Рынок кибербезопасности России

Российский рынок информационной безопасности к 2025 году стал одним из самых быстрорастущих сегментов цифровой экономики: по оценкам Центра стратегических разработок, его объём достиг 364 млрд руб. при росте 16,1% за год. Доклад «Рынок ИБ в России 2026–2031» показывает не только масштаб, но и изменение структуры, что делает этот массив данных важным источником для исследователей в области информационных технологий, экономики и управления.

По прогнозу Центра, в 2026–2031 годах рынок информационной безопасности в России будет расти в среднем на 19,4% в год, что приведет к более чем двукратному увеличению объема к 2031 году. Значительная часть прироста придется на услуги: уже в 2025 году объем услуг в сфере информационной безопасности оценивается в 93,5 млрд руб. с ростом 10,7% год к году, прежде всего за счет услуг удаленной защиты и мониторинга, когда специализированные организации берут на себя круглосуточный контроль и реагирование на инциденты для заказчиков.

Структура рынка описывается шестью ключевыми направлениями:

защита сетевой инфраструктуры; защита конечных устройств (компьютеров, мобильных устройств и других рабочих станций); защита инфраструктуры (серверов, виртуальных сред, промышленных систем); защита прикладных программ и сервисов; защита данных; управление доступом и цифровыми идентичностями пользователей и устройств. В 2025 году наибольшую долю занимает защита сетей: около 32,5% рынка (88,1 млрд руб.), тогда как защита инфраструктуры и конечных устройств формирует 16,6% (45,0 млрд руб.) и 14,9% (40,3 млрд руб.) соответственно. Быстрее всего растет защита прикладных систем, где темпы увеличения достигают порядка 45,6% в год, что отражает усложнение архитектуры приложений, широкое использование программных интерфейсов и рост числа уязвимостей в распределенных программных комплексах.

Рынок заметно концентрирован: в ключевых подсегментах доминируют российские компании. В защите инфраструктуры и приложений лидируют, в частности, Positive Technologies и BI.ZONE, в сетевой защите сильные позиции занимает UserGate, в защите данных — Infowatch. Показательно, что отечественные разработчики занимают ведущие позиции именно в тех сегментах, где отказ от зарубежных решений наиболее критичен: в сетевых экранах и средствах фильтрации трафика, защите конечных устройств, системах централизованного управления событиями информационной безопасности и реагирования на инциденты, комплексах предотвращения утечек данных и системах управления правами доступа.

В докладе российская динамика сопоставляется с оценками международных исследовательских компаний, изучающих мировой рынок информационной безопасности. На глобальном уровне быстрее всего растут решения для защиты облачных инфраструктур и приложений, средства контроля использования облачных сервисов, системы оценки подверженности угрозам и подходы, в центре которых управление цифровыми идентичностями пользователей и сервисов. В России при этом дольше сохраняется высокая доля классических решений для защиты сети и рабочих станций, что подчеркивает специфику развития в условиях санкций и ограниченного доступа к зарубежным платформам и открывает поле для сравнительных исследований цифрового суверенитета и регуляторных моделей.

Отдельный пласт доклада связан с технологиями. Отмечается переход к проектированию систем защиты с «заложенным» использованием искусственного интеллекта и активное внедрение генеративных моделей, в том числе решений, которые извлекают и анализируют накопленные в организации данные для поддержки аналитиков по безопасности. Такие модели применяются для расстановки приоритетов при обработке потока оповещений, предварительного анализа инцидентов и автоматического формирования рекомендаций, что снижает нагрузку на специалистов и частично компенсирует дефицит кадров. Это меняет устройство центров мониторинга безопасности и поднимает вопрос о новых компетенциях на стыке информационной безопасности и методов машинного обучения.

Важным направлением роста становится защита облачно-родной, то есть изначально развернутой в облачной среде, инфраструктуры. Речь идет о контроле конфигураций и уязвимостей, защите облачных приложений, защите программных интерфейсов, управлении правами и идентичностями в облаке. На этом фоне возрастает значение защиты данных и подходов к управлению безопасностью данных, нацеленных на выявление, классификацию и защиту информации в распределенных системах, что напрямую связано с исследованиями

в области управления данными и защиты частной жизни.

Услуги в сфере информационной безопасности из исключения превращаются в устойчивую норму. По мере распространения управляемых сервисов защиты, удаленных центров мониторинга и других форм «безопасности по подписке» выстраиваются новые отношения между поставщиками и заказчиками, в которых границы ответственности за инциденты и последствия атак требуют отдельного анализа. Вокруг центров мониторинга формируется экосистема, включающая отраслевые центры для промышленности, топливно-энергетического комплекса, финансового сектора, а также услуги по сбору и обмену информацией об угрозах и активностях злоумышленников.

Регуляторная среда одновременно стимулирует развитие рынка и усложняет вход на него. Ужесточение требований к защите критической информационной инфраструктуры, персональных данных и финансовых сервисов повышает спрос на решения для управления рисками и соответствия требованиям, системы учета и расследования инцидентов, а также средства аудита. При этом сохраняется острый дефицит квалифицированных специалистов: по оценкам, нехватка кадров в сфере информационной безопасности будет заметна как минимум до конца текущего десятилетия. На этом фоне усиливается курс на автоматизацию, упрощение пользовательских интерфейсов и использование систем искусственного интеллекта как инструмента поддержки специалистов разного уровня подготовки.

Прогноз до 2031 года строится как базовый сценарий с сохранением высоких темпов роста и постепенным смещением структуры рынка в пользу услуг, решений для облачной инфраструктуры и средств защиты, встроенных в процессы разработки и эксплуатации программных систем. Среди ключевых факторов роста называются дальнейшая цифровизация отраслей, увеличение масштаба и сложности кибератак, ужесточение требований регуляторов и продолжение замещения зарубежных решений в критически важных сегментах.

Для научного сообщества этот массив данных формирует четкий круг вопросов. Как замещение зарубежных систем влияет на инновационный потенциал отрасли и структуру конкуренции на рынке информационной безопасности? Как меняется распределение ответственности за киберриски между заказчиками и поставщиками услуг? Какие институциональные решения необходимы