F6

Цепи в динамике: отраслевой отчет киберустойчивости бизнеса 2025-2026

Введение

Рост активов vs уровень защищенности

Киберугрозы продолжают эволюционировать и все заметнее влияют на устойчивость бизнеса. При этом меняется не только их количество, но и характер. Вместо точечных атак все чаще реализуются масштабные сценарии, затрагивающие сразу несколько элементов инфраструктуры и приводящие к сбоям ключевых бизнес-процессов.

Киберпреступность сформировалась как отдельная индустрия с собственной структурой и логикой работы. Атакующие выстраивают процессы по тем же принципам, что и их жертвы в корпоративной среде. Они формируют управленческую и операционную модель целых отделов и, как следствие, масштабируют операции, выбирая цели с максимальным эффектом. В этих условиях формальный подход к уровню угроз, а также фокус на отдельных мерах защиты увеличивает вероятность серьезных инцидентов.

В различных отраслях закрепляются новые сценарии атак. Так в финансовом секторе снижается доля попыток прямого хищения средств и усиливается акцент на деструктивное воздействие. Ключевыми приоритетами являются вывод из строя критически важных систем, нарушение доступности сервисов и репутационные потери. При этом атаки все чаще реализуются через дочерние компании подрядчиков и менее защищенные элементы инфраструктуры.

В данных условиях компаниям становится сложнее контролировать риски и своевременно выявлять потенциальные угрозы, что делает переход от точечных решений к системному управлению кибербезопасностью частью общей модели управления бизнесом.

Звенья одной цепи

В результате исследования экспертами F6 были выявлены следующие особенности. Подход к управлению активами в компаниях по-прежнему остается неоднородным. В одних организациях уже есть понятный учет, регулярная проверка и контроль, в других подход по-прежнему остается фрагментарным.

Компании продолжают наращивать цифровые активы во всех рассматриваемых периодах, вследствие чего снижается уровень защищенности, не успевая за ростом инфраструктуры.

Ключевая проблема заключается в том, что процессы управления не всегда успевают за этим ростом. Инфраструктура масштабируется быстрее, чем контроль над ней. В данном контексте уровень защищенности снижается. По итогам года часть компаний компенсирует ситуацию, тем не менее разрыв полностью не исчезает.

Отдельно выделяется ИТ-сектор, ставший лидером по оптимизации цифровых активов. Компании активно сокращают лишние и устаревшие ресурсы, наводят порядок в инфраструктуре и повышают ее управляемость, что подтверждает высокий уровень цифровой зрелости и системный подход.

Однако в рейтинге защищенности сектор занимает лишь пятое место, подтверждая общую тенденцию, что одного сокращения активов недостаточно.

Ключевая проблема кроется в масштабе и сложности инфраструктуры. Эффект от оптимизации нивелируется большим количеством сервисов, интеграций и зависимостей. Это создает дополнительную нагрузку на систему и увеличивает количество потенциальных точек входа.

Результаты отчета позволяют:

- увидеть, как рост цифровых активов влияет на уровень защищенности;
- понять, в каких отраслях риски выше;
- определить, где система работает устойчиво, а где есть уязвимости.

Полгода и год: куда движется рынок

В ходе исследования были проанализированы два временных среза, краткосрочный (октябрь 2025 – апрель 2026) и долгосрочный (май 2025 – апрель 2026), что позволило увидеть не только текущую ситуацию, но и понять, как меняется подход компаний со временем.

В разрезе последних шести месяцев наблюдается лишь незначительное увеличение уровня защищенности. Некоторые компании усилили процессы мониторинга и ревизии активов, при этом в ряде случаев изменения остаются точечными и не формируют устойчивой системы.

Однако при рассмотрении годового среза картина выглядит более уверенно. Компании, которые показывали умеренный прогресс, постепенно переходят к более системному управлению, демонстрируя улучшения в контроле за инфраструктурой, выстраивании процессов и более осознанной работы с рисками.

Таким образом, даже если краткосрочные показатели кажутся незначительными, в долгосрочной перспективе происходят изменения. Бизнес постепенно адаптируется к росту цифровых активов и уровню угроз, снижая вероятность серьезных последствий.

