюджет в бюджет ИТ. Несмотря на существенный перекос в сторону неавтономности ИБ, такой подход в целом согласуется с мировыми трендами. Растущий объем расходов на ИБ напрямую влияет на приоритеты проектов ИТ и цифровой трансформации, что требует от менеджмента переходить к гибким бизнес-интегрированным моделям финансирования ИБ. Согласно отчету Deloitte⁶ в мире 58% организаций бюджеты на информационную безопасность полностью интегрируются в бюджеты различных инициатив, связанных с бизнесом (ИТ, цифровая трансформация, облачные инвестиции и так далее), в 55% компаний бюджет сохраняет автономность, в том числе в рамках проектов. При этом 25% всех опрошенных организаций применяют комбинированный подход, когда бюджет ИБ остается автономным в одних инициативах, но интегрированным в других. Таким образом, подавляющая часть компаний в мире склонна сегодня к интеграции ИБ-затрат в расходы по приоритетным бизнес-направлениям, нежели к их сепарированию. С одной стороны, такой подход позволяет гармонизировать защиту непрерывно растущей ИТ-инфраструктуры, но с другой может ограничивать гибкость управления безопасностью, т.к. ИБ-менеджмент лишается эффективного контроля над процессом бюджетирования и над расходованием средств.

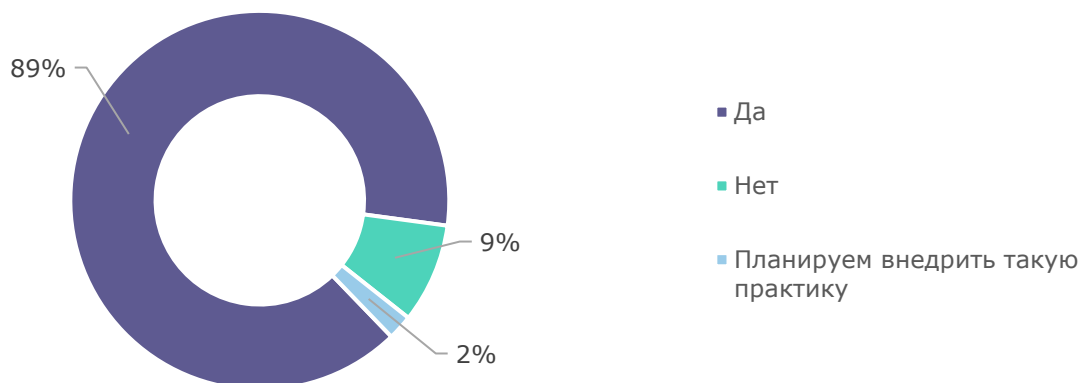
Целеполагание при инвестировании в ИБ

Для эффективного управления информационной безопасностью, включая планирование и приоритезацию расходования средств, в мировой и отечественной практике широко применяется риск-ориентированный подход, основанный в том числе на стандартах, таких как ГОСТ Р ИСО/МЭК 27005 (ISO/IEC 27005:2022). Следование подобным методикам помогает оценивать затраты на основе анализа угроз, уязвимостей и потенциального ущерба от угроз, минимизируя вероятность недофинансирования необходимых мер по предотвращению кибератак.

