Сайберус

ИНСТИТУТ ЭКОНОМИКИ РОСТА ИМ. СТОЛЫПИНА П.А.

Кибербезопасность России: сила технологического развития

cyberus.com

2026

Резюме
исследования

Фонд развития результативной кибербезопасности Сайберус совместно с Институтом экономики роста им. П.А. Столыпина представляет результаты исследования основных этапов развития российской индустрии кибербезопасности, ее текущего состояния и роли в экономике.

Обращение авторов

Какую современную российскую отрасль можно сравнить с… советской космической программой — по влиянию на экономику, технологии и имидж страны? На наш взгляд — кибербезопасность.

«С чего вдруг?», — скажете вы. Космос был символом эпохи: о запуске спутника и полете Гагарина знала вся страна, за ними следил весь мир. Кибербезопасность — ее противоположность: она редко оказывается в центре внимания, да и едва ли вы назовете хотя бы одного «космонавта», бороздящего киберпространство.

Однако сходств больше, чем различий. Как и космическая отрасль, кибербезопасность — это сильная инженерная школа, нестандартное мышление и опыт создания собственной индустрии с нуля. Небольшое сообщество специалистов разрабатывает решения, которыми ежедневно пользуются миллионы.

Кибербезопасность обеспечивает надежность цифровой среды — от госуслуг и банков до промышленности и космоса. За четверть века Россия сформировала одну из немногих в мире суверенных отраслей кибербезопасности с полноценной экосистемой решений, компаний и экспертизы.

При этом ее роль остается недооцененной, хотя именно она формирует доверие к технологиям и устойчивость инфраструктуры.

Это исследование — попытка осмыслить путь отрасли и ее значение для цифрового развития страны. Мы рассматриваем кибербезопасность не только как составляющую технологического лидерства, но и как основу для сотрудничества с нашими зарубежными партнерами, которые сегодня также ищут надежные модели построения цифровой экономики и достижения киберсуверенитета — и могут опереться на наш опыт.

А еще это приглашение к диалогу о том, как распорядиться этим наследием и каким может быть будущее отрасли.

Сергей Войнов,

управляющий директор
фонда «Сайберус»

Уважаемые коллеги!

Представляем вашему вниманию исследование, посвященное российской индустрии кибербезопасности. На наш взгляд, это именно тот российский сектор, который по праву можно назвать по-настоящему конкурентным в экономике XXI века — экономике будущего.

Безопасность всегда была и остается базовым столпом устойчивости любого государства. Сегодня, в эпоху тотальной цифровизации, этот столп обретает новое, критическое измерение. Мир столкнулся с лавинообразным ростом кибератак, которые наносят ущерб, исчисляемый триллионами, дестабилизируя работу компаний, государственных органов, систем здравоохранения и образования. В этих условиях кибербезопасность становится не просто технической функцией, а фундаментом стабильности операционной деятельности и национальной экономики в целом.

Уникальность российского опыта, подробно раскрытая в данном докладе, заключается в том, что в России был пройден путь от пионера индустрии до построения собственной зрелой школы. Менее чем за 15 лет отрасль дважды кардинально трансформировалась, доказав свою способность к адаптации и самовоспроизведению. События последних лет стали стресс-тестом, который отечественная школа выдержала: несмотря на беспрецедентное внешнее давление и уход ключевых иностранных вендоров, цифровая инфраструктура страны устояла. Это стало возможным благодаря своевременной политике государства, развитию собственного технологического стека и сильнейшему сообществу профессионалов.

Сегодня мы видим, что отрасль информационной безопасности стала полноценным драйвером экономического роста. Ее прямой и косвенный вклад в ВВП исчисляется триллионами рублей, а каждый вложенный в защиту рубль многократно окупается, предотвращая ущерб. Мы обладаем высококонкурентным рынком с полным спектром отечественных решений и передовыми методиками оценки киберзащищенности.

Накопленный Россией опыт — это не просто внутреннее достояние. В условиях нарастающих глобальных рисков он может стать надежной базой для построения национальных школ кибербезопасности в других странах. Экспорт модели, технологий и компетенций — это то ценное, что Россия сегодня может и должна предложить своим международным партнерам, внося вклад в формирование устойчивого и безопасного цифрового пространства будущего.

Приглашаю вас к ознакомлению с исследованием.

Антон Свириденко

Исполнительный директор
Института экономики роста
им. П.А. Столыпина

Оглавление

Об исследовании

Периметр и цели исследования

Исследование посвящено анализу российской индустрии кибербезопасности как комплексной системы, состоящей из трех ключевых и взаимосвязанных компонентов:

1. Рынок и технологии (компании, продукты и решения, продажи);
2. Люди (подготовка кадров, специалисты и роли, сообщество);
3. Оценка эффективности (подходы и методы оценки защищенности).

Ключевые задачи:

— системно описать пусть становления отрасли, выявить закономерности ее развития

— проанализировать текущее состояние рынка, его основные характеристики,

— оценить роль индустрии кибербезопасности в российской экономике.

В рамках исследования было выделено три этапа становления индустрии: развитие по модели уязвимого паритета до 2016 г., фокус на отечественные технологии с 2017 по 2021 гг., переход к киберсуверенитету с 2022 гг. Каждый этап рассмотрен последовательно через призму трех компонентов для определения его ключевых особенностей. Далее приведена оценка общего вклада отрасли в российскую экономику.

Исследование проводилось по открытым источникам по состоянию на 4 квартал 2025 г. — 1 квартал 2026 г. Понятия «информационная безопасность» и «кибербезопасность» использованы как синонимы.

Партнеры

Выражаем благодарность представителям индустрии кибербезопасности, которые также приняли участие в подготовке исследования

SOLAR positive technologies

F6 CyberED

Ключевые выводы

Кибербезопасность — индустрия, которая формирует доверие к технологиям, поддерживает инновации и становится значимым фактором развития экономики страны в цифровую эпоху. За последние 15 лет отрасль смогла дважды трансформироваться и перейти к модели киберсуверенитета, потенциально воспроизводимой в других странах.

ЭКОНОМИКА

Скрытый драйвер роста: более 3,6 трлн руб. — оценка совокупного вклада индустрии в экономику страны в 2025 году

Прежде всего, это эффекты для отраслей с высоким уровнем цифровизации. При доле в интернет-экономике — всего 1,3% — ИБ-отрасль защищает основу цифрового развития России.

ИНВЕСТИЦИИ

Экономика защиты для компаний: каждый рубль, вложенный в ИБ-решения, может давать тройную отдачу

Вложения в ИБ-решения в 2024 году помогли крупным компаниям предотвратить прямой ущерб от кибератак в размере от 0,4 до 1,1 трлн руб.

ТРАНСФОРМАЦИЯ

Непрерывное развитие: динамика отрасли обеспечивается ее новаторством и адаптивностью

Масштабная цифровизация с 2017 года дала новый импульс к развитию рынка и отечественных ИБ-игроков. После 2022 года это поспособствовало плавному переходу к модели киберсуверенитета.

ГОСПОЛИТИКА

Всегда в фокусе: последовательная госполитика — фактор успеха индустрии

Кибербезопасность была и остается приоритетом цифровой трансформации страны. Это создало почву для устойчивого развития рынка и инноваций, в том числе для появления передовых подходов к измерению киберустойчивости.

ТЕХНОЛОГИИ

100% сделано в России: полный стек решений

Рынок кибербезопаности сегодня — конкурентная среда и 200+ отечественных решений от 100+ вендоров*, обеспечивающих страну ключевыми компонентами киберсуверенитета.

ЛЮДИ

Сила в людях: в России одно из самых мощных ИБ-сообществ в мире

В 5 раз увеличилась аудитория отраслевых конференций с 2021 года. Больше 100 тыс. специалистов обеспечивают кибербезопасность в разветвленной структуре ИБ-ролей.

*Российские поставщики решений с выручкой более 100 млн руб. в год в категории СЗИ по открытым данным.

Роль кибербезопасности в эпоху цифровизации

За последние 15 лет цифровизация заметно изменила российскую экономику и способы взаимодействия государства, бизнеса и общества.

Цифровой ландшафт российской экономики сегодня

32,2 трлн руб.

прогноз объема цифровой экономики по итогам 2025 г.[1]

74,7%

уровень цифровой зрелости ключевых отраслей и социальной сферы в 2023 г.[2]

>1,5 млн

ИКТ-специалистов[3]

>99%

государственных и муниципальных услуг оказываются в электронной форме[4]

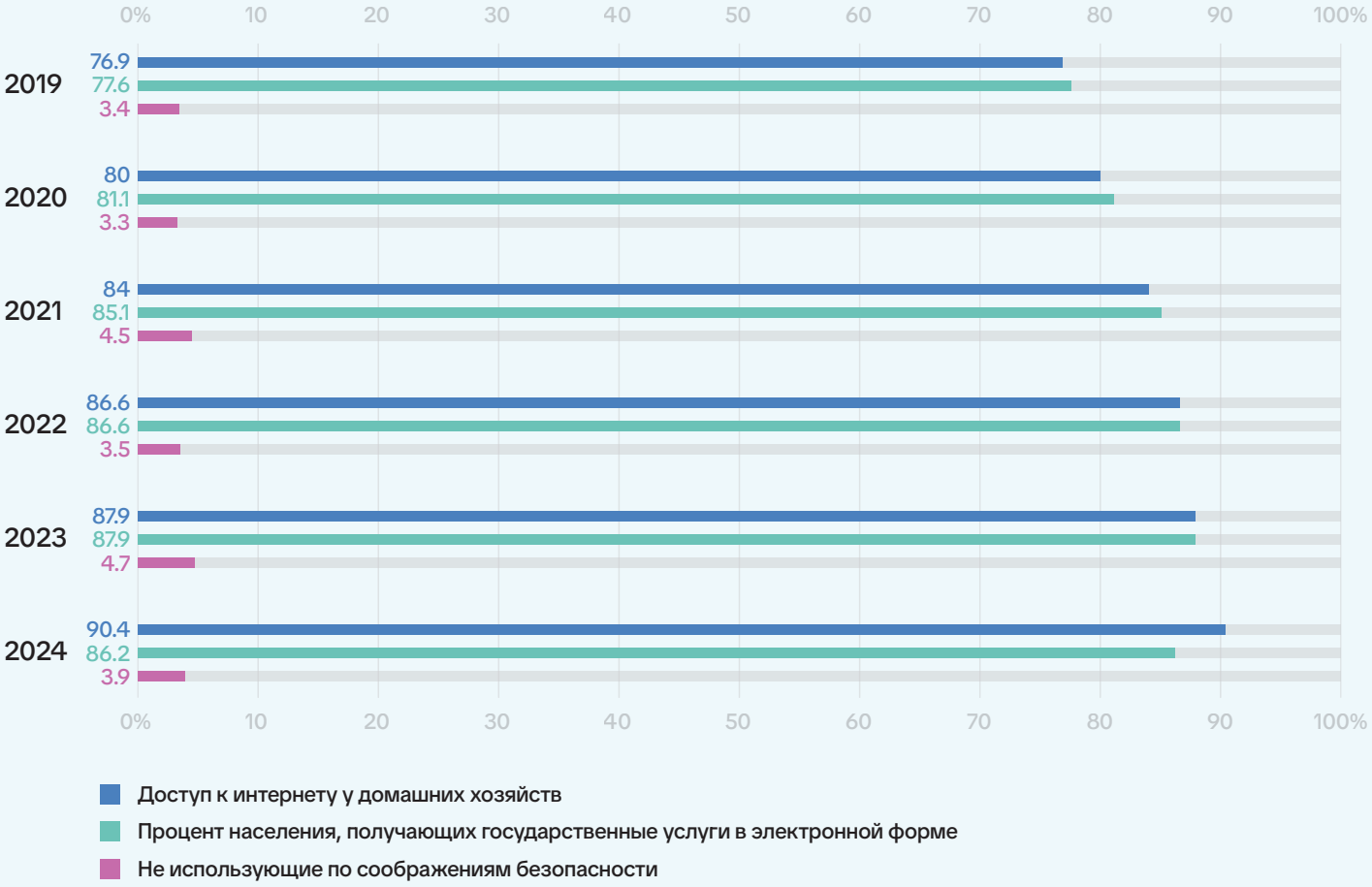
Источники: Минцифры России, РАЭК, ИСИЭЗ ВШЭ

Оценка объемов интернет-экономики уже в 2025 г. превышает 30 трлн руб., показывая темпы роста на уровне 30–40% ежегодно[1]. Почти половина всех российских организаций теперь используют интернет для получения цифровых сервисов и обучения персонала[1]. А численность специалистов в сфере ИКТ составила более 1,5 млн человек[3].