Факты и цифры

Анализ динамики цифровых активов компаний за несколько срезов — октябрь 2025 – апрель 2026 и май 2025 – апрель 2026.

Данные F6 Attack Surface Management

Среднее количество цифровых активов по отраслям

Отрасль	Оценка (Май 25)	Оценка (Окт 25)	Оценка (Апр 26)	Изменение (Окт 25 – Апр 26), %	Изменение (Май 25 – Апр 25), %
ИТ	5934	4157	4327,6	4,10%	-27,10%
Ритейл	1871	3445	2906,8	−15,62%	55,30%
Финансы	1682	1824	3617,3	98,32%	115,10%
Строительство	676	1811	2176,4	20,18%	222,00%
Промышленность	990	1310	1390,4	6,14%	40,40%
Транспорт и логистика	1303	1246	3790,5	204,21%	191,00%
ТЭК	1780	1206	1662	37,81%	-6,60%

Рост числа цифровых активов не всегда связан с развитием бизнеса или расширением инфраструктуры. В ряде случаев это результат отсутствия контроля, так как в процессе работы у компаний остаются неиспользуемые ресурсы, дублируются сервисы, накапливаются забытые точки доступа.

По итогам исследования ИТ-сектор показывает наибольший результат по сокращению числа активов. Компании системно убирают лишние и устаревшие ресурсы, упорядочивают инфраструктуру и повышают ее управляемость.

Такая динамика отражает более зрелый подход. Активами начинают управлять не разрозненно, а как целой системой. Это снижает избыточность и позволяет лучше контролировать инфраструктуру.

Уровень защищенности отраслевых инфраструктур

Данные F6 Attack Surface Management

Уровень защищенности отраслей

Отрасль	Оценка (Май 25)	Оценка (Окт 25)	Оценка (Апр 26)	Изменение (Окт 25 – Апр 26), %	Изменение (Май 25 – Апр 26), %
ТЭК	5	6,3	6,1	−3,17%	22,00%
Промышленность	5,4	5,8	6	3,45%	11,10%
Транспорт и логистика	4,8	6,3	5,9	−6,35%	22,90%
Финансовые организации	5,8	5,6	5,9	5,36%	1,70%
ИТ	5	5,6	5,4	−3,57%	8,00%
Ритейл	4	4,9	5,1	4,08%	27,50%
Строительство	5,7	5,5	4,9	−10,91%	-14,00%

Рейтинг на апрель 2026

Отрасль	№ в рейтинге
ТЭК	1
Промышленность	2
Транспорт и логистика	3
Финансовые организации	4
ИТ	5
Ритейл	6
Строительство	7

Остальные результаты показывают разнонаправленную динамику. Одни отрасли ускорили рост под давлением инцидентов, другие удерживают достигнутый уровень, оставшаяся часть находится в зоне повышенного риска.

Интересной особенностью является позиция ИТ-сектора. Несмотря на сокращение числа активов, компании этой отрасли занимают лишь пятое место в рейтинге защищенности. Таким образом, оптимизация инфраструктуры не всегда напрямую переходит в рост уровня безопасности, а эффективность защитных мер зависит от комплексного подхода к управлению активами и рисками.