⁶ «Global Future of Cyber Survey, 4th Edition», Deloitte, 2024

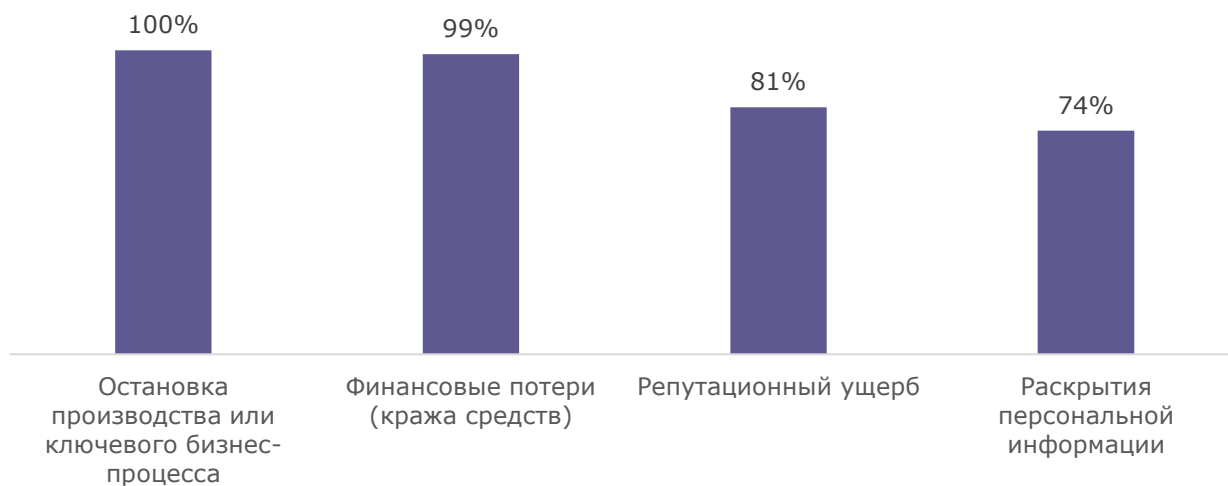
Практика формализации критических рисков при формировании стратегии информационной безопасности широко распространена среди крупных организаций РФ – 89% респондентов указали на применение соответствующих методик, демонстрируя высокий уровень зрелости методологической работы структур ИБ.

Диаграмма 4. Применение методик определения критических рисков, %



Наиболее важными и общими для всех отраслей категориями рисков, по степени значимости с точки зрения информационной безопасности, являются остановка бизнес-процесса (100% респондентов) и прямые финансовые потери (кража денежных средств, 99%). Риски, связанные с раскрытием персональных данных, оказались критически-значимыми только для 74%.

Диаграмма 5. Степень критичности рисков по ключевым категориям, %



Определение объема инвестиций в ИБ

В ходе исследования респондентам предлагалось выбрать один или несколько подходов, которыми их организации руководствуются при определении объёмов финансирования информационной безопасности.

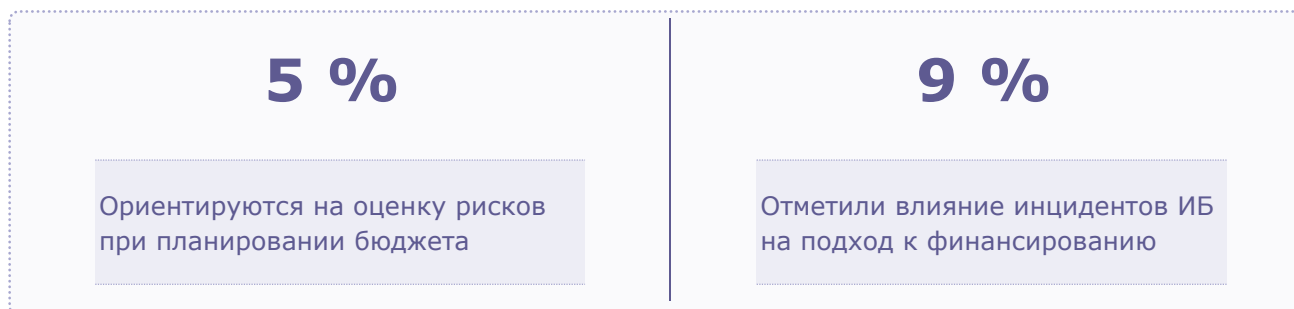
Диаграмма 6. На что вы опираетесь, определяя необходимый уровень затрат на ИБ?



Наиболее распространёнными практиками оказалось планирование бюджета экстенсивными методами, исходя из общего объема бюджета ИТ или операционных нужд поддержания работы информационной безопасности — такие подходы применяют 64% и 66% организаций соответственно.⁷

В итоге, несмотря на проведенную большинством респондентов оценку критичных рисков, только 5% (компании со средним бюджетом на ИБ в 348 млн руб./год) указали, что при принятии решения об объемах финансирования информационной безопасности ориентируются на эту оценку рисков и потенциальный ущерб от кибератак.

