Ростелеком
Солар

Исследование рынка информационной безопасности в России по клиентским сегментам

2022 ГОД

Оглавление

1. Введение

В 2021 году группа рыночной аналитики компании «Ростелеком-Солар» впервые реализовала проект по оценке объема рынка информационной безопасности (ИБ) в России. В этом году стартовала вторая волна проекта, с уточнением данных и прогнозированием.

В данном исследовании освещается текущая ситуация на рынке ИБ в России, рассматривается движение сегментов, их объемы и занимаемые доли рынка, а также прогнозируется развитие рынка до 2025 года.

2. Методология

Этапы проведения исследования:

1

КАБИНЕТНОЕ ИССЛЕДОВАНИЕ:

оценка мировых трат на ИБ и экстраполяция данных на российский рынок.

Методология:

изучение данных аналитических агентств, анализ выручки компаний по отраслям, ее соотнесение с покупательской способностью.

2

АНАЛИТИЧЕСКИЙ ЭТАП:

оценка текущего объема продаж средств обеспечения информационной безопасности и прогноз по сегментам (для каждого сегмента своя методология).

Методология:

анализ данных закупок (44-ФЗ и 223-ФЗ, СПАРК-Интерфакс, данные РБК по крупнейшим компаниям, данные аналитических компаний партнеров).

3

КОЛИЧЕСТВЕННЫЙ ЭТАП:

оценка бюджетов на ИБ, а также сегментация клиентов и определение их характерных особенностей.

Методология:

количественный опрос потребителей по сегментам с использованием заранее утвержденной анкеты.

Параметры исследуемых сегментов

Общий объем рынка средств обеспечения информационной безопасности был рассчитан по 4-м основным сегментам, их параметры представлены в таблице:

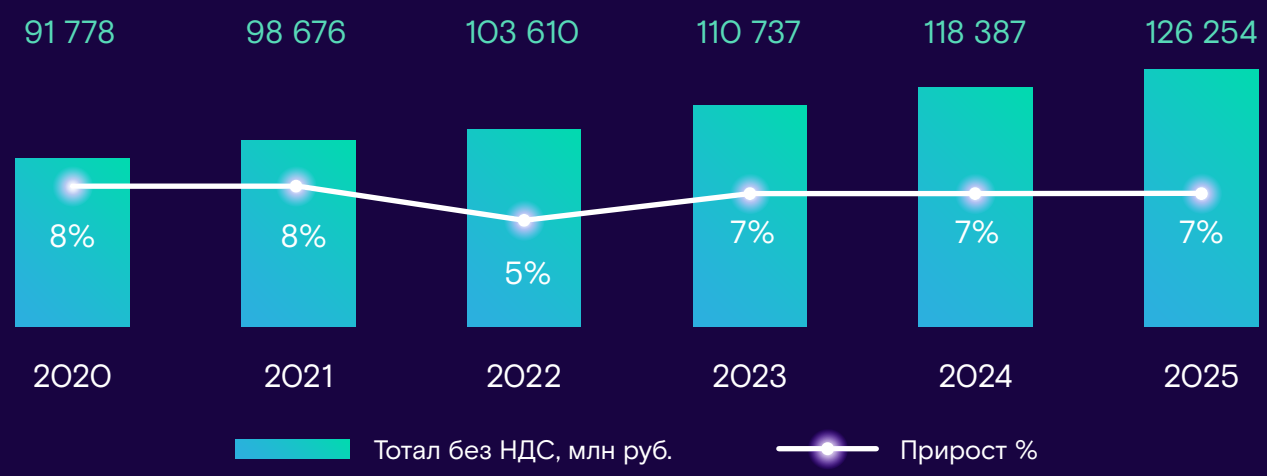
СЕГМЕНТ	
B2G	Федеральные и региональные органы исполнительной власти, силовые ведомства
B2E	Крупнейшие предприятия[1]
B2B	Сегмент 1 – СМБ, малые и микропредприятия[2]
	Сегмент 2 - средние предприятия[3]
	Сегмент 3 - крупные предприятия[4]
B2C/SOHO	Домашние пользователи, ИП