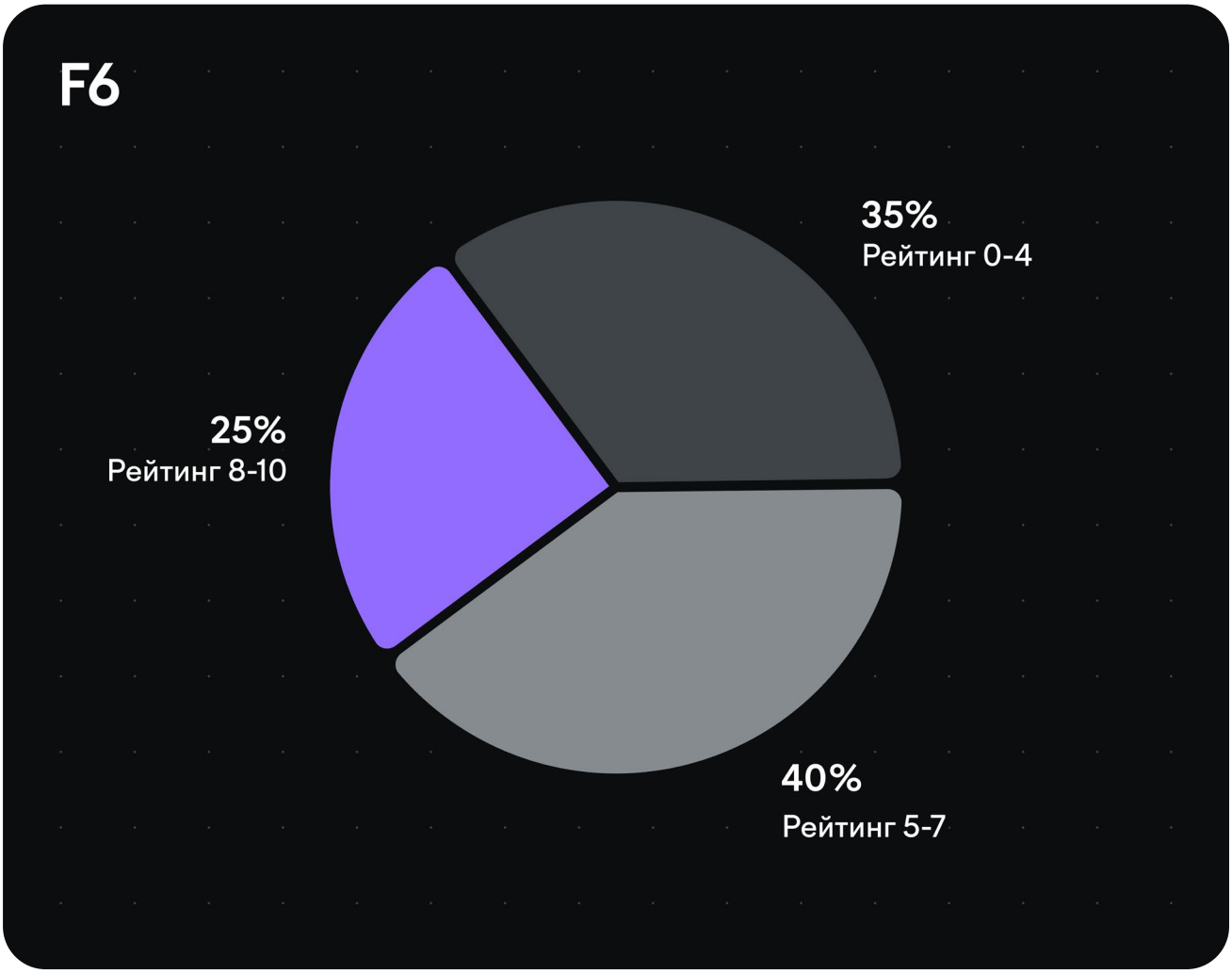
Ключевые значения

5,7 из 10
Средняя оценка
у проанализированных компаний

0,2 (ИТ)
Минимальный
зафиксированный балл

3071
Среднее количество цифровых
активов по отраслям

130 474 (Финансы)
Самое большое количество
активов



Анализ 1 000 компаний в ключевых отраслях экономики России, проведенный экспертами F6, выявил важные закономерности в уровне киберзащиты.

Рост цифровых активов по-прежнему остается устойчивым, что создает давление на системы и увеличивает зону экспозиции угроз. При этом в полугодовом срезе рост показателей защищенности в большинстве отраслей замедлился.