На изменение объемов инвестиций (бюджетов) на ИБ в российских компаниях влияет ряд факторов, отражающих как внутренние, так и внешние процессы. Согласно проведенному опросу, компании ориентируются в первую очередь на изменение финансовых показателей бизнеса (75% респондентов), т.к. поддержание текущего уровня или расширение деятельности требует пропорционального усиления мер защиты. Следующими по степени влияния на объем финансирования ИБ оказываются нормативные требования (государственное или отраслевое регулирование) и изменение численности штата организации, такие факторы подчеркнули 44% и 24% соответственно. И лишь 9% респондентов отметили существенное влияние инцидентов ИБ на изменение объема и подходов к финансированию ИБ.



⁷ Респонденты могли выбрать несколько подходов, которые используются при бюджетировании

Выводы

В условиях сохраняющейся высокой интенсивности кибератак на российские компании, а также усиления государственного регулирования, бизнес сталкивается с необходимостью укрепления своих систем информационной безопасности и обеспечения соответствия новым требованиям. Это создает устойчивый спрос на технические решения и услуги ИБ, подталкивает организации к пересмотру стратегий защиты и объемов инвестиций в информационную безопасность.

Целью данного исследования было выявление ключевых особенностей механизма формирования ИБ бюджетов заказчиков (прямых инвестиций в ИБ) и факторов, влияющих на рост или сокращение расходов на информационную безопасность внутри организаций:

1. **294 млн рублей в год – средний бюджет крупной компании на информационную безопасность**, что на 29% больше, чем в 2024 году. Лидерами по размеру бюджета являются компании ИТ и финансового сектора, бюджеты которых достигают в среднем 447 и 507 млн рублей в год.
2. **Финансирование ИБ происходит экстенсивно.** Наиболее распространённой практикой определения объемов финансирования ИБ оказалось планирование бюджета экстенсивными методами, исходя из общего объема бюджета ИТ или текущих операционных нужд поддержания работы ИБ. Такие подходы применяют 64% и 66% организаций соответственно.
3. **89% компаний проводят оценку критических рисков ИБ.** Практика формализации критических рисков при формировании стратегии информационной безопасности широко распространена среди крупных организаций РФ – 89% респондентов указали на применение риск-ориентированных методик, демонстрируя высокий уровень зрелости в решении этой задачи.
4. **Только 5% компаний ориентируются на оценку рисков при бюджетировании ИБ.** Несмотря на проводимую большинством респондентов оценку рисков кибербезопасности, только 5% указали, что при принятии решения об объемах финансирования (бюджета) на информационную безопасность ориентируются на проведенную работу по оценке рисков и потенциального ущерба от кибератак.
5. **Только 9% компаний отметили влияние инцидентов ИБ на изменение объема и подходов к финансированию ИБ.** Основными факторами, которые могут оказать существенное влияние на объемы бюджетов ИБ (как в большую, так и в меньшую сторону), оказались изменение финансовых показателей бизнеса (75% респондентов), нормативные требования (государственное или отраслевое регулирование) и изменение численности штата организации (44% и 24% соответственно). И лишь 9% респондентов отметили влияние инцидентов ИБ на изменение объема и подходов к финансированию ИБ.

Исследование показало уверенный рост инвестиций в информационную безопасность за последние несколько лет. Компании всё больше осознают степень важности кибербезопасности, но при этом можно сделать вывод о неустойчивой коммуникации в большинстве случаев между бизнесом и ИБ. Наблюдается качественный разрыв между практиками методологической оценки реальных угроз, рисков кибератак и практиками формирования бизнесом объема планируемых затрат на ИБ. Несмотря на то, что крупные российские организации в целом успешно справляются с кибератаками сегодня, наблюдается необходимость переосмысления подходов в работе ИБ с бизнесом для дальнейшего повышения качества и эффективности кибербезопасности.