[1] Предприятия с годовой выручкой свыше 70 млрд руб.
[2] Предприятия с годовой выручкой менее 800 млн руб. и штатной численностью менее 250 сотрудников
[3] Предприятия с годовой выручкой от 800 млн до 5 млрд руб. и штатной численностью более 250 сотрудников
[4] Предприятия с годовой выручкой от 5 млрд руб. и штатной численностью более 250 сотрудников

3. Объем рынка информационной безопасности в России

В денежном выражении общий объем рынка информационной безопасности (со стороны трат конечных пользователей) в 2021 году составил ~ 98,6 млрд руб. без НДС. Прирост по отношению к предыдущему году положительный и составляет 8%. При построении прогнозных объемов продаж учитывались данные за I квартал 2022 года, а также прирост по отношению к предыдущим периодам и прогнозные данные аналитических агентств партнеров.

Рис. 1. Динамика общего объема рынка информационной безопасности в денежных тратах конечных пользователей



В 2022 году объем рынка ожидается на уровне 104 млрд руб., рынок замедлит свой рост в основном за счет сокращения бюджетов в сегменте B2B и вырастет на 5% по сравнению с итогами 2021 года.

Факторы роста:

- Кратный рост угроз кибербезопасности. Многие сценарии, о которых говорилось как о теоретических, стали реальностью – бизнес вынужден защищаться
- Регуляторное давление. Государство усилило давление как на бизнес, так и на собственные структуры с целью повышения киберзащиты. Прежде всего это Указ Президента РФ от 01.05.2022 № 250, Указ Президента Российской Федерации от 30.03.2022 № 166 и ряд других нормативных документов
- Нехватка специалистов, а также уход многих технологических компаний при возросшем уровне атак вынуждает российские организации искать сервисных подрядчиков, которые могли бы взять на себя работы по резкому усилению киберзащиты и постоянному поддержанию этого высокого уровня
- Благоприятная налоговая политика для ИТ-компаний
- Импортозамещение

Угрозы (риски)

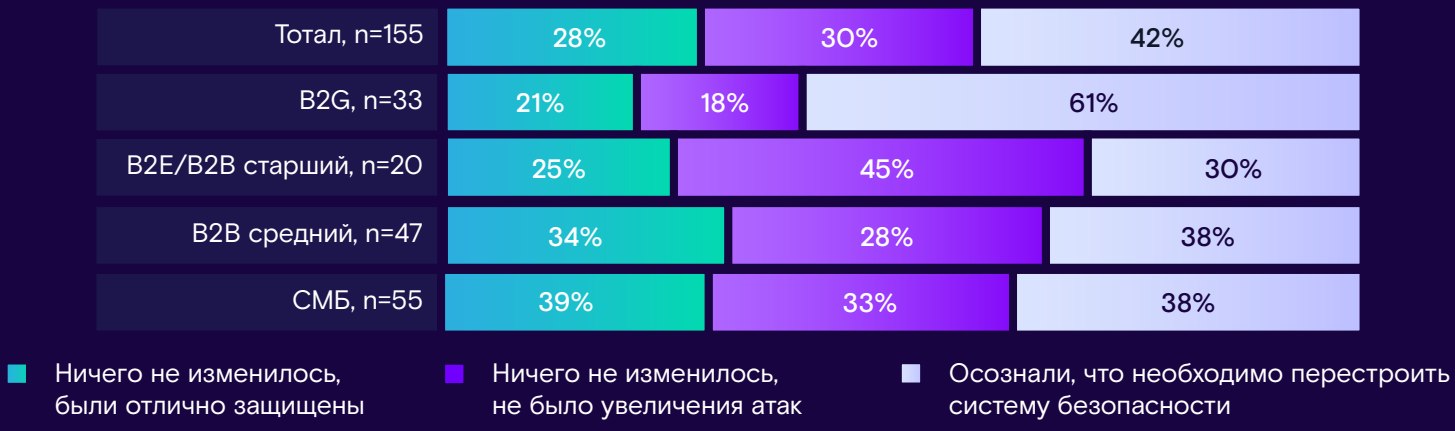
- Сегмент среднего и малого предпринимательства сильно сократил свои затраты на киберзащиту
- Значительная утечка/нехватка талантов/специалистов области
- Ограниченное использование глобальных облачных сервисов из-за санкционного риска, правил защиты персональных данных и политики импортозамещения
- Уход западных игроков – затраты на иностранные (покупка, эксплуатация) СЗИ составляли существенную часть затрат на кибербезопасность. Российские решения есть не во всех сегментах, также они чаще всего дешевле западных аналогов. В результате компании не закупают ни обновления иностранных решений (они недоступны), ни российские решения, если они не работают, как требуют клиенты, что приводит к фактическому падению затрат в 2022 году и в целом к замедлению роста рынка