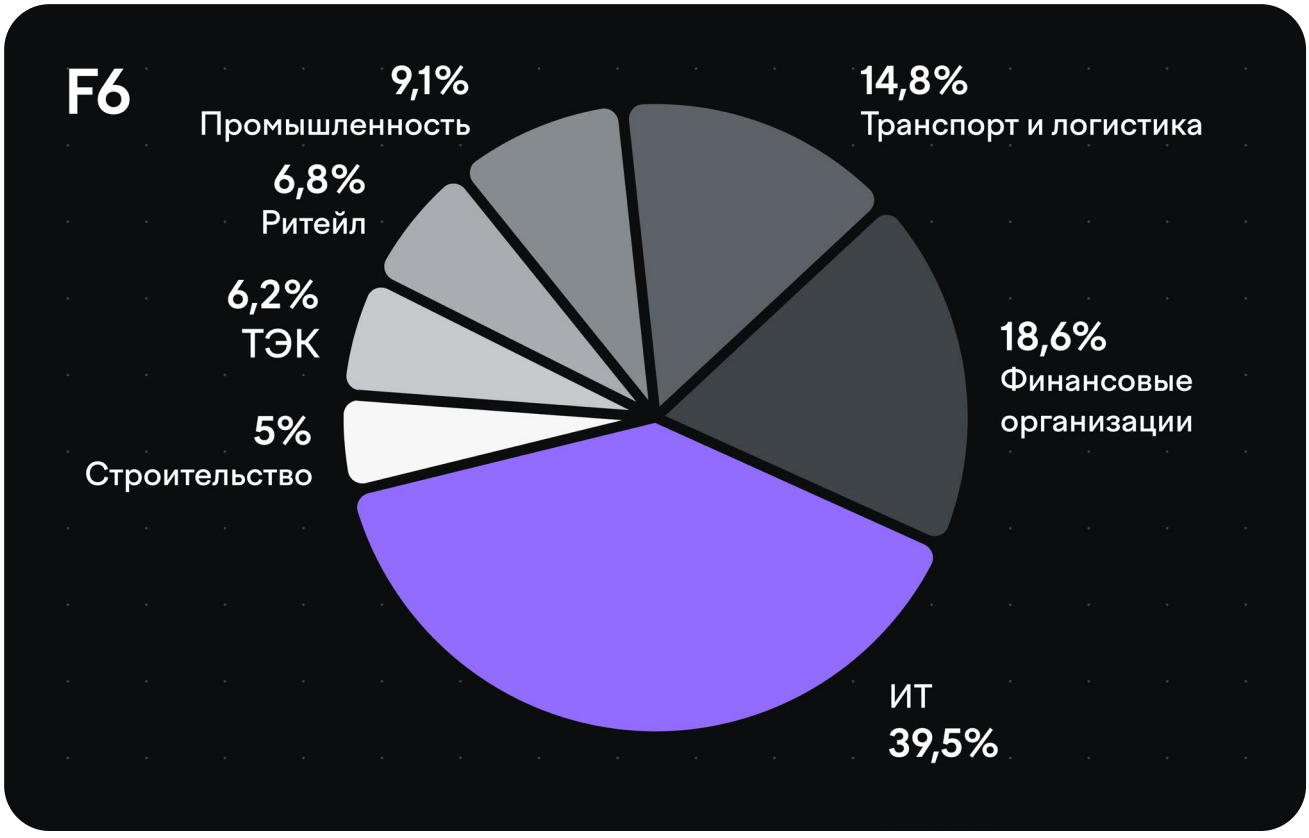
Большинство компаний остаются уязвимыми: **75%** имеют уровень защиты ниже **7 баллов**, **35%** — ниже **4**. При этом только **25%** компаний достигли диапазона **7–10 баллов**.

Минимальный зафиксированный балл составляет 0,2, который является абсолютным минимумом, зафиксированным у ИТ-компаний, и закономерным результатом масштабной инфраструктуры.

В некоторых секторах среднее количество цифровых активов уменьшилось, как и рекордные значения, указывая на планомерные шаги по оптимизации и упорядочиванию инфраструктуры.

Компании, выстраивающие решения системно и на основе анализа, опережают рост числа атак, в то время как фрагментарный подход превращает даже незначительные инциденты в серьезные последствия.

Среднее количество критических проблем по отраслям



ИТ-сектор ожидаемо лидирует по количеству критических проблем: высокие темпы развития и сложность инфраструктуры создают больше уязвимостей, чем бизнес успевает контролировать. Второе место занимают финансовые организации, где высокий уровень цифровизации и критичность сервисов увеличивают требования к устойчивости и выявляют больше значимых проблем. На третьей позиции транспорт и логистика, где рост распределенных систем и интеграций расширяет поверхность риска и усложняет контроль. Четвертое место делят промышленность, строительство и ритейл, для которых характерен разный уровень зрелости, но общим остается наличие уязвимостей на уровне процессов и управления инфраструктурой.

