Сайберус

ИНСТИТУТ ЭКОНОМИКИ РОСТА ИМ. СТОЛЫПИНА П.А.

РЕЗЮМЕ ИССЛЕДОВАНИЯ

# **Кибербезопасность России:** сила технологического развития

cyberus.com

2026

Полная версия 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.

# 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.

1

ЭКОНОМИКА 4

### 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.

2

ИНВЕСТИЦИИ 5

### 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.

3

ТРАНСФОРМАЦИЯ 6

### 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.

4

ГОСПОЛИТИКА 7

### 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.

5

ТЕХНОЛОГИИ 8–9

### 100% сделано в России: полный стек решений

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

6

ЛЮДИ 10

### 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.

В исследовании понятия «кибербезопасность» и «информационная безопасность» используются как синонимы.

# Кибербезопасность как драйвер роста экономики

Высокий уровень зрелости российской ИБ-индустрии — скрытый фактор общего экономического роста страны. На фоне растущего числа киберугроз киберустойчивость создает условия для поддержания цифрового доверия и ускоренного развития отраслей экономики, активно внедряющих новые технологии.

**3,6–5,3 трлн руб.**

Оценка совокупного вклада отрасли кибербезопасности в российскую экономику на 2025 г.*

**~2% ВВП**

В него входят:

Синергетические эффекты за счет создания условий для ускоренного развития других отраслей экономики и поддержания цифрового доверия

Прямой предотвращенный ущерб от кибератак — неслучившиеся потери выручки, компенсации контрагентам, расходы на восстановление операционной деятельности и др.

Косвенный предотвращенный ущерб — репутационный ущерб, ущерб от нарушения цепочек поставок, снижение оценки стоимости компаний и др.

Прямой вклад — добавленная стоимость, которую создает сама ИБ-отрасль

**x12**

Совокупный мультипликатор на уровне экономики

*В основе оценки лежит аппроксимация страновых эффектов, посчитанных Всемирным банком для стран с высоким уровнем развития кибербезопасности, применение детализированных мультипликаторов роста добавленной стоимости по отдельным отраслям российской экономики, а также методы сценарного моделирования при разном уровне расходов на ИБ-решения.

Источники: Минэкономразвития России, Всемирный банк, ЦСР, экспертная оценка

# Экономика защиты для компаний: инвестиции в устойчивость бизнеса

С 2022 года 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. Результаты исследования показывают, что для крупных компаний расходы на ИБ-решения окупаются.

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

**0,3**
**трлн руб.**
Размер рынка ИБ

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

У заказчиков растет запрос на оценку эффективности расходов на ИБ и уровень собственной защищенности. На российском рынке развиваются общемировые практики и разрабатываются новые подходы к измерению киберустойчивости, понятные топ-менеджменту.

**до 30 000**
**человек**
выросло количество зарегистрированных исследователей на багбаунти-платформах с 2022 года

**в 6 раз**
увеличилось суммарное количество запущенных программ багбаунти и кибериспытаний, в т. ч. от крупнейших ИТ-компаний, банков и государственных структур

*Оценка за 2024 г. Для оценки использовались методы сценарного моделирования ущерба при разном уровне расходов на ИБ-решения, рассматривалось два сценария (с минимальным и максимальным прямым ущербом).

Источники: Всемирный банк, ЦСР, Positive Technologies, «Кибериспытание», экспертная оценка

# 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<br>УЯЗВИМЫЙ ПАРИТЕТ | 2017–2021<br>ФОКУС НА ОТЕЧЕСТВЕННЫЕ РЕШЕНИЯ | 2022–2025<br>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<br>+ [2] Результативная кибербезопасность и недопустимые события | [1] [2]<br>+ [3] Кибериспытания<br>+ [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.