4. Параметры потребления кибербезопасности

Российский заказчик ожидает появления возможности комплексного решения проблем в области кибербезопасности и удобных инструментов коммуникации для выстраивания взаимоотношений. Очень осторожно подходит к выбору партнера и смотрит на «исторические данные компании поставщика», что говорит о желании развивать долгосрочное партнерство, а не решать «сиюминутную проблематику».

В тоже время 42% (!) компаний в РФ осознали необходимость перестройки системы безопасности после февраля 2022 года. В основном это компании сегмента B2G (более 60% ФОИВ и РОИВ).

Рис. 2. Изменения в кибербезопасности с начала 2022 года



Среди основных причин такой перестройки можно выделить замену инфраструктуры в целом и требования регуляторов (в рамках импортозамещения), что выгодно для российских ИБ-компаний. В условиях, когда большинство иностранных производителей СЗИ покинули российский рынок, стремительно вырос спрос на отвоеванные решения, что дает возможность заместить их при наличии технологий.

При этом в коммерческих компаниях основным фактором перестройки системы также служит кратный рост угроз кибербезопасности и, как следствие, недостаточно высокий уровень защиты, сложность и дороговизна поддержки.

Целевые атаки (26%) и троянцы-шифровальщики (32%) – наиболее опасные атаки, по мнению респондентов, а общая ИТ- и сетевая инфраструктура наиболее уязвимы к угрозам.

В среднем компании сталкиваются с 3 крупными инцидентами в год, а средний ущерб от инцидента составляет 4–6 млн руб. В свою очередь средняя сумма на восстановление составляет около 2 млн, а длительность пресечения – около 4 дней.

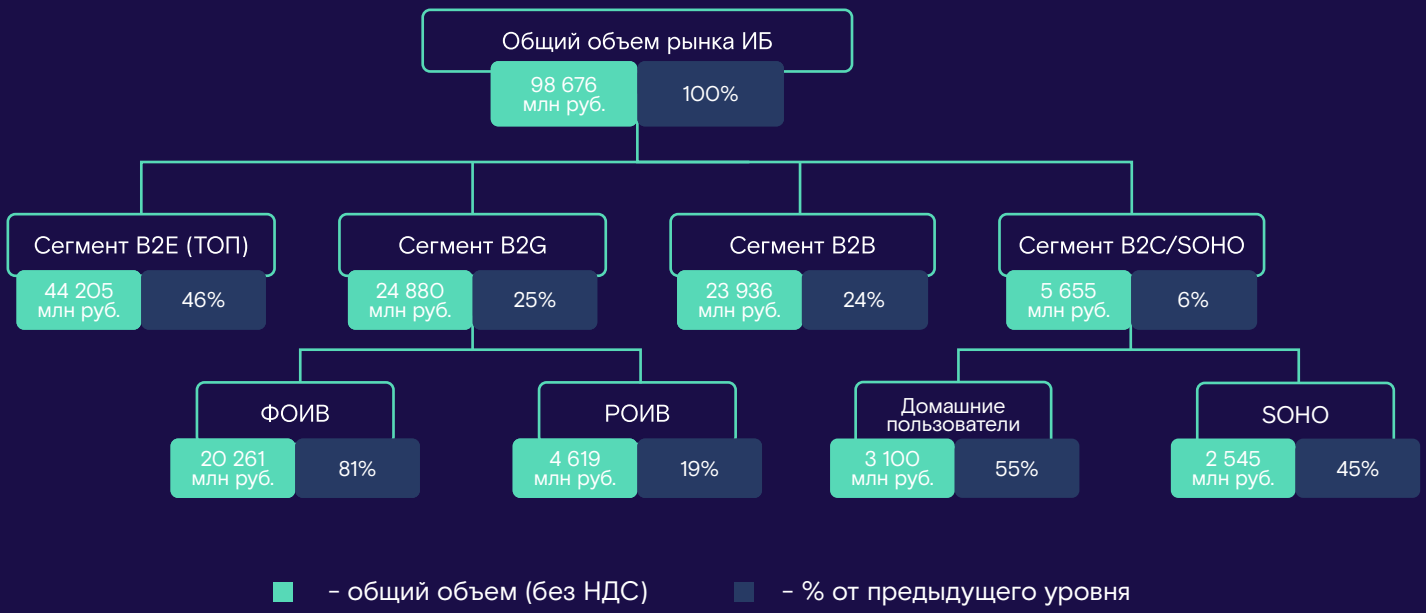
Основными мерами после инцидентов называют усиление и развитие ИБ-инфраструктур и разработку планов реагирования.