Вывод:

киберустойчивость все больше становится индикатором зрелости управленческих решений, показывая, где компании способны управлять рисками эффективно, а где находятся под постоянным давлением угроз.

Как проводился анализ

Отчет базируется на оценке данных **F6 Attack Surface Management** — системы, которая анализирует публичные цифровые активы компаний и степень контроля над ними.

В исследование включены **1 000 крупнейших компаний России и СНГ** из семи ключевых отраслей экономики.

Для каждой организации фиксировался набор внешних активов: домены, поддомены, IP-адреса, веб-приложения, SSL-сертификаты, облачные сервисы и интеграции с подрядчиками.

Затем оценивались ключевые параметры безопасности: актуальность обновлений, настройки DNS и TLS, состояние почтовой инфраструктуры, наличие уязвимых портов и следы возможных компрометаций в открытых источниках.

Все выявленные риски распределялись по восьми категориям, отражающим основные направления киберустойчивости:

1. Сетевая безопасность.
2. Почтовая инфраструктура.
3. DNS и доменные зоны.
4. Уязвимости и устаревшее ПО на внешнем периметре.
5. SSL/TLS-конфигурации.
6. Утечки данных.
7. Вредоносная активность.
8. Упоминания в дарквебе.

Каждая категория оценивается по шкале от 0 до 10, а итоговый балл компании вычисляется как среднее значение, которое демонстрирует уровень защищенности внешнего периметра.

На финальном этапе система консолидирует результаты и рассчитывает сводную оценку, отражающую уровень защищенности внешнего периметра компании на основе восьми вышеперечисленных категорий риска.

Эта оценка выступает единым цифровым индикатором, позволяя сопоставлять уровень защиты компаний, выявлять отраслевые тенденции и определять зоны риска, требующие приоритетного внимания.

Динамика по отраслям

Рынок кибербезопасности переживает трансформацию от эпизодических угроз к постоянному фону рисков.

Киберинциденты больше не исключение, а часть повседневной операционной реальности бизнеса.

В этих условиях компании вынуждены пересматривать подходы к защите, переходя от реакции на атаки к системному управлению рисками.

Однако скорость этих изменений остается неравномерной, формируя разрыв в уровне защищенности между отраслями.

ИТ и медиа

5,4	4 327	37 053
Средняя оценка	Среднее количество активов	Максимум активов

ИТ-компании показали впечатляющий прогресс в управлении цифровой инфраструктурой. Они активно упорядочили и сократили устаревшие и дублирующие ресурсы, внедрили стандартизацию систем и практики оптимизации. **В краткосрочной перспективе изменения минимальны (+4,1%), однако по итогам года сектор демонстрирует значительное сокращение активов (–27,1%).** Такие меры позволили повысить эффективность использования ресурсов и снизить избыточные нагрузки на инфраструктуру.

Однако, несмотря на успехи, ИТ-сектор демонстрирует снижение позиций в отраслевом рейтинге защищенности. Масштаб и сложность инфраструктуры остаются значительными, а оптимизация активов не всегда успевает компенсировать растущие зоны риска. **Это подчеркивает ключевую проблему, что даже лидеры в части цифровой зрелости сталкиваются с постоянным давлением на систему кибербезопасности и остаются уязвимыми для инцидентов.**

Большое количество внешних сервисов, облачных решений и подрядчиков увеличивает зону контроля, а слабый аудит может стать критически слабым звеном.

Вывод:

Успех в оптимизации активов не всегда напрямую отражается на рейтинге киберустойчивости, и скорость роста цифровой инфраструктуры остается критическим фактором риска. Оптимизация активов эффективно работает вместе с полным контролем инфраструктуры и внешних связей.

Топливно-энергетический комплекс (ТЭК)

6,1
Средняя оценка

1 662
Среднее количество активов

13 522
Максимум активов

Компании топливно-энергетического комплекса демонстрируют умеренный рост цифровых активов, сохраняя управляемость инфраструктуры и контроль над ключевыми системами. Отрасль последовательно усиливает практики кибербезопасности. Внедряет сегментацию сетей, контроль доступа, мониторинг технологических и корпоративных контуров, а также аудит интеграций с подрядчиками.