По уровню цифровизации государственных услуг Россия входит в число стран-лидеров по данным ООН[6] и Всемирного банка[7]. Доля населения, получающая госуслуги в электронном виде, превысила 86%[8].

Одним из факторов роста цифровых отраслей стало цифровое доверие — уверенность пользователей в надежности и защищенности ИТ-инфраструктуры и решений. При повсеместном доступе к интернету доля людей, не использующих интернет по причинам безопасности, остается на крайне низком уровне.

Цифровое доверие в российской экономике



Источники: ИСИЭЗ, Росстат

Обратная сторона стремительного цифрового развития — новые угрозы и постоянный рост атак со стороны злоумышленников.

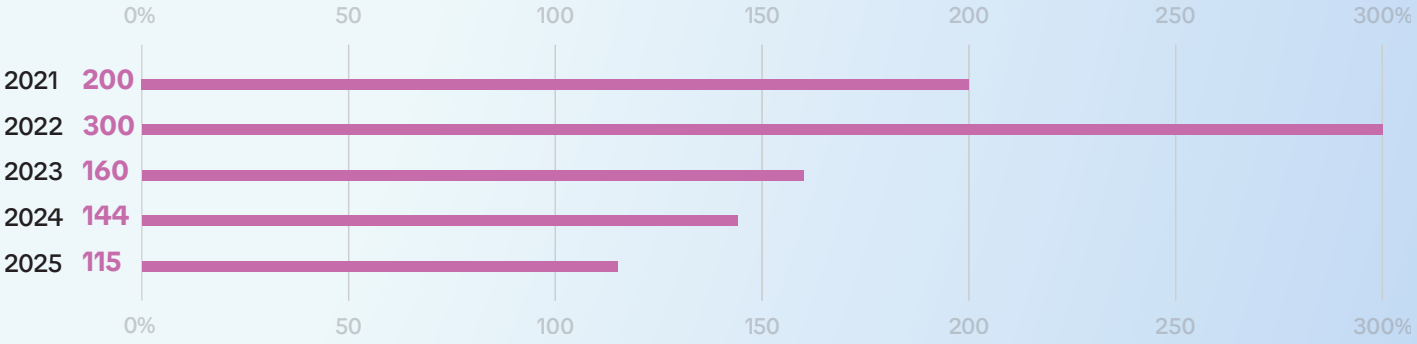
По мере дальнейшего развития технологий растущий цифровой ландшафт экономики все больше привлекает злоумышленников. А в месте с ним в зоне риска оказываются и объекты из реального мира. Статистика в индустрии во многом неоднородна, но отражает одни и те же тенденции: рост количества инцидентов, схожий выбор целей и усложнение векторов атак. При этом с 2022 г. экономика столкнулась с еще большим давлением и двукратным увеличением числа атак по сравнению с предыдущим годом по некоторым оценкам[9]. Для сравнения по оценкам Всемирного банка число публично известных киберинцидентов в мире растет в среднем на 21% в год[10].

Программы-вымогатели (ransomware) по-прежнему называют ключевой киберугрозой для российского бизнеса с 2021 г.[11]

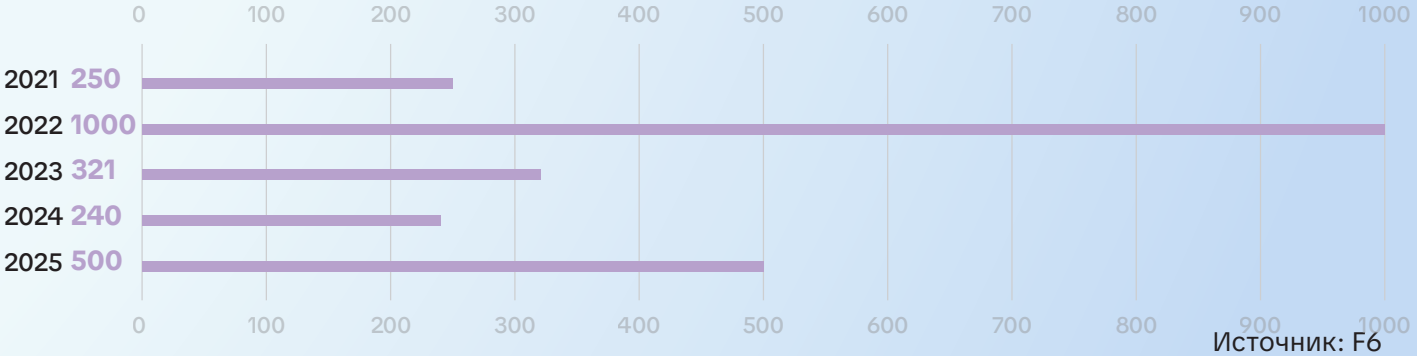
1 млрд руб.

составил максимально запрошенный выкуп от вымогателей в 2022 г.[12]

Рост количества программ-вымогателей



Максимально запрошенный выкуп, млн руб.



Источник: F6

В марте 2022 г. был зафиксирован всплеск и DDoS-атак — их количество выросло практически в 8 раз. Среди них были зафиксированы рекордные по мощности и продолжительности атаки. Самая продолжительная длилась практически 3 месяца[13].

В сложившихся условиях российская кибербезопасность была проверена на практике и показала свою эффективность. С 2000-х гг. отрасль прошла путь от точечных инноваций, получивших признание на мировом уровне, до одной из самых комплексных и зрелых экосистем в мире, предлагая новую модель построения киберсуверенитета.

Как трансформировалась индустрия. Факторы успеха

Российская отрасль кибербезопасности сегодня доказывает свою зрелость, устойчивость и способность создавать значимую добавленную стоимость. Суверенные технологии кибербезопасности — неотъемлемая часть технологического лидерства страны. Оно возникает там, где знания, инженерная культура, нестандартное мышление и энергия созидания складываются в целостную модель. Для ВЭБ.РФ это одно из приоритетных системно значимых технологических направлений, которое мы поддерживаем.

Николай Цехомский,
первый заместитель
председателя ВЭБ.РФ

Этапы трансформации российской индустрии, 2010–2025 гг.

Российская ИБ-отрасль — один из первых игроков мировой индустрии с уникальным сочетанием новаторства и адаптивности. За последние 15 лет рынок прошел две трансформации: от гибридной модели к концепции киберсуверенитета.

	2010–2016 УЯЗВИМЫЙ ПАРИТЕТ	2017–2021 ФОКУС НА ОТЕЧЕСТВЕННЫЕ РЕШЕНИЯ	2022–2025 КИБЕРСУВЕРЕНИТЕТ
Рынок и технологии			
Объем рынка, млрд руб.	16,5 → 66,3	72,3 → 185,9	193 → 374
Доля российских вендоров в продажах на конец периода	~50%	61%	>90%
Количество новых ИБ-продуктов в Реестре российского ПО	>150 (2016)	+112 в среднем ежегодно	+138 в среднем ежегодно
Количество компаний, предоставляющих ИБ-решения	—	8,4 тыс. (2020)	11,5 тыс. (2025)
Сообщество			
Количество ИБ-специалистов, чел.	55 тыс. (2016)	91 тыс. (2021)	~135 тыс. (2025)
Аудитория ключевых ИБ-конференций за период, офлайн-участники	>34 тыс.	>69 тыс.	~200 тыс.
Ср. время обнаружения злоумышленника ИБ-специалистами*	—	37 дней	9 дней
Системные подходы			
Новые отечественные концепции, модели и методологии	[1] Кибериммунитет	[1] Кибериммунитет + [2] Результативная кибербезопасность и недопустимые события	[1] [2] + [3] Кибериспытания + [4] Архитектор комплексной кибербезопасности

*MTTD, mean-time-to-detect, по данным Positive Technologies

Источники: ЦСР, ЦСР «Северо-Запад», TAdviser, Лаборатория Касперского, Positive Technologies, ГК «Солар», НИУ ВШЭ, СКБ Контур, экспертная оценка.

Предыстория

Россия — пионер мировой индустрии информационной безопасности

1988

Первая советская программа-антивирус Aidstest (Virus Hunter)

1990

Сообществом специалистов (включая советских) основана Computer Antivirus Research Organization (CARO)

1992

первая версия российского антивируса SpiderWeb (позднее Dr.Web)

1997

основана Лаборатория Касперского

С момента создания первых антивирусных программ в конце 1980-х гг. отечественные разработчики — команды, возглавляемые Дмитрием Лозинским, Игорем Даниловым, Евгением Касперским и др. — были пионерами индустрии программного обеспечения (ПО) для информационной безопасности. Уже в начале 1990-х гг. в России создаются компании-производители антивирусного ПО, специализированные ИБ-интеграторы, центры обучения и др.

В период 2000–2010 гг. рыночный сектор ИБ в России обретает форму. Согласно первым крупным исследованиям в 2010 году объем рынка составил 16,7 млрд руб. Наиболее активными заказчиками услуг выступили крупные компании финсектора, телеком и государственные структуры[14].

На протяжении 2006–2010 гг. — наравне с растущим уровнем киберугроз — одним из самых важных драйверов роста рынка ИБ в России стало государственное регулирование, в частности Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ и Федеральный закон «О персональных данных» от 27 июля 2006 г. №152-ФЗ, который ввел ответственность организаций за несоблюдение нужного уровня информационной безопасности[10]. Это позволило привлечь внимание бизнеса к индустрии кибербезопасности и сделать информационную безопасность одним из пунктов повестки компаний всех секторов экономики. По некоторым исследованиям за 2009 г. в 80% компаний среднего и крупного бизнеса появились менеджеры, ответственные за информационную безопасность[15].

Предлагая новые и эффективные технологии для борьбы с актуальными угрозами, российские ИБ-разработчики и исследователи к 2000 г. не только хорошо себя зарекомендовали внутри страны, но и начинали активно заявлять о себе на международном уровне. Так, в июне 1999 г. открылось первое зарубежное представительство компании «Лаборатория Касперского» в Великобритании[16].

2010

1. Уязвимый паритет

Распространение зарубежных решений
и риски внешней зависимости

2016

2017

Фокус на отечественные решения

2021

2022

Построение киберсуверенитета

2025

1.1 Рынок и технологии

Этап адаптации зарубежных продуктов и услуг наряду с разработкой собственных решений. Основные драйверы роста — сбалансированная госполитика и начавшаяся цифровизация бизнеса и госсектора.