5. Структура рынка информационной безопасности в России

Для того чтобы наиболее точно построить модель прогноза рынка ИБ до 2025 года, необходимо спуститься на уровень ниже и рассмотреть его сегментно.

Структура распределения объема ИБ-рынка по клиентским сегментам в 2021 году представлена на рисунке 3.

Рис 3. Структура трат рынка информационной безопасности по сегментам в 2021 году, без НДС



5.1 Сегмент B2E

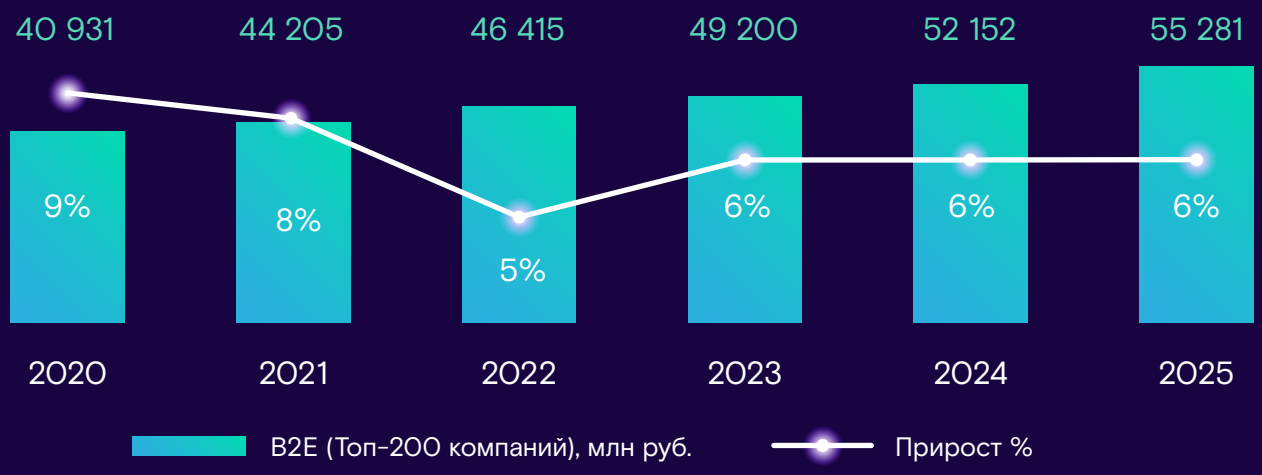
В 2021 году в денежном выражении составлял большую часть рынка – около 45–50%, ~44 млрд руб.

Данный сегмент не будет снижать темпы трат на ИБ, а будет демонстрировать прирост, однако не такой быстрый, как прогнозировалось нами в конце 2021 года, и составит в 2022 году ~ 46,4 млрд руб. без НДС.