Дополнительное внимание уделяется защите критически важных систем. Компании развивают централизованный мониторинг, отслеживают изменения в конфигурациях и усиливают контроль за промышленными и ИТ-средами.

При этом остается технический долг в виде высокой сложности инфраструктуры, необходимости синхронизации ИТ и ОТ-сегментов, а также рисков, связанных с подрядчиками и цепочками поставок.

Вывод:

ТЭК демонстрирует, что даже при росте цифровых активов можно сохранять лидерство в защищенности за счет системного контроля и зрелых процессов на уровне всей инфраструктуры.

Промышленность

6,0
Средняя оценка

1 390
Среднее количество активов

15 065
Максимум активов

Компании промышленного сектора демонстрируют умеренный рост цифровых активов **(+6,% полугодовой срез, +40,4% за год),** сохраняя баланс между развитием инфраструктуры и ее управляемостью. Отрасль последовательно усиливает базовые практики кибербезопасности, внедряет сегментацию сетей, контроль доступа, мониторинг промышленных и корпоративных систем, а также выстраивает взаимодействие между ИТ и производственными контурами.

Вывод:

Промышленный сектор демонстрирует высокий уровень зрелости и занимает второе место в рейтинге, который достигается за счет баланса между развитием инфраструктуры и ее управляемостью.

Транспорт и логистика

5,9	3 790	62 876
Средняя оценка	Среднее количество активов	Максимум активов

Компании отрасли активно наращивают цифровые активы **(+204,2% в срезе май 25 – октябрь 25, +191% май 25 – апрель 26),** опережая другие сектора, и параллельно усиливают контроль инфраструктуры. Активно используется мониторинг сетевой активности, управление доступом и аудит интеграций с внешними сервисами и подрядчиками.

Дополнительно усиливается контроль за критическими системами. Компании внедряют централизованное логирование, отслеживают изменения в конфигурациях и повышают прозрачность цепочек поставок, что позволяет быстрее выявлять отклонения и потенциальные угрозы.

При этом отрасль продолжает сталкиваться с высокой зависимостью от распределенных систем, сложных цепочек интеграций, уязвимости в API и рисками, связанными с подрядчиками и логистическими платформами.

Вывод:

Высокий уровень защищенности возможен даже при росте инфраструктуры, но требует глубокого контроля всех интеграций и внешних связей.

Финансовый сектор

5,9
Средняя оценка

3 617
Среднее количество активов

130 474
Максимум активов

Компании финансовой отрасли сохраняют высокий уровень защищенности, при этом стремительно наращивая цифровые активы **(+98,3% по итогам полугодового среза, +115,1% в разрезе года).** Такой рост инфраструктуры остается управляемым благодаря системным процессам контроля, регулярному мониторингу и быстрой реакции на потенциальные угрозы.

Дополнительным фактором выступает регуляторное давление. Значительная часть организаций финансовой отрасли относится к объектам критической информационной инфраструктуры, где требования к кибербезопасности закреплены на уровне законодательства и обязательны к исполнению. В этих условиях обеспечение информационной безопасности становится прямым юридическим обязательством, несоблюдение которого влечет ответственность.

Череда кибератак, прошедшая в 2025 году, также сыграла немаловажную роль в формировании текущего рейтинга отрасли. Компании усилили защиту не только клиентских данных, но и всей инфраструктуры, делая ее более управляемой и устойчивой к угрозам.

Отрасль демонстрирует зрелый подход к кибербезопасности. Постоянное обновление систем, тщательный аудит подрядчиков и внимание к деталям превращают защиту в прогнозируемый и эффективный процесс.

Однако, сложность операций и внутренней инфраструктуры может приводить к непрозрачным зонам риска.

Вывод:

Финансовый сектор показывает, что высокая защищенность совместима с активным развитием инфраструктуры. Однако, системный контроль за подрядчиками и процессами остается критически важным для сохранения не только лидирующих позиций, но и устойчивости.