в 4 раза

вырос объем российского ИБ-рынка с 2010 г. по 2016 г.

55%

доля российских компаний в продажах

59%

российские игроки в сегменте EPP, наиболее крупном сегменте рынка ПО для корпоративного ИБ

>30%

доля российских компаний в сегменте услуг

18

Упоминаний в Gartner Magic Quadrants. Успешный выход российских продуктов на мировые рынки

Источники: TAdviser, IDC, Gartner, ComNews, Anti-Malware.ru

Период 2010–2016 гг. характеризуется лидерством отечественных компаний в сегментах ПО и услуг, но отставанием от зарубежных вендоров в быстрорастущих направлениях, прежде всего в аппаратных средствах защиты информации. Так, в 2012 г. на трех иностранных лидеров в сегменте аппаратных решений приходилось 46,5% продаж[17]. И в дальнейшем их позиции усиливались, в том числе за счет локализации производства в России[18]. В то же время в сегменте EPP — крупнейшем сегменте корпоративного ИБ-ПО — российские игроки занимали 59%[19] рынка. Также отечественные компании-интеграторы выступали ведущими поставщиками услуг ИБ, их доля в сегменте составляла более 30%[20].

Таким образом, с точки зрения структуры рынка, можно говорить о наличии на рынке «уязвимого паритета»: развитие собственных технологий наравне с адаптацией зарубежных решений. В среднем 55% ежегодных продаж СЗИ приходилось на российские компании, 45% — на зарубежные*. При этом российские производители достаточно оперативно реагировали на современные тенденции и запросы рынка.

*Экспертная оценка

Важнейшим драйвером, обеспечившим рост отрасли, развитие и внедрение решений ИБ в России была начавшаяся активная цифровизация бизнеса и госсектора. Цифровая экономика страны аккумулировала 2,8% ВВП, а на все ИКТ-зависимые сегменты экономики приходилось уже 19% ВВП[20]. Все это требовало постоянного укрепления защиты растущей цифровой инфраструктуры от активно эволюционирующих киберугроз.

Другим ключевым фактором стала госполитика, одновременно обеспечившая своевременный доступ российских заказчиков к передовым зарубежным технологиям и стимулирующая непрерывную разработку российских решений мирового уровня. Существенная доля рынка приходилась на закупки предприятий с госучастием, естественных монополий и госучреждений — общий объем заключенных ИБ-контрактов в рамках 44-ФЗ и 223-ФЗ достиг 41,5 млрд руб. при общем объеме рынка в 66,3 млрд руб. в 2016 г.[21]

При этом:

— в 1,43 раза выросло число новых патентов, связанных с информационной безопасностью, в 2016 г. по сравнению с 2010 г.[22]

— в 2016 г. Роспатент и Федеральный институт промышленной собственности включили 21 ИБ-решение в список 100 лучших изобретений года[23].

Кроме того, продолжился активный выход российских компаний на зарубежные рынки. Отечественные решения получили признание на мировом уровне и регулярно включались в рейтинги глобальных аналитических компаний, например отчеты Gartner Magic Quadrant, связанные с информационной безопасностью[24]. С 2010 по 2016 гг. четыре российские компании были упомянуты в пяти различных категориях данных исследований в качестве визионеров, нишевых игроков и лидеров рынка. Это указывает как на зрелость технологий, так и на высокий экспортный потенциал российский ИБ-решений уже на этом этапе.

1.2 Люди

Активный рост сообщества и развитие профессиональных навыков в соответствии с общемировыми тенденциями, формирование календаря регулярных отраслевых конференций

55 тыс.
специалистов в сфере ИБ

>9 тыс.
участников профильных конференций к 2016 г.

66
российских CTF-команд на ctftime.org

Источники: «ЦСР «Северо-Запад» и Positive Technologies, ctftime.org, экспертная оценка

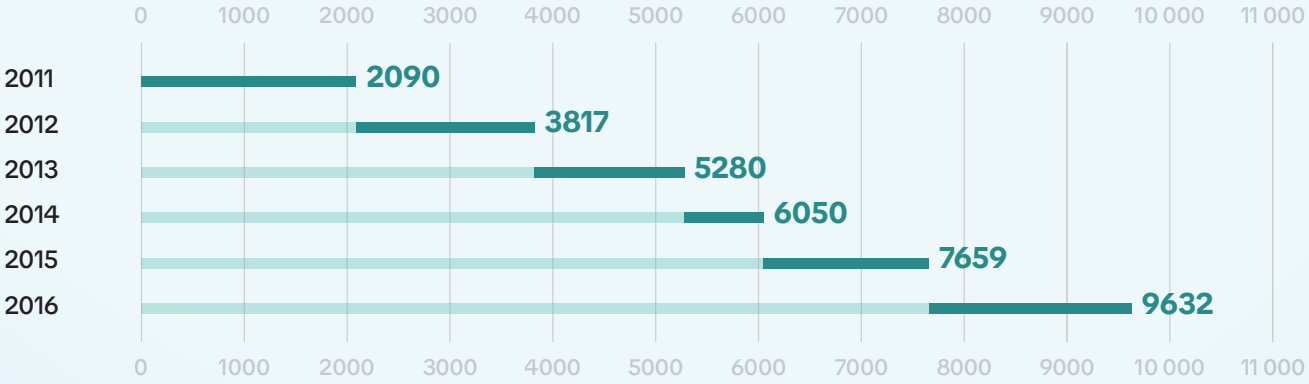
К 2016 г. численность ИБ-специалистов в индустрии превысила 50 тыс. человек[25]. Уже в этот период в мире отмечается ключевая роль сообщества и специализированных соревнований (hacking competitions, CTF) в развитии профессиональных навыков. Эта тенденция была заметна и в России. К 2016 г. усилиями энтузиастов и производителей ИБ-решений в России сформировалось устойчивое кибербезсообщество и стала активно развиваться культура CTF-соревнований (capture the flag exercises).

Количество российских CTF-команд

Источник: по данным ctftime.org

Также с начала 2010-х гг. в России сложился календарь регулярных отраслевых конференций. Среди самых известных: Positive Hack Days, Инфофорум, Уральский форум (Магнитка), OffZone и др. ИБ-мероприятия начинают ежегодно привлекать тысячи человек, создавая условия для укрепления ИБ-сообщества и обмена опытом в индустрии.

Количество офлайн-участников регулярных ИБ-конференций



В оценку включены ежегодные ИБ-конференции с аудиторией не менее 500 человек к 2025 г.

Источник: на основе публичных данных

На государственном уровне были разработаны и приняты шесть открытых профессиональных стандартов в сфере ИБ (обновлены в 2022 г.), а на их основе — федеральные государственные образовательные стандарты.

1.3 Оценка эффективности

Разработка ИБ-стандартов, появление первых отечественных комплексных подходов к построению кибербезопасности

На этапе становления российской индустрии кибербезопасности первым шагом в направлении оценки эффективности защиты от киберугроз стало внедрение различных стандартов и сертификации.

В 2010–2016 гг. на рынке активно адаптировались передовые западные стандарты, фреймворки, подходы к обеспечению информационной безопасности: ISO/IEC 27001, BS 7799, BS 31100, международный стандарт безопасности данных платежных карт PCI DSS и др. Эти подходы нашли отражение и в отечественных отраслевых стандартах, таких как СТО БР ИББС. Для обеспечения защищенности продолжает проводиться аттестация объектов информатизации.

В этот период деятельность по информационной безопасности во многом ориентирована на выполнение установленных требований и соответствие стандартам без дополнительной оценки уровня реальной защищенности. В условиях непрерывно растущего количества киберугроз становилось ясно, что необходимо развитие существующих подходов и разработка инновационных концепций построения ИБ.

В ответ на это в начале 2010-х гг. «Лаборатория Касперского» предложила новую концепцию — Кибериммунитет. Она зародилась еще в 2002 г. В отличие от традиционных моделей с защитой поверх готовой инфраструктуры этот подход предполагает выстраивание защиты сразу на уровне архитектуры, т. е. создание цифровых систем — приложений, устройств и сервисов — изначально более устойчивых к кибератакам. Это позволяет минимизировать уязвимости и снизить ущерб даже в случае ошибок в коде[27].

2010

Уязвимый паритет

2016

2017

2. Фокус на отечественные решения

Поддержка отечественной индустрии как необходимый фактор устойчивой цифровизации

2021

2022

Построение киберсуверенитета

2025

2.1 Рынок и технологии

Поддержка отечественных технологий и переход информационной безопасности на стратегический уровень. Основные драйверы роста — системное развитие цифровой экономики и включение ИБ в приоритеты цифровой трансформации России.

185 млрд руб.
размер рынка в 2021 г.

>60%
продаж приходится на российские компании

в 3 раза
выросло количество отечественных ИБ-решений

Источники: Минцифры России, ЦСР

В декабре 2016 г. в послании к Федеральному Собранию[28] Президент РФ Владимир Путин предложил запустить масштабную системную программу развития цифровой экономики с опорой на российские компании, научные, исследовательские и инжиниринговые центры страны, подчеркнув, что это является вопросом национальной безопасности и технологической независимости России.

В июле 2017 г. Правительство РФ разработало и утвердило программу развития цифровой экономики до 2024 г. А уже в мае 2018 г. был запущен национальный проект «Цифровая экономика», включающий в себя федеральный проект «Информационная безопасность»[29].

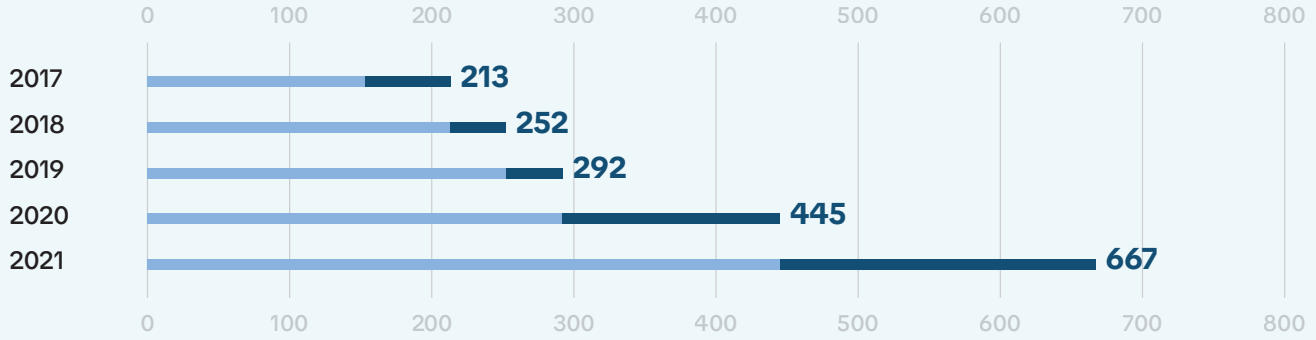
Таким образом начался переходный период, в котором фокус — в том числе на российском ИБ-рынке — сместился в сторону отечественных решений. На этом этапе происходит бурный рост отечественных решений в таких новых сегментах, как:

Сегмент	Примеры российских решений
Управление внешними поверхностями атак (External Attack Surface Management)	ScanFactory, Метаскан
Инфраструктура ложных целей (Distributed Deception Platform)	Xello
Защита компонентов контейнерной инфраструктуры (Container Security)	Luntry
Отслеживание угроз (Threat Intelligence)	RST Cloud
Повышение осведомленности сотрудников по вопросам информационной безопасности (Security Awareness)	Start-X, Phishman и др.