Факторы роста:

Компании сегмента столкнулись с кратным ростом угроз кибербезопасности начиная с февраля 2022 года, однако не сократили расходы на ИБ, а переориентировали их в рамках комплексных подходов к защите. Также в связи с уходом вендоров все чаще вставал вопрос об импортозамещении. По результатам проекта, в 30% коммерческих компаний доля отечественных средств защиты составит более 50% уже к концу 2023 года.

Рис 4. Динамика объема рынка информационной безопасности в сегменте B2E



Наиболее важными киберинцидентами компании сегмента называют компрометацию инфраструктуры (включая контроллеры доменов), утечку баз данных с персональными и/или финансовыми данными клиентов, а также хищение денежных средств со счетов компании.

Чаще всего компании не оценивают потери в ходе киберинцидентов (почти 2/3 компаний не производили оценку). Наибольшие потери среди тех, кто все же оценивает, приносят: хищение денежных средств со счетов компании – в среднем 20,8 млн руб.; приостановка бизнес-процессов вследствие кибератаки – 18,4 млн руб.; утечка/утрата конфиденциальной информации, включая ноу-хау, интеллектуальную собственность, – 18,1 млн руб.

Несмотря на большую численность сотрудников, компании достаточно быстро восстанавливаются после инцидентов – на восстановление требуется от 3 до 7 дней в зависимости от типа инцидента.

Большинство компаний проводят расследования киберинцидентов своими силами примерно 1 раз в год.

5.2 Сегмент B2G

В данный сегмент мы включаем федеральные и региональные органы исполнительной власти (в том числе проекты по цифровой экономике и закрытые статьи), а также силовые ведомства.

В сегмент B2G входят ФОИВ (более 80% от всех трат сегмента), бюджеты которых распределены по следующим каналам:

1. Собственная безопасность, это примерно 10 млрд руб. – тут не будет падения трат, так как бюджеты системообразующих органов будут перераспределяться, смещаясь в сторону комплексного подхода к защите и под действием регуляторного давления.

2. Закрытые статьи (гособоронзаказ и закрытые контракты).
3. ГИС, проекты по цифровой экономике (от Минцифры) – тут мы видим значительное увеличение бюджетов как со стороны поступающих к нам запросов, так и со стороны анализа рынка (закупочных баз, интервью с экспертами и т. п.), а также посредством перераспределения в связи с регуляторной нагрузкой.

В целом государство усилило давление как на бизнес, так и на собственные структуры с целью повышения их киберзащиты. Прежде всего по требованиям Указа Президента Российской Федерации от 01.05.2022 № 250, Указа Президента Российской Федерации от 30.03.2022 № 166 и ряда других нормативных документов.

B2G-сегмент – это 25% рынка, и его рост год от года составляет 10%. Согласно прогнозам, этот рост сохранится и останется основным драйвером рынка информационной безопасности в России.

Рис 5. Динамика объема рынка информационной безопасности в сегменте B2G

Наиболее важными киберинцидентами представители сегмента называют заражение сети, сегментов инфраструктуры ВПО, контроль сетевого оборудования, а также утечку баз данных с персональными и/или финансовыми данными.

Большинство органов государственной власти проводят расследования киберинцидентов своими силами примерно 1 раз в год. Лишь 32% имеют собственное подразделение SOC.

5.3 Сегмент B2B

Емкость сегмента B2B (старший, средний, СМБ) в денежном выражении, согласно прогнозам, в 2022 году снизится на 1% и составит 23,8 млрд руб. Связано это прежде всего с сокращением выручки компаний, экономией на ИТ, уходом с рынка.