Ритейл

5,1
Средняя оценка

2 906
Среднее количество активов

24 556
Максимум активов

Компании торгового сектора смогли стабилизировать рост цифровых активов, аккуратно управляя инфраструктурой и минимизируя новые зоны риска **(-15,6% полугодовой срез, +55,3% за год).** Казалось бы, система работает слаженно, и инфраструктура находится под контролем, но отраслевой рейтинг фиксирует шестое место.

Инциденты последних месяцев показали, что слабое звено чаще всего скрывается не в технологиях, а в бизнес-процессах и работе с подрядчиками. Недостаточный контроль за внешними партнерами и их интеграциями остается ключевым источником уязвимостей, подчеркивая необходимость системного подхода к киберустойчивости и усиленного аудита всех подрядчиков.

Вывод:

при отсутствии контроля подрядчиков, учета активов и базовых управленческих процессов уровень безопасности не успевает за ростом бизнеса.

Строительство и девелопмент

4,9	2 176	27 342
Средняя оценка	Среднее количество активов	Максимум активов

Отрасль продемонстрировала резкий годовой рост цифровых активов **(+222%),** вследствие чего процессы безопасности не успевают за расширением инфраструктуры. В результате сектор занимает последнее, седьмое место, в рейтинге, что подчеркивает системную особенность. В отличие от отраслей, изначально развивавшихся в цифровой среде, таких как финансы и ИТ, строительный сектор относительно недавно начал интегрировать цифровые технологии в операционные процессы. Это отражается на уровне зрелости подходов к кибербезопасности.

Во многих компаниях информационная безопасность по-прежнему воспринимается как вспомогательная функция, а не как часть критической инфраструктуры бизнеса. Как следствие, инвестиции в эти направления остаются ограниченными, а процессы управления активами и рисками развиты недостаточно.

Такой разрыв между темпами цифровизации и уровнем зрелости управления приводит к накоплению уязвимостей, так как инфраструктура растет, но контроль над ней остается фрагментарным.

Вывод:

Для повышения киберустойчивости строительным компаниям необходимо усилить аудит подрядчиков, автоматизировать инвентаризацию активов и внедрить системный контроль за бизнес-процессами и доступом к инфраструктуре.

Баланс между ростом и управляемостью.

Картина, сложившаяся к апрелю, демонстрирует четкое расслоение отраслей по уровню киберустойчивости.

В верхней части рейтинга закрепились ТЭК, промышленность и транспорт с логистикой, те отрасли, где рост цифровых активов сопровождается выстроенными процессами контроля и системным управлением инфраструктурой.

На противоположной стороне находятся ИТ, ритейл и строительство. Несмотря на разную динамику, их объединяет общий фактор — разрыв между ростом активов и зрелостью процессов безопасности.

ИТ-сектор демонстрирует попытку взять инфраструктуру под контроль через оптимизацию и сокращение активов, однако этого оказывается недостаточно для удержания позиций в рейтинге. Ритейл стабилизирует рост, но сталкивается с уязвимостями в работе с подрядчиками и бизнес-процессах. Строительство и девелопмент, напротив, наращивают активы максимально быстро, что усиливает нагрузку на инфраструктуру и обостряет существующие риски.

Таким образом, ключевым фактором становится не сам объем цифровых активов, а способность компаний управлять ими как единой системой. Лидеры рейтинга показывают, что устойчивость формируется на уровне процессов через контроль изменений, прозрачность интеграций и дисциплину в работе с внешними сервисами.

В то же время отстающие отрасли демонстрируют, что даже отдельные успешные инициативы, будь то оптимизация активов или стабилизация инфраструктуры, не дают полного эффекта без системного подхода.

Вывод:

На этом фоне становится очевидно, что дальнейшее развитие бизнеса будет зависеть не столько от внедрения новых технологий, сколько от способности выстраивать системное управление цифровой средой, возможности предвидеть критически опасные сценарии и поддерживать работоспособность всех сервисов при наступлении таких сценариев. Именно в этой области сегодня формируется разница между устойчивостью и уязвимостью.

F6

Технологии для борьбы с киберугрозами

info@f6.ru +7 495 984-33-64 f6.ru