Были запущены и совершенно новые продукты. Например, в 2017 году состоялся первый релиз кибериммунной операционной системы KasperskyOS от Лаборатории Касперского[30].

К моменту старта программы «Цифровая экономика» в Едином реестре российских программ для электронных вычислительных машин и баз данных[31] было более 200 отечественных решений для обеспечения информационной безопасности. С 2017 по 2021 гг. количество продуктов в реестре выросло более чем в три раза.

Решения по информационной безопасности в Едином реестре российского ПО



Источник: на основе данных из реестра

Во многом этому способствовала активная политика импортозамещения. В 2017 г. был принят ФЗ №187, предписывающий использование российских решений на объектах критической инфраструктуры. В 2019 г. появилась возможность получения субсидий для льготного кредитования проектов по цифровой трансформации на основе отечественного ПО.

Кроме того, в 2020 г. была запущена федеральная программа мер поддержки ИТ, которая в дальнейшем оказала существенное влияние на рынок ИТ в целом и на ИБ-производителей в частности[32]. Если в 2017 г. объем рынка составлял 72,3 млрд руб.[33], то к завершению переходного этапа развития отрасли объем российского рынка ИБ достиг 185 млрд руб. (рост в 2,5 раза). При этом более 60% рынка приходилось на долю российских компаний[34].

Важно отметить, что уже к 2022 г., в том числе благодаря последовательной госполитике, страна подошла с практически полным стеком отечественных ИБ-решений. Единственным пробелом оставались отдельные продукты, такие как NGFW.

2.2 Люди

Повышение роли дополнительного образования для закрытия потребности в кибербез-специалистах по мере цифровизации экономики. Разработка новых форматов обучения с фокусом на практическую отработку навыков, начало развития культуры багбаунти.

>90 тыс.
количество ИБ-специалистов в России к концу 2021 г.

в 1,5 раза
вырос объем подготовки специалистов

до 18%
снижена нехватка кадров

Источники: ЦСР «Северо-Запад» и Positive Technologies

Активное развитие и усложнение ИТ-инфраструктуры и необходимых для ее защиты ИБ-решений требовало роста количества и качества профессиональных кадров. Несмотря на объективную важность фундаментального образования для разработки и развития передовых ИБ-технологий, скорость выпуска специалистов высшими учебными заведениями не соответствовала запросам быстро развивающегося рынка. В 2016 г. нехватка специалистов по информационной безопасности в России достигла 25%[35].

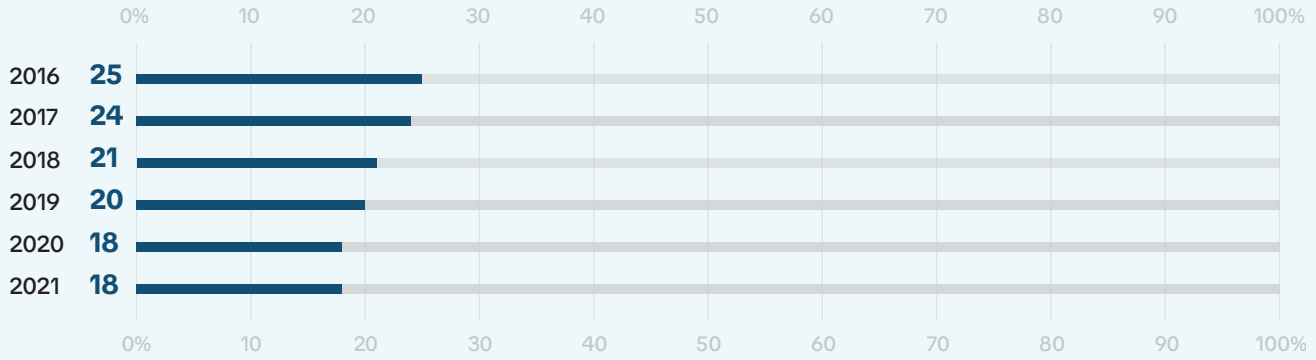
Для устранения дефицита кадров были приняты меры на государственном уровне. В частности, в федеральном проекте «Информационная безопасность» были предусмотрены практико-ориентированные образовательные мероприятия.

Темпы выпуска новых ИБ-специалистов государственными и коммерческими образовательными учреждениями выросли с 2017 по 2021 гг. на 55,6%. К концу переходного периода специалистов в области ИБ готовили более сотни высших учебных заведений. Две ИБ специальности вошли в топ-10 самых популярных ИТ-программ высшего образования — «Информационная безопасность» (6,6% выпускников) и «Информационная безопасность автоматизированных систем» (1,7%)[36].

В итоге в 2021 г. общее количество ИБ-специалистов в России превысило 90 тыс. человек. Нехватка кадров была уменьшена до 18%[35], оказавшись ниже, чем, например, в США, Бразилии и Нидерландах.

*Нехватка ИБ-специалистов характерна для всего мира: в 2015 дефицит кадров в мире оценивался в 1,5 млн человек, а в 2018 году составлял уже примерно 2,93 млн по данным GISWS и ISC2.

Нехватка ИБ-специалистов в России



Источник: ЦСР «Северо-Запад» и Positive Technologies

Параллельно с образовательными программами большой вклад в этот период начинают вносить соревновательные инициативы самого сообщества. Примерно в этот же период начинает активно трансформироваться подход к CTF-соревнованиям. Если раньше они были ориентированы преимущественно на специалистов по наступательной кибербезопасности, то, например, с 2016 г. соревнования в рамках фестиваля Positive Hack Days начинают проводиться в формате Standoff — противостояния атакующих (red team) и защищающихся (blue team) команд[37]. Таким образом, формат соревнований адаптировался к запросам отрасли, предоставив специалистам по мониторингу и противодействию атакам возможность отрабатывать практические навыки наравне с атакующими.

В 2021 г. российские CTF-команды уверенно входят в рейтинг лучших команд мира: две команды — в топ-10 рейтинга. Помимо этого, в начале 2020-х гг. появляются и первые отечественные программы и платформы багбаунти — компании начинают приглашать независимых исследователей в области безопасности (багхантеров/белых хакеров) для поиска уязвимостей в своих продуктах за вознаграждение. Багбаунти-площадки становятся важным инструментом консолидации сообщества практической кибербезопасности.

2.3 Оценка эффективности

Переход к новым принципам построения кибербезопасности, развитие концепции «недопустимых для бизнеса событий»

В период 2016–2021 гг. в России эффективность киберзащиты по прежнему преимущественно рассматривалась через призму классического подхода — создание модели угроз и нарушителя, проведение оценок соответствия/защищенности, внедрение компенсирующих мер. Это не позволяло оценивать эффективность ИБ в произвольный момент времени и более комплексно в условиях быстро меняющихся ИТ-инфраструктур.

Как было отмечено выше, поиск новаторских подходов активизировался еще в конце 2010-х годов. Именно в это время со стороны заказчиков возник запрос на новые системы измерения эффективности кибербеза. В переходный период ответом на недостатки традиционных подходов к ИБ и усиливающиеся риски реализации киберугроз стала концепция результативной кибербезопасности. В основе подхода лежит понятие «недопустимых для бизнеса событий»[38] (т. е. событий, которые могут привести к критическому ущербу), а критерием эффективности киберзащиты считается невозможность реализации этих событий в случае кибератаки.

Важными элементами результативной кибербезопасности являются:

1. Фокус на практический, ощутимый результат для бизнеса вместо формального соблюдения процессов и требований;

2. Измеримость и проверяемость безопасности;

3. Непосредственное вовлечение высшего руководства компании-заказчика. Так, кибербезопасность стала интегрироваться в стратегические цели бизнеса.

Примерно с 2021 г. наметился сдвиг в мышлении специалистов. По данным Positive Technologies, в это время уже в каждом третьем проекте клиенты указывали целевые системы, для которых необходимо было проверить возможности атакующих[39].

2010

Уязвимый паритет

2016

2017

Фокус на отечественные решения

2021

2022

3. Построение киберсуверенитета

проверка на прочность и новая модель защиты

2025

События начала 2022 г. — санкционное давление, последовательный и одномоментный уход крупнейших западных поставщиков, занимавших 39% рынка кибербезопасности страны в 2021 г., — стали уникальным опытом не только для российской, но и для мировой ИБ-отрасли.

К этому моменту Россия уже обладала высоким уровнем цифровизации, но рекордный рост кибератак (от 80 до 200% по разным оценкам) не привел к критическим сбоям. Россия стала первой цифровой державой, одновременно подвергшейся такому давлению и технологической изоляции, которой удалось успешно защитить свою инфраструктуру. Сегодня страна входит в десятку стран по абсолютным расходам на кибербезопасность и предлагает новый подход к построению кибербезопасности на мировом уровне.

3.1 Рынок и технологии

Новый виток развития отечественной индустрии кибербезопасности на фоне ухода иностранных поставщиков ИБ-решений: сохранение конкурентной среды, полный стек собственных технологий во всех ключевых сегментах, выход бизнеса на багбаунти

20–25%
среднегодовой рост рынка с 2022 по 2025 гг.

374 млрд руб.
объем рынка по итогам 2025 г.

200+
ведущих российских ИБ-решений в ключевых сегментах рынка

Источники: ЦСР, экспертная оценка

Российский рынок ИБ с 2022 по 2025 гг. вырос на 94% — со 193 млрд до 374 млрд руб. Среднегодовой темп роста составил 20–25%, что делает рынок одним из наиболее динамичных ИТ-сегментов[40].

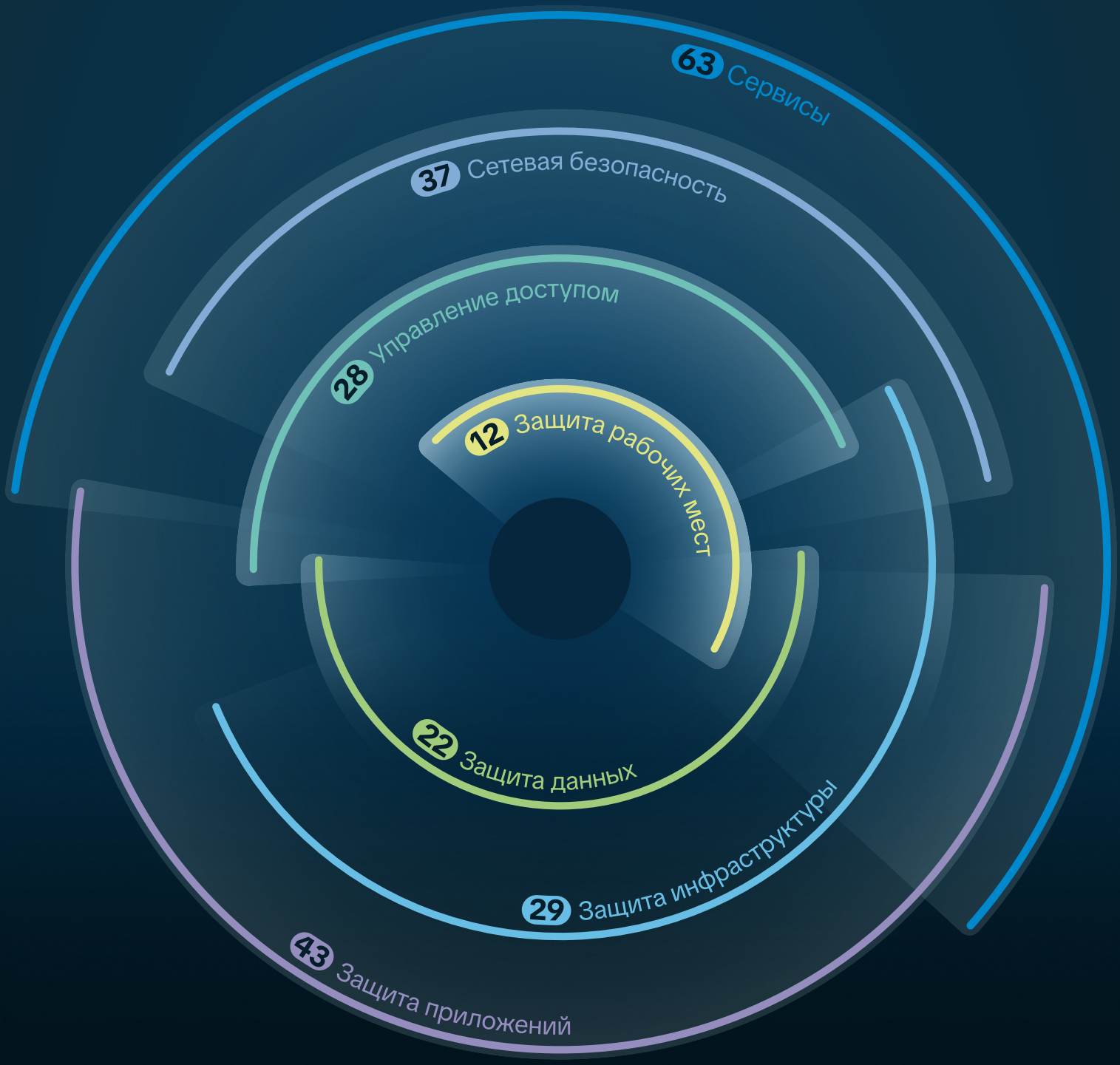
Несмотря на то, что доля зарубежных вендоров на внутреннем российском рынке в 2023 г. сократилась до 7%, уровень конкуренции остался сопоставим с общемировыми показателями. На 10 крупнейших поставщиков в России и в мире приходится 55% и 40% соответственно. И новые игроки продолжают выходить на рынок[41].

С 2020 по 2025 гг. количество компаний в сфере ИБ увеличилось на 38%. Если в 2020 г. их насчитывалось 8,4 тыс., то уже к середине 2025 г. стало 11,5 тыс. Прирост количества организаций, занимающихся разработкой СЗИ и ИТ-систем, защищенных с использованием СЗИ, составил 91,4%, компаний, специализирующихся на защите от утечек данных, а также на научных исследованиях в области ИБ — 40%[42]. Кибербезопасность вошла в топ-3 отраслей по показателю рентабельности продаж[43].

Полный стек российских решений

Российский ИБ-рынок сегодня обеспечивает страну решениями во всех ключевых сегментах защиты информации, покрывая текущие потребности экономики. На рынке представлено более 800 решений, из них 200+ продуктов и сервисов приносят 100+ ведущим российским компаниям годовую выручку от 100 млн руб. в каждой категории.

Конкурентный рынок позволяет постоянно совершенствовать технологии и сервисы и обеспечивать страну ключевыми компонентами киберсуверенитета.



Сегменты рынка и количество ведущих вендоров по категориям

Сервисы — 63

26 Управляемые сервисы безопасности (MDR/SOC/MSS)

3 Непрерывное измерение защищенности (кибериспытание, багбаунти)

22 Классическая оценка защищенности (пентесты, редтим)

3 Расследование инцидентов

9 Сервисы обучения и повышения осведомленности

Защита приложений — 43

15 Управление уязвимостями (VM/EAP/CAASM/EASM/ ASCA, AEV/BAS)

6 Тестирование безопасности приложений (в т.ч. анализ кода, S/DAST)

11 Межсетевые экраны веб-приложений (WAF)

3 Защита контейнеров

8 Защита от распределенных атак (DDoS Protection)

Сетевая безопасность — 37

20 Управление сетевым трафиком (NGFW/UTM/IDPS/VPN)

6 Анализ сетевого трафика (NDR/NTA)

7 Пограничная фильтрация контента (SEG/SWG)

4 Централизованный анализ вредоносного ПО (Network Sandbox)

Защита инфраструктуры — 29

8 Управление событиями безопасности (SIEM)

4 Оркестрация и управление рисками (SOAR/IRP/GRC)

8 Платформы киберразведки (TI/TIP)

4 Промышленная безопасность

5 Платформы ложных целей (DP/DDP)

Управление доступом — 28

11 Управление учетными данными и доступом (IdM/IGA/SSO/MF)

9 Контроль привилегированных пользователей (PAM)

8 Системы управления открытыми ключами (PKI)

Защита данных — 28

9 Системы аудита и управления данными (DSP/DCAP/DAG)

8 Предотвращение утечек данных (DLP)

5 Шифрование данных на узлах (Encryption)

Защита рабочих мест — 12

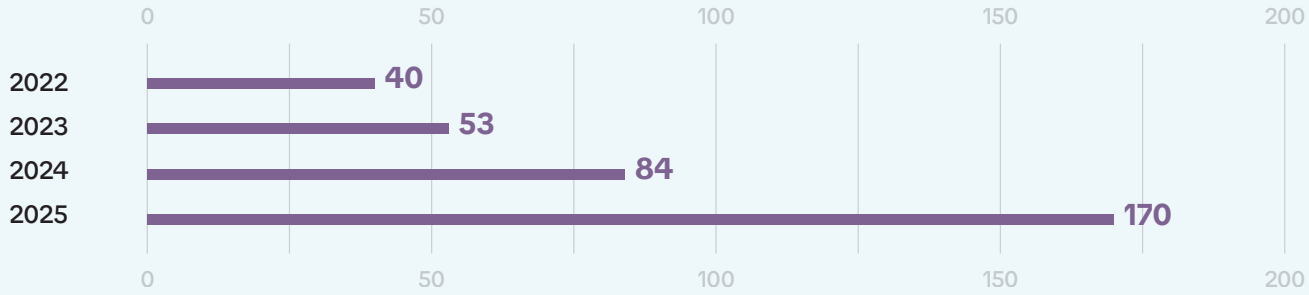
12 Платформы защиты рабочих мест (EPP/EDR)

Российские поставщики решений с выручкой более 100 млн руб. в год в категории по открытым данным

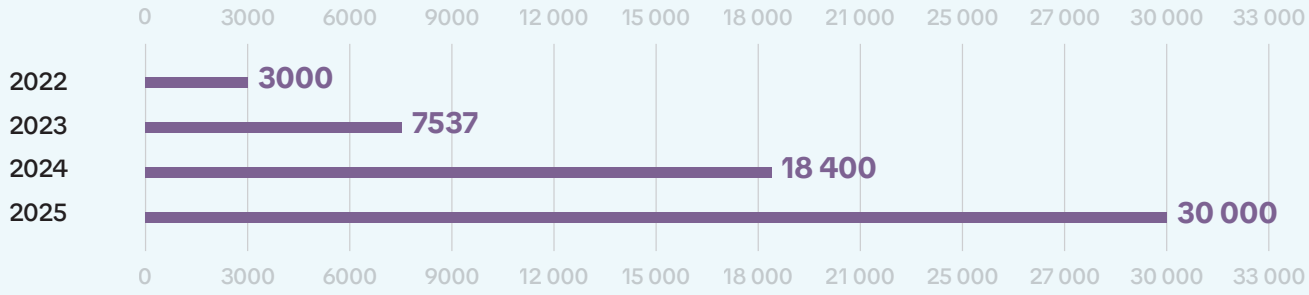
Еще одним направлением в повышении информационной безопасности как госорганов, так и бизнеса стало дальнейшее развитие программ багбаунти и киберполигонов для моделирования атак, особенно в страховом, финансовом и государственном секторах. Сегодня Россия входит в лидеры по количеству багбаунти-платформ в мире[44].

В стране работают три багбаунти-площадки, на которых размещено более 250 публичных и частных программ от организаций из разных секторов экономики: финансов, торговли, медиа, транспорта, государственных сервисов и др. При этом количество принятых отчетов, за которые были выплачены вознаграждения, выросло в 4,8 раза с 2022 по 2024 гг.[46]

Багбаунти программы



Исследователи на багбаунти-площадках



На основе данных о платформе Standoff Bug Bounty

Источник: Positive Technologies

Для субъектов РФ и госкомпаний катализатором выхода на багбаунти выступило Минцифры, когда ввело параметр «Информационная безопасность» в рейтинг цифровой трансформации госорганов как один из показателей цифровой зрелости[46]. Ведомство запустило собственную багбаунти-программу в 2023 г.[47] А в 2024 г. только на BI.ZONE Bug Bounty вышло в три раза больше организаций из госсектора[48].

Важную роль в создании благоприятной среды для роста индустрии сыграла последовательная госполитика*. В частности, на ИБ-отрасль распространяются преференции, направленные на поддержку и стимулирование развития ИТ-компаний. Более 1500 отечественных компаний в сфере ИТ получили поддержку от государства в течение пяти лет реализации национального проекта «Цифровая экономика»[49].

Основные направления поддержки аккредитованных ИТ-компаний и их сотрудников в России в 2025 г.

Направление	Мера поддержки
Фискальные послабления	Сниженный налог на прибыль: 5% для аккредитованных ИТ-компаний с 70% доходов от ИТ-деятельности с 2025 г. Освобождение от уплаты НДС при реализации ПО, включенного в единый реестр российского ПО Сниженная ставка по страховым взносам: 7,6% для аккредитованных ИТ-компаний с 70% доходов от ИТ-деятельности
Снижение административной нагрузки	Мораторий на плановые проверки до конца 2025 г. Упрощенный наем иностранных сотрудников
Финансовая поддержка	Гранты для финансирования ИТ-проектов
Льготы для сотрудников	Льготная ипотека для сотрудников ИТ-компаний на покупку жилья на первичном рынке по ставке до 6% годовых Отсрочка от призыва на военную службу для сотрудников, соответствующих установленным требованиям
Другое	Акселерация ИТ-проектов

Источник: Минцифры России

*В рамках исследования не рассматривались меры госполитики по борьбе с кибермошенничеством

Последовательная госполитика как фактор развития отрасли

Государственная политика во многом определила развитие российской ИБ-отрасли, последовательно повышая значимость информационной безопасности.

Фундамент госполитики в области ИБ

2000

Доктрина информационной безопасности: отмечена возрастающая роль информационной сферы

2004

Образование ФСТЭК России — одного из ключевых регуляторов отрасли.

Первый отраслевой стандарт по обеспечению информационной безопасности (Банк России)

2006

149-ФЗ «Об информации, информационных технологиях и о защите информации»

152-ФЗ «О персональных данных»

2011

99-ФЗ: лицензирование деятельности в области ИБ

2013

Гос. система обнаружения, предупреждения и ликвидации последствий комп.атак на информационные ресурсы (ГосСОПКА)

Приказы ФСТЭК России №17 и №21: меры и требования по защите информации в Государственных информационных системах (ГИС) и Информационных системах персональных данных (ИСПДн)

2015

Создание базы данных уязвимостей ФСТЭК России

2016

Создание единого реестра отечественного ПО

Повышение роли ИБ в рамках цифровизации, фокус на критическую информационную инфраструктуру (КИИ)

2016

Обновленная Доктрина информационной безопасности: отмечен трансграничный характер информационных технологий и их роль в ускорении экономического развития

2017

Стратегии развития информационного общества в на 2017–2030 годы

Программа «Цифровая экономика Российской Федерации»

187-ФЗ о безопасности критической информационной инфраструктуры (КИИ)

2018

Федеральный проект «Информационная безопасность» (основные участники: Минцифры, ФСБ, ФСТЭК, ФСО, РКН)

Национальный координационный центр по компьютерным инцидентам (НКЦКИ)

2020

Первый пакет мер поддержки ИТ-отрасли, в том числе снижение налога на прибыль и тарифов страховых взносов, освобождение отечественного ПО от НДС и др.