Рис 6. Динамика объема рынка информационной безопасности в сегменте B2B

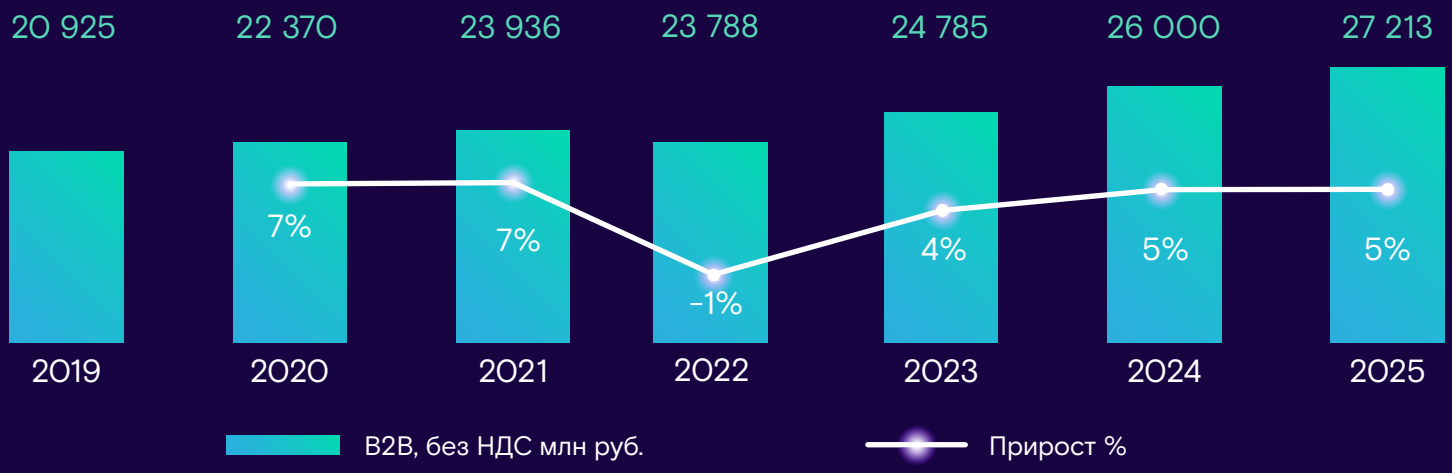


Рис 7. Динамика объема рынка информационной безопасности в B2B по сегментам

	2020	2021	2022	2023	2024	2025
B2B (сегмент 1), млн руб.	12 318	13 181	13 312	14 111	15 099	16 156
Прирост B2B (сегмент 1), %		7%	1%	6%	7%	7%
B2B (сегмент 2), млн руб.	7785	8252	8087	8330	8580	8751
Прирост B2B (сегмент 2), %		6%	-2%	3%	3%	2%
B2B (сегмент 3), млн руб.	2267	2503	2388	2344	2322	2306
Прирост B2B (сегмент 3), %		10%	-5%	-2%	-1%	-1%

Наиболее важными/опасными типами инцидентов компании сегмента называют компрометацию инфраструктуры (включая контроллеры доменов), приостановку бизнес-процессов вследствие кибератаки, а также хищение денежных средств со счетов компании.

Восстановительные работы в зависимости от типа инцидента занимают от 4 до 11 дней.

5.4 Сегмент B2C

Траты на информационную безопасность сегмента B2C/SOHO в 2021 году составили ~ 6% от общих трат сегмента, или 5,6 млрд руб. Согласно прогнозам, общий объем сегмента в денежном выражении к 2025 году составит 7 млрд руб.

6. Выводы

Компании в РФ осознали необходимость перестройки системы безопасности к концу 2022 года. Это связано с рядом факторов, основные из них:

- Кратный рост угроз кибербезопасности. Многие сценарии, о которых говорилось как о теоретических, стали реальностью – бизнес вынужден защищаться.
- Регуляторное давление. Государство усилило давление как на бизнес, так и на собственные структуры с целью повышения киберзащиты.
- Необходимость в импортозамещении.

В целом факторы не дали рынку просесть и позволили обеспечить его рост в деньгах конечных пользователей, хотя и не такой высокий, как было спрогнозировано годом ранее. Причем драйвером роста, как и в предыдущем году, является сегмент B2G (ФОИВ и РОИВ).

Ростелеком
Солар

rt.ru
rt-solar.ru

E-mail:
info@rt-solar.ru
support@rt-solar.ru

По вопросам исследований
research_group@rt-solar.ru

Телефоны:
+7 (499) 755-07-70 — продажи и общие вопросы
+7 (499) 755-02-20 — техническая поддержка

125009, Москва, Никитский пер., 7, стр. 1.