# 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

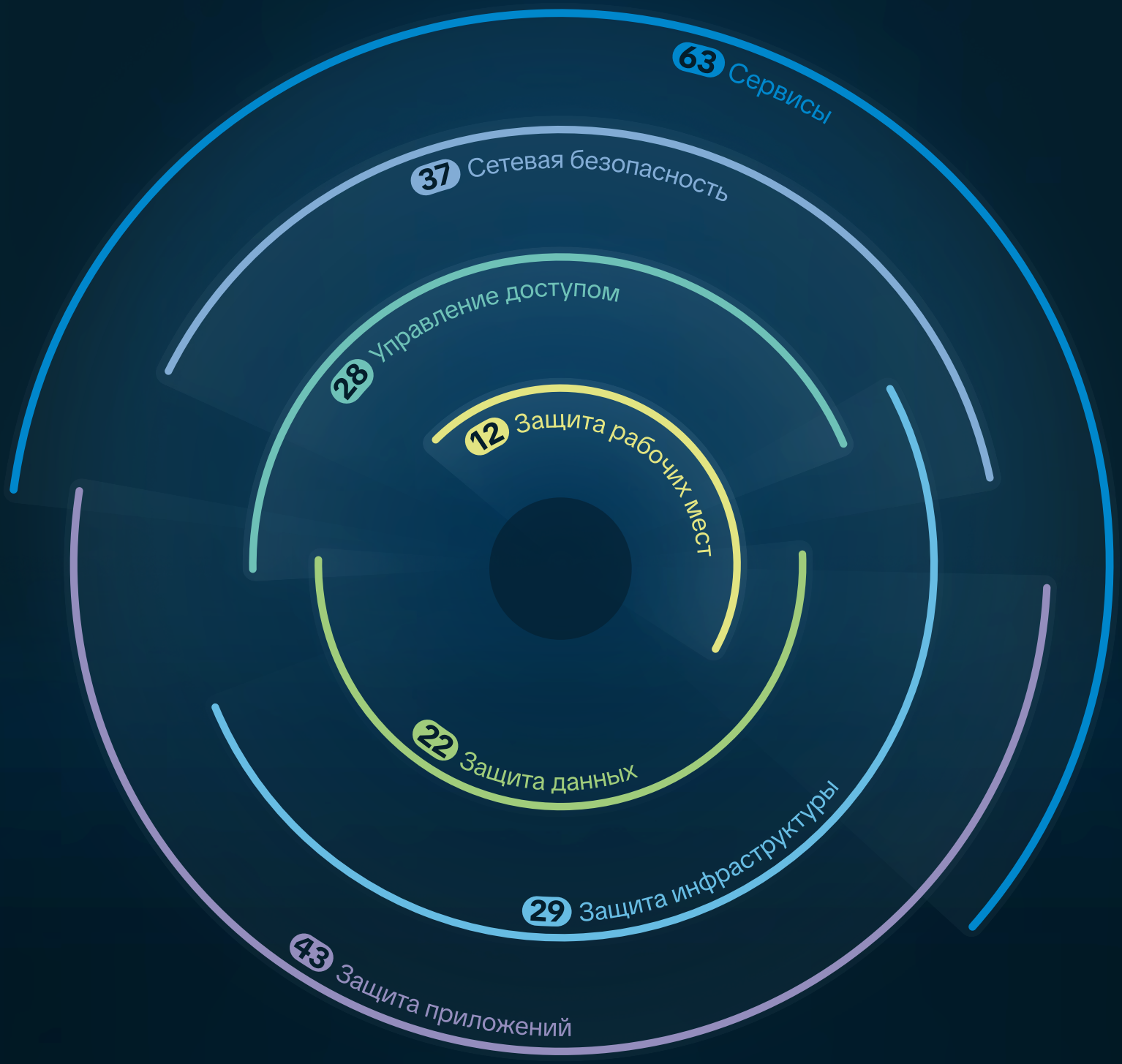
Методика определения недопустимых событий от Минцифры России

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

# 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**

# 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

**4**
направления

**40+**
ролей от старта до топ-уровня

**25+**
специализаций

Начальный уровень (0–3 года)

Продвинутые роли и специализация (3–5 лет)

Топ-уровень (>5 лет)

Дальнейшее развитие

**Имитация атак и проверка защищенности**

- Исследователь безопасности

**Противодействие и расследования**

- Аналитик SOC L1
- Специалист по управлению уязвимостями

**Поддержка и администрирование систем ИБ**

- Администратор ИБ
- Инженер по ИБ
- Администратор средств защиты информации
- Инженер по сетевой безопасности
- Специалист поддержки по ИБ

**Безопасная разработка**

- Специалист по безопасной разработке приложений

- Специалист по анализу защищенности → 7 специализаций
- Пентестер → 2 специализации (для внутреннего использования)
- Эксперт Red Team
- Исследователь безопасности (реверс-инженер) → 4 специализации
- Аналитик по выявлению и реагированию на инциденты → Threat Hunter; Аналитик Threat Intelligence; Аналитик SOC L3; Специалист по цифровой криминалистике
- Аналитик SOC L2
- Антифрод-аналитик
- Консультант по ИБ → 12 специализаций
- Специалист по управлению доступами → Эксперт КИИ (рост из инженера АСУ ТП); Консультант по ИБ КИИ; Специалист по защите информации КИИ
- AppSec-инженер → 4 специализации
- DevSecOps-инженер → SecOps-аналитик (Cloud & Container Security); Cloud Security инженер; MLSecOps-инженер

Дополнительные роли

- Менеджер продукта по ИБ
- Руководитель ИБ-проектов
- Аналитик ИБ
- Системный аналитик по ИБ

- Белый хакер топ-уровня / Свободный исследователь
  - Переходят **часто** → Предприниматель / C-level в ИБ
  - Переходят **редко** → Заместитель / советник CISO
- Эксперт Red Team → Заместитель / советник CISO
- Руководитель направления SOC → Заместитель / советник CISO
- Архитектор / проектировщик ИБ → Заместитель / советник CISO
- Руководитель направления AppSec
- Архитектор безопасности приложений
- Руководитель безопасности продукта

Заместитель / советник CISO

Запрос на CISO, знающих AppSec

Директор по ИБ (CISO)/ C-level в ИБ

Дополнительные роли для совмещения с основной из любого направления

- Преподаватель / тренер кибербезопасности

Схема составлена с учетом наличия различных позиций по направлению ИБ в компаниях. На схеме не отражены ИБ-роли, связанные с организационно-правовой защитой информации. Эти роли составляют самостоятельное направление в сфере ИБ и требуют отдельного анализа.

Роль — совокупность задач, которые решает специалист, требующие определенного набора знаний и навыков.

Топ-уровень

Старт ▶

Резюме
исследования

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