2021

Второй пакет из 60+ мер поддержки ИТ-компаний

Развитие новых подходов и киберсуверенность

2022

Расширение льгот для ИТ-компаний, в т. ч. обнуление налога на прибыль, кредиты по льготной ставке и гранты; для сотрудников — льготная ипотека и др.

Увеличена квота на целевое обучение в ВУЗах по специальности ИБ до 30% на 2023 г.

Указ Президента России №166 об ограничении на использование импортных СЗИ на объектах КИИ

Указ Президента России №250 об организации структур информационной безопасности на объектах КИИ и ответственности руководителей

2023

Публичная программа поиска уязвимостей Госуслуг от Минцифры России

Минцифры России ввело параметр «Информационная безопасность» в рейтинг цифровой трансформации госорганов как один из показателей цифровой зрелости.

Приказ ФСБ России №213 о мониторинге защищенности информ. ресурсов

2024

Нац. проект «Экономика данных и цифровая трансформация государства», в том числе фед. проект «Инфраструктура кибербезопасности» (отв. — Минцифры России)

2025

Конвенция ООН против киберпреступности, разработанная по инициативе России

Введение требований к доверенному ПО

Методика определения недопустимых событий от Минцифры России

Приказ ФСТЭК России №117 (взамен приказа ФСТЭК №17)

3.2 Люди

Формирование одного из самых мощных ИБ-сообществ в мире, объединяющего рынок, государство и другие отрасли для борьбы с киберугрозами. Рост аудитории отраслевых мероприятий и развитие кибербезопасности как перспективного карьерного направления.

~135 000
человек — оценка численности ИБ-специалистов в 2025 г.

>47 000 человек
количество выпускников по направлению ИБ за период с 2022 по 2025 гг.

в 5 раз
увеличилась аудитория отраслевых конференций с 2021 г.

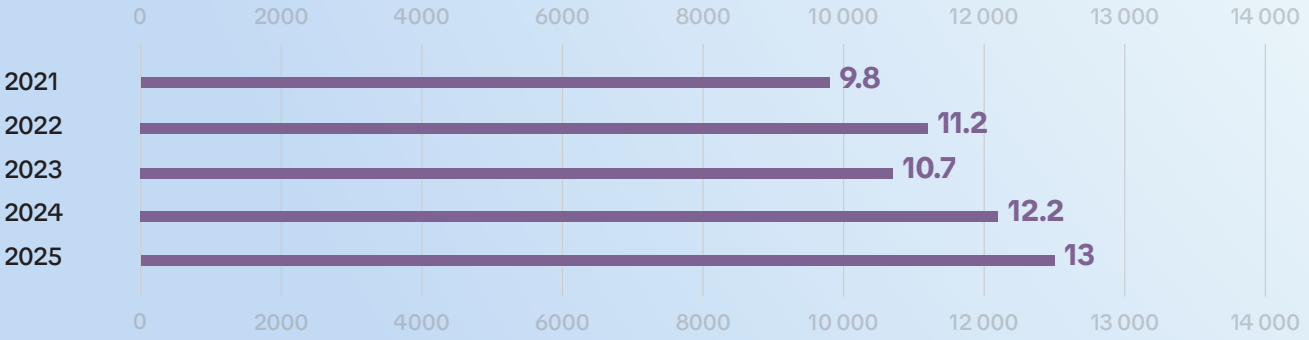
на 33%
увеличился ежегодный выпуск ИБ-специалистов с 2021 г.

Источники: ЦСР, экспертная оценка

В 2022 г. были предприняты дополнительные меры по повышению выпуска новых кадров: квота приема на целевое обучение по ИБ-специальностям была установлена на уровне 30%[50] (по сравнению с 20% в предыдущем году)[51].

Общее число выпускников по специальности «Информационная безопасность» в 2026 г. должно составить 13,9 тыс. человек. За период с 2021 по 2025 гг. этот показатель вырос на 33%. Количество занятых в ИБ-отрасли превысило 110 тыс. человек еще в 2023 г.[35] Сегодня информационная безопасность входит в тройку наиболее востребованных специальностей[52].

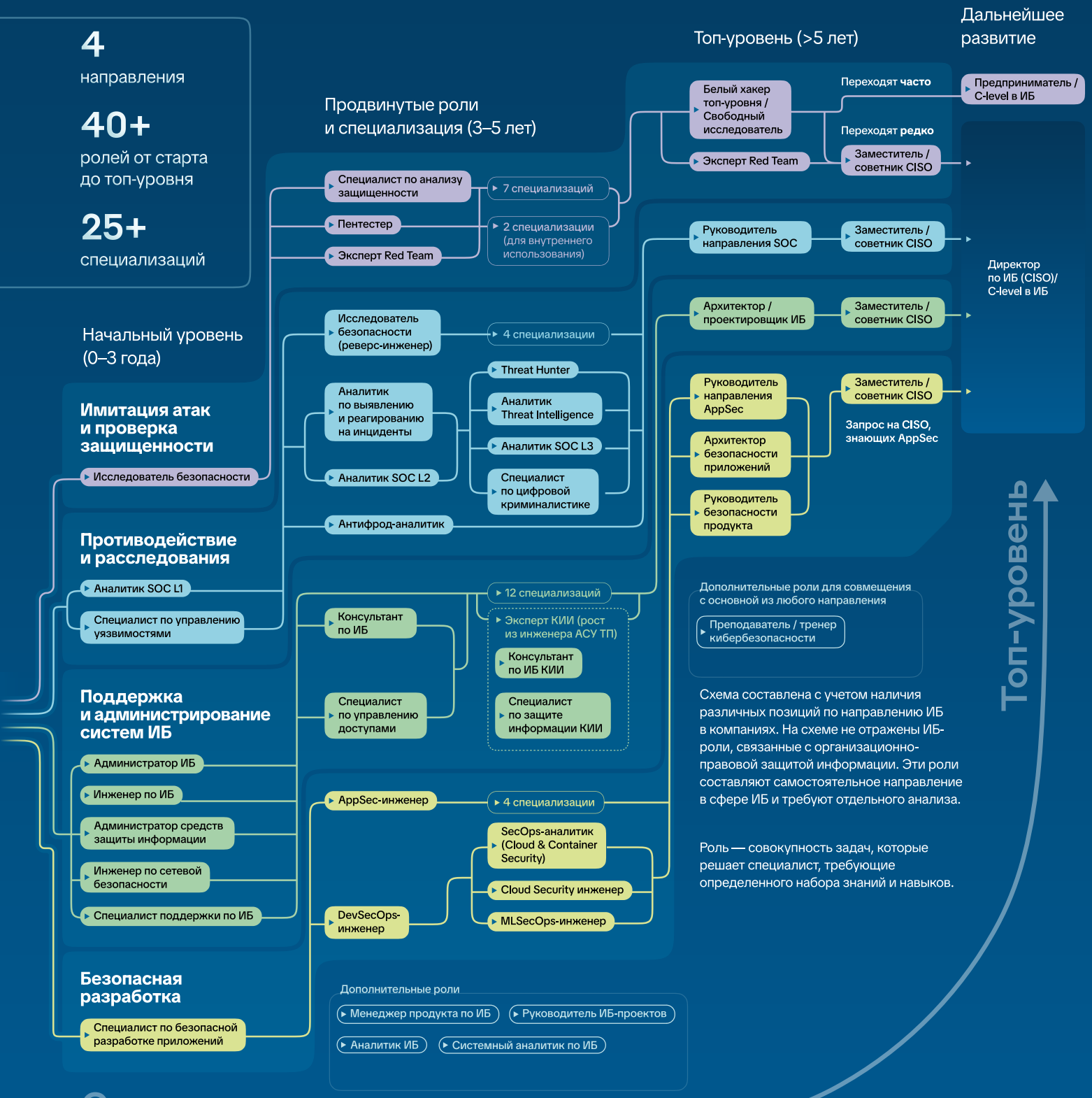
Выпуск кадров в сфере информационной безопасности



Источник: на основе данных ЦСР «Северо-Запад» и Positive Technologies

Сообщество развивает роли и специальности внутри индустрии. Зрелость отрасли отражается в разветвленной структуре ролей в кибербезопасности. Топовые специалисты запускают новый виток развития индустрии.

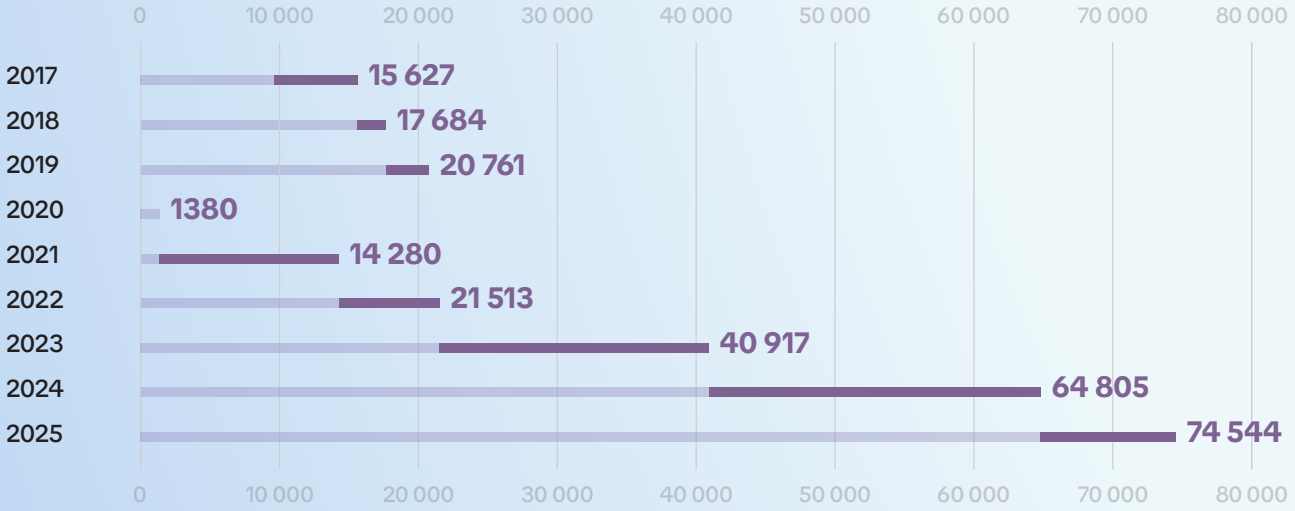
Схема ключевых ролей в результативной кибербезопасности



Еще одним источником заработка и профессионального развития для многих исследователей кибербезопасности стал поиск уязвимостей за вознаграждение (багхантинг) на фоне роста популярности багбаунти среди госорганов и бизнеса. По отдельным оценкам для 73% исследователей багхантинг является дополнительным видом деятельности[45]. При этом уровень выплат на отечественных платформах оценивается как сопоставимый с выплатами на зарубежных площадках[53].

Важной частью индустрии являются регулярные ИБ-конференции и популяризация отрасли со стороны самого кибербез-сообщества. Так, к 2025 г. только профильная офлайн аудитория конференций достигла 75 тыс. человек в год. Это в 5 раз больше показателей за 2021 г.

Количество офлайн-участников регулярных ИБ-конференций



В оценку включены ежегодные ИБ-конференции с аудиторией не менее 500 человек к 2025 г.

В 2023 г. крупнейшее отраслевое ежегодное мероприятие — фестиваль Positive Hack Days — стало привлекать не только профильных специалистов, но и широкую публику, способствуя повышению осведомленности граждан в сфере ИБ. Сегодня по охвату аудитории Positive Hack Days является одной из самых крупных конференций в мире, посвященной тематике информационной безопасности, наравне с DEFCON (США, ~30 тыс. участников офлайн), RSA (США, 40+ тыс. участников офлайн[54]) и BlackHat (США, >20 тыс. участников офлайн).

3.3 Оценка эффективности

С 2022 г. крупный российский бизнес и государственные структуры активно встраивают информационную безопасность в свои стратегии управления рисками и бизнес-модели. Масштабируется использование результативного подхода к кибербезу, продвигается ответственный подход к построению комплексной ИБ, проводятся кибериспытания для измерения уровня киберзащиты в деньгах.

в 2022 г.

приняты указы №166 и 250, Минцифры России запустил подготовку реестра и методики определения недопустимых событий

в 2023 г.

более 60% опрошенных специалистов и руководителей уже определили недопустимые для своих организаций события

20%

организаций прошли киберучения или запустили программы багбаунти

с 37 до 9 дней

сократилось среднее время обнаружения злоумышленника (MTTD) в период с 2021 по 2025 гг.

Источник: Минцифры России, Positive Technologies

Если в 2021 г. по данным опросов большинство компаний имели лишь базовые средства защиты и реагировали на инциденты постфактум , то уже через год ситуация заметно изменилась[55]. В условиях, когда количество и сложность кибератак неуклонно растет, попытки «защититься от всего сразу» теряют смысл и приводят к неэффективному распределению ресурсов. Принятые в начале 2022 года Указ Президента Российской Федерации от 30.03.2022 №166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» и Указ Президента РФ от 01.05.2022 г. №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» дали старт перестройке отношения бизнеса к ИБ и оценке ее эффективности.

Указ №250 потребовал прямого подчинения структуры информационной безопасности руководителю организации, определил его персональную ответственность и потребовал выделения отдельной должности или присвоения функции управления информационной безопасностью существующему заместителю — вице-президенту по ИТ или директору по безопасности.

Кроме того, произошло смещение фокуса внимания ИБ на «недопустимые события». Бизнесу становится необходимо понимать, как ИБ влияет на бизнес-процессы, ИТ и цифровую трансформацию. Отныне организация на уровне топ-менеджмента должна самостоятельно определить, какие события являются недопустимыми. Обычно это 3–7 событий, которые в случае их реализации имеют катастрофические последствия для бизнеса.

В 2022 г. Минцифры запустил подготовку реестра и методики определения недопустимых событий для облегчения этой работы на местах[56]. Концепция недопустимых событий призвана помочь организациям не «распыляться» на все задачи и системы, которые у них есть, а сфокусироваться именно на том, что может повлечь за собой критический ущерб. Тем самым, появляется возможность оптимально использовать существующие ресурсы и направить внимание ИБ на самое важное.

Уже в 2023 г. опросы показали, что 71% российских компаний знакомы с концепцией результативной кибербезопасности, более 60% — определили или планируют определить недопустимые для себя события. В 20% организаций проводились киберучения или работают программы багбаунти. В целом результаты отражали активный рост осведомленности и спроса на результативную кибербезопасность. Параллельно среднее время обнаружения злоумышленника (mean time-to-detect, MTTD) сократилось с 37 дней в 2021–2023 гг. до 17 дней в 2023–2024 гг. и уже до 9 дней в 2025 г.[57]

Как подтверждение зрелости отечественной отрасли ИБ на рынке появляются новые концепции киберзащиты, ориентированные на структурные изменения в подходах к измерению эффективности и качественному повышению безопасности.

Архитектор комплексной кибербезопасности[58]

Группа компаний «Солар» в 2025 г. предложила новый формат организации ИБ — услугу «Архитектор кибербезопасности». Она ориентирована на крупный бизнес и масштабные проекты по обеспечению киберустойчивости. Компания как архитектор комплексной кибербезопасности берет на себя ответственность за полный цикл формирования защищенной цифровой среды: аудит текущего ИБ-ландшафта, разработку архитектуры, выбор решений без привязки к конкретным вендорам, координацию подрядчиков и контроль конечного результата. Таким образом обеспечивается системный подход к построению единой киберустойчивой ИБ-инфраструктуры. Среди потенциальных заказчиков — организации из госсектора, машиностроения, металлургии и транспортной отрасли.

Кибериспытание[59]

Кибериспытание — уникальная российская методика непрерывной оценки защищённости, позволяющая определить уровень кибератаки, которую предприятие способно выдержать. Она меняет подход к кибербезопасности: вместо формального соответствия — проверка в реальных условиях. Само измерение становится фактором устойчивости, система усиливается под давлением.

Как это работает

Независимые исследователи строят полные цепочки атак, используя реальные инструменты и векторы: от внешнего периметра до социальной инженерии и подрядчиков.

1. **Фокус на недопустимых событиях.**
   Оценивается не наличие уязвимостей, а возможность довести атаку до критического результата: остановки операций, сбоев процессов, утраты или искажения данных. Единица результата — предотвращённое недопустимое событие.
2. **Непрерывность.**
   Атака развивается во времени без «конца проекта». Любые изменения в ИТ-ландшафте сразу учитываются. Устойчивость подтверждается только при длительном давлении.
3. **Реалистичность.**
   Проверяется вся компания, без ограничения периметром. Используются реальные векторы (сотрудники, подрядчики, инфраструктура, внешняя среда).
4. **Достоверность.**
   Атаки проводят независимые специалисты с разной экспертизой.
5. **Вендоронезависимость.**
   Оценка не привязана к конкретным решениям. Итоги валидируются независимым советом по единым критериям, что обеспечивает прозрачность и доверие.
6. **Измерение в деньгах.**
   Ключевая метрика — CQ (стоимость невзлома): максимальное вознаграждение за атаку, при котором недопустимое событие не достигнуто. Это позволяет напрямую сопоставлять безопасность с рисками и бюджетами.
7. **Оплата за результат.**
   Вознаграждение выплачивается за достигнутый результат, а не за активность. Это открывает новые модели ответственности, включая привязку оплаты подрядчиков к уровню защиты.

Как результат, кибериспытание переводит компанию в состояние, при котором каждая волна атак повышает её готовность. Защита отрабатывается на практике, а слабые места устраняются в цикле: испытание → корректировка → внедрение → повторная проверка.

Sk Capital рассматривает индустрию кибербезопасности как одно из целевых направлений для инвестиций. В последние годы здесь происходит настоящая трансформация, а значит возникает множество возможностей.

Рассчитываем, что при нашей поддержке будут сформированы новые технологические лидеры, способные обеспечить импульс опережающего развития не только внутреннему рынку, но и наращивать международное присутствие, став частью комплексного экспортного предложения.

Со своей стороны мы готовы предоставлять им не только капитал, но и необходимую экспертизу и другие доступные нам ресурсы.

Владимир Сакович,
Генеральный директор
Sk Capital

Кибербезопасность как драйвер роста экономики

Высокий уровень зрелости российской ИБ-отрасли — скрытый фактор общего экономического роста страны.

3,6–5,3
трлн руб.

оценка совокупного вклада отрасли кибербезопасности в российскую экономику на 2025 г.

~2% ВВП

Роль кибербезопасности часто недооценивается, а самая отрасль воспринимается как малая часть экономики, связанная с узкоспециализированными рисками. Однако повышение уровня кибербезопасности приводит не только к снижению потерь, но и к общему экономическому росту — во многом за счет повышения оптимизма бизнеса. На фоне растущего числа киберугроз киберустойчивость создает условия для поддержания цифрового доверия и ускоренного развития отраслей экономики, активно внедряющих новые технологии.

В рамках исследования было выделено четыре ключевых направления вклада отрасли в экономику:

1. прямой вклад — добавленная стоимость, которую создает сама отрасль ИБ, и ее вклад в общий экономический рост и занятость;
2. прямой предотвращенный ущерб от кибератак, то есть неслучившиеся потери выручки, компенсации контрагентам, расходы на восстановление операционной деятельности и др.;
3. косвенный предотвращенный ущерб, например, репутационный ущерб, ущерб от нарушения цепочек поставок, снижение оценки стоимости компаний и др.;
4. синергетические эффекты за счет создания условий для ускоренного развития других отраслей экономики.

Прямой вклад ИБ-отрасли оценивался на основе доли отрасли в общей выручке ИТ-индустрии и ее доли в ВВП страны. Позитивные синергетические эффекты были оценены двумя способами:

— по общей методологии Всемирного банка[10];

— а также с применением детализированных мультипликаторов на основе данных Росстата по динамике добавленной стоимости. По результатам расчетов можно отметить, что эффекты прежде всего сконцентрированы в промышленности (более 2,5 трлн руб).

Таким образом, суммарный вклад ИБ-отрасли в экономику России в 2025 г. даже без учета косвенного предотвращенного ущерба составил 3,6–5,3 трлн руб.

Вклад импортозамещения

100 млрд руб. принесла ИБ-отрасли активизация импортозамещения только в 2025 г.

Доля российских поставщиков на внутреннем ИБ-рынке за последние четыре года существенно выросла: с 61% в 2021 г. до более 90% в 2025 г. Такое перераспределение сил позволило отечественным вендорам заработать только в 2025 г. на 106 млрд руб. больше. А к 2030 г. объем продаж за счет импортозамещения может превысить 200 млрд руб.

Для крупных компаний расходы на ИБ-решения окупаются. По результатам исследования оценка прямого предотвращенного ущерба только для них составила 0,4–1 млрд руб. в 2024 г.

Это особенно важно с учетом того, что с 2022 г. активно перестраивается отношение бизнеса к кибербезопасности и измерению ее эффективности. Эксперты отмечают рост вовлеченности первых лиц компаний в вопросы киберустойчивости и того, как ИБ влияет на бизнес-процессы, ИТ и цифровую трансформацию.

1 рубль, вложенный в ИБ-решения, может сохранить до 3,5 рублей в виде предотвращенного ущерба

0,4–1,1
трлн. руб
Оценка прямого предотвращенного ущерба для крупных компаний

0,3
трлн. руб
Размер рынка ИБ

Методология

Источники данных и инструменты оценки

— анализ открытой статистики, публикаций государственных органов и исследований по рынку (российские и зарубежные источники). Мониторинг высказываний представителей органов власти и отраслевого сообщества;

— экспертные оценки;

— методология Всемирного банка и собственные расчеты.

Точные оценки ряда отраслевых параметров затруднены как в глобальном, так и в российском масштабе в связи с отсутствием или несопоставимостью статистических данных и разнообразием методологических подходов. В целом в рамках исследования использовался консервативной подход, в рамках которого не учитывались метрики, по которым не было достаточных данных.

Для оценки экономических эффектов использовались собственные расчеты. Также было применено аппроксимирование результатов исследований и оценок Всемирного банка, основанных на эконометрическом анализе упоминаний о киберинцидентах в глобальных СМИ.

Суммарный позитивный эффект, представленный в исследовании, включает прямой вклад ИБ-отрасли в экономику, а также оценку уровня позитивных синергетических эффектов по двум сценариям. Приведенная оценка предотвращенного ущерба не добавлялась для избежания двойного счета, так как предотвращенный ущерб учтен в методологии Всемирного банка при оценке синергетического эффекта[10]. Для его расчета проводилось моделирование объема потерь, которые могли бы случиться в отсутствии киберзащиты с двумя сценариями: минимальным и максимальным ущербом.

В расчете не учтены предполагаемые Всемирным банком негативные эффекты от высокого уровня развития кибербезопасности для отраслей сельского хозяйства и строительства в связи с отсутствием свидетельств существования таких эффектов в российской экономике. Они предположительно возникают в ряде стран из-за избыточных с точки зрения экономической эффективности расходов на кибербезопасность в этих отраслях в связи с требованиями регулирования, в том числе в других юрисдикциях, применяемого к транснациональным корпорациям, а также возможного эффекта «перетока» ресурсов в отрасли с большим выигрышем.

Перечень ключевых сегментов рынка СЗИ и услуг ИБ и количество ведущих отечественных вендоров составлен экспертно на основе рыночной сегментации Gartner и исследований ЦСР.

Команда проекта

Фонд развития результативной кибербезопасности Сайберус

Сергей Войнов	управляющий директор
Иван Скородумов	пресс-служба
Рубен Бунятян	пресс-служба
Елена Степанова	старший аналитик
Юлия Даргель	пресс-служба
Ноган Ушанова	бизнес-ассистент
Кирилл Блинов	креативный директор
Василий Дриго	арт-директор
Илья Ускоев	дизайнер

Институт экономики роста им. П.А. Столыпина

Антон Свириденко	исполнительный директор
Борис Копейкин	главный экономист

Эксперты

Роман Краснов	Фонд Цифровых Исследований «КиберПрогноз»
Сергей Балыбердин	АО «Кибериспытание»
Дмитрий Федоров	Positive Technologies
Егор Зайцев	АО «Кибериспытание»

Список источников

1. По данным РАЭК. Источник: Экономика рунета вновь выросла на 40%, как и годом ранее | ComNews
2. Белая книга цифровой экономики 2023: https://d-economy.ru/analitic/belaja-kniga-cifrovoj-jekonomiki-2023/
3. ИСИЭЗ ВШЭ: https://issek.hse.ru/news/1114086450.html
4. Минцифры России: https://digital.gov.ru/target/naczionalnyj-proekt-ekonomika-dannyh-i-czifrovaya-transformacziya-gosudarstva
5. Краткий статистический сборник «Цифровая экономика», 2025, ИСИЭЗ ВШЭ: https://www.hse.ru/primarydata/icekr
6. UN E-Government Survey 2024: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024
7. 2025 GovTech Maturity Index, Всемирный банк: https://www.worldbank.org/en/programs/govtech/gtmi-2025-update
8. Статистический сборник «Индикаторы цифровой экономики», ИСИЭЗ ВШЭ: https://issek.hse.ru/news/1026730357.html
9. ГК «Солар»
10. Всемирный банк: https://www.worldbank.org/en/topic/digital/publication/Cybersecurity-Economics-for-Emerging-Markets
11. F6: https://www.f6.ru/media-center/press-releases/cyberthreats-2025/
12. По данным Group-IB. Источник (Коммерсант): https://www.kommersant.ru/doc/5679329
13. ГК «Солар», Отчет об атаках на онлайн-ресурсы российских компаний за 2022 год: https://rt-solar.ru/analytics/reports/3289/
14. IDC, Russia IT Security Services 2011—2015 Forecast and 2010 Vendor Shares. Источник: https://www.itweek.ru/security/article/detail.php?ID=133162
15. Leta, Рынок информационной безопасности 2009: начало эпохи compliance, 2009
16. «Лаборатория Касперского»: https://esg.kaspersky.com/ru/about-company/brief-history
17. IDC, 2012. Источник («Код Безопасности»): https://www.securitycode.ru/company/news/kod_bezopasnosti_po_otsenke_idc_zanimaet_vtoroe_mesto_po_obemu_postavok_apparatnykh_ib_resheniy_na_r_/
18. ComNews: https://www.comnews.ru/content/110097/2017-10-19/check-point-ukorenyaetsya-v-rossii
19. Anti-Malware.ru: https://www.anti-malware.ru/russian_antivirus_market_2010_2012
20. По данным РАЭК. Источник (ТАСС): https://tass.ru/ekonomika/4193251
21. Информзащита: https://www.infosec.ru/press-center/news/rynok-ib-po-itogam-2018-goda-otsenka-informzashchity/

22. На основе данных платформы Роспатент: https://searchplatform.rospatent.gov.ru/patents
23. Роспатент: https://rospatent.gov.ru/ru/inventions_utility_models
24. Gartner: https://www.gartner.com/en/research/magic-quadrant
25. Исследование «ЦСР «Северо-Запад» и Positive Technologies: https://ptsecurity.com/about/news/issledovanie-cz-sr-severo-zapad-i-positive-technologies-deficzit-kadrov-na-rynke-ib-rossii-k-2027-godu-dostignet-60-tysyach/
26. «Лаборатория Касперского»: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-obuyavlyaet-11-noyabrya-dnyom-kiberimmuniteta
27. «Лаборатория Касперского»: https://os.kaspersky.ru/cyber-immune-development/
28. КонсультантПлюс: https://www.consultant.ru/document/cons_doc_LAW_207978/
29. Минцифры России: https://digital.gov.ru/activity/czifrovizacziya-gosudarstva/vedomstvennyj-proektnyj-ofis-vpo/administrirovanie-soprovozhdenie-ispolneniya-naczionalnoj-programmy-czifrovaya-ekonomika-rossijskoj-federaczii/informaczionnaya-bezopasnost
30. «Лаборатория Касперского»: https://os.kaspersky.ru/soczialnye-seti/s-yubileem-20-let-kasperskyos/#
31. Реестр российского программного обеспечения: https://reestr.digital.gov.ru/
32. Минцифры России: https://digital.gov.ru/activity/mery-podderzhki-it-otrasli
33. По оценке TAdviser
34. Прогноз развития рынка решений для информационной безопасности в Российской Федерации в 2022–2026 годах. ЦСР: https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-resheniy-dlya-informatsionnoy-bezopasnosti-v-rossiyskoy-federatsii-v-2022-2026-godakh/
35. Рынок труда в информационной безопасности в России в 2024–2027 гг.: прогнозы, проблемы и перспективы. ЦСР «Северо-Запад» и Positive Technologies: https://ptsecurity.com/research/analytics/rynok-truda-v-informaczionnoj-bezopasnosti-v-rossii-v-2024-2027-gg-prognozy-problemy-i-perspektivy/#
36. ФинЭкспертиза: https://finexpertiza.ru/press-service/researches/2022/bolsh-tsifr-nadezhd/
37. Positive Research: https://ptresearch.media/articles/platforma-standoff-365-segodnya
38. Positive Technologies: https://ptsecurity.com/research/analytics/pentests-2021-attack-scenarios/
39. Positive Research: https://ptresearch.media/articles/chto-nuzhno-i-chego-ne-nuzhno-hotet-ot-ib
40. Прогноз развития рынка кибербезопасности в Российской Федерации на 2025–2030 годы. ЦСР: https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-kiberbezopasnosti-v-rossiyskoy-federatsii-na-2025-2030-gody/
41. Исследование Б1: https://b1.ru/insights/news/media-center/b1-russian-information-security-market-survey-press-release-19-march-2025/

42. СКБ Контур: https://kontur.ru/press/news/79988-chislo_uchastnikov_rynka_ib_vyroslo
43. DGCompass от Т1. Источник (ICT.Moscow): https://ict.moscow/projects/ai/research/dgcompass-issledovanie-32-tekhnologicheskikh-otraslei-rossii/
44. По данным открытого проекта Open-Sourced Collection of Bug Bounty Platforms https://github.com/disclose/bug-bounty-platforms
45. Positive Technologies: https://ptsecurity.com/research/analytics/itogi-raboty-platformy-standoff-bug-bounty-na-noyabr-2024-goda/#
46. Коммерсант: https://www.kommersant.ru/doc/6173384
47. Минцифры России: https://digital.gov.ru/activity/kiberbezopasnost/bagbaunti-minczifry
48. BI.ZONE: https://bi.zone/news/bi-zone-bug-bounty-gossektor-i-fintekh-stali-osnovnymi-drayverami-bagbaunti-v-2024-godu
49. По данным АНО «Национальные приоритеты». Источник (TAdviser): Льготы и меры поддержки для ИТ-компаний в России.
50. Распоряжение Правительства России №3502-р от 17 ноября 2022 г. Источник (Российская газета): https://rg.ru/documents/2022/11/23/pravitelstvo-rasp3502-site-dok.html?
51. CNews: https://www.cnews.ru/news/top/2022-11-22_v_rossijskih_vuzah_vyrosla
52. Яков и Партнеры: https://yakovpartners.ru/publications/social-public-sector/
53. Positive Technologies: https://ptsecurity.com/research/analytics/itogi-pervogo-goda-raboty-platformy-standoff-365-bug-bounty/
54. RSAC: https://www.rsaconference.com/about/faq
55. Positive Technologies: https://ptsecurity.com/research/analytics/new-cybersecurity-from-process-to-result/
56. Коммерсант: https://www.kommersant.ru/doc/5524837
57. Positive Technologies: https://ptsecurity.com/research/analytics/results-of-incident-investigation-and-retrospective-analysis-projects-2024-2025/#
58. ГК «Солар»: https://rt-solar.ru/about_company/comprehensive_information_security/ https://rt-solar.ru/events/news/5455/
59. АО «Кибериспытание»: https://cyberfy.ru/

Вся информация, содержащаяся в настоящем документе (далее также «Исследование»), предназначена только для информационных целей, носит исключительно ознакомительный характер и не является профессиональной консультацией или рекомендацией. Лица, пользующиеся информацией, приведенной в Исследовании, соглашаются с тем, что информация может стать устаревшей, неточной или неполной. Команда, проводившая Исследование, не дает обещаний или гарантий относительно точности, полноты, адекватности, своевременности или актуальности информации, содержащейся в Исследовании. Независимая проверка данных и предположений, изложенных в Исследовании — не проводилась. Если какое-либо лицо полагается на информацию, содержащуюся в материалах Исследования, то оно делает это исключительно на свой собственный риск. Авторы Исследования, их аффилированные лица, а также организаторы презентации не несут какой-либо юридической, финансовой или иной ответственности за прямые, косвенные или иные последствия использования или трактовки информации, представленной в Исследовании. Для принятия значимых решений рекомендуется привлекать профильных экспертов и опираться на актуальные официальные источники данных.

Фонд развития результативной кибербезопасности Сайберус объединяет силы разработчиков технологий киберзащиты, бизнеса и государства для построения безопасного цифрового будущего России и мира.

Фонд инвестирует в лидеров рынка и перспективные технологии, создаёт новые продукты, решает общеиндустриальные задачи и способствует развитию экспорта технологий в страны-партнёры.

Партнёрам
partner@cyberus.com

СМИ
pr@cyberus.com