 **Авторы**

Екатерина Кваша
Заместитель генерального директора



Выражаем благодарность **Роману Краснову**, основателю Фонда Цифровых Исследований «КиберПрогноз» за участие в подготовке данного материала

Методология проведения исследования

Исследование проводилось с мая по июнь 2025 года на основе анализа открытых источников, опроса заказчиков (пользователей) продуктов и услуг информационной безопасности. Опрос охватывал более 100 российских компаний - представителей крупного бизнеса. Целевую аудиторию опроса составили руководители финансового блока и руководители, ответственные за информационную безопасность, компаний таких отраслей как:

1. Топливо-энергетический комплекс
2. Ритейл
3. Горнодобывающий сектор
4. Государственный сектор
5. Промышленность (машиностроение, химическая, металлургия и др.)
6. Финансовый сектор
7. ИТ-сектор
8. Транспорт
9. Строительство

В данном исследовании объем инвестиций в информационную безопасность оценивался без учета затрат на оплату труда, обучение и повышение квалификации. При оценке и интерпретации результатов в спорных случаях мы исходили из принципа добросовестности игроков рынка и доверяли предоставленным сведениям.

ЦСР выражает благодарность всем участникам опроса за предоставленные сведения.

Диаграмма 7. Распределение организаций-респондентов по выручке

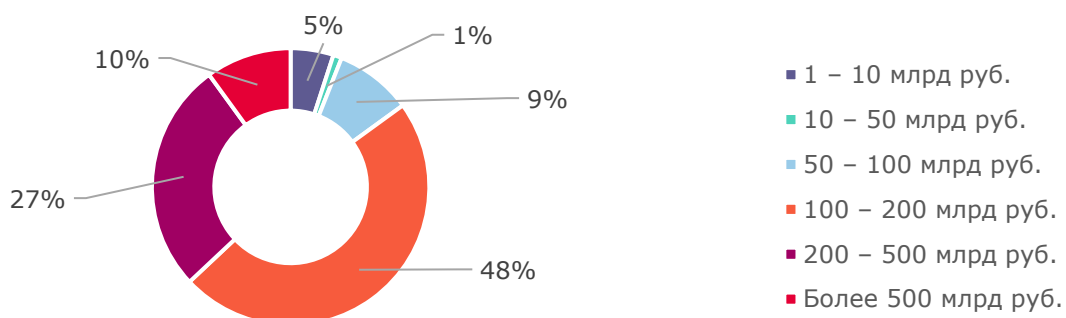
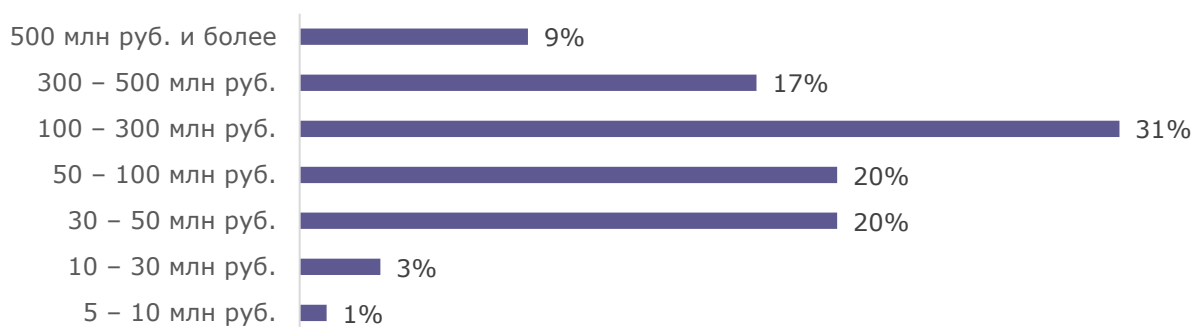


Диаграмма 8. Распределение организаций-респондентов по объему бюджета ИБ



© 2021 Фонд «Центр стратегических разработок» (ЦСР).
Все права защищены. При использовании информации
из документа ссылка на ЦСР обязательна.

Москва, 125009, Газетный пер., 3–5 стр. 1, 3 этаж
Тел.: +7 (495) 410-15-53
E-mail: info@csr.ru

csr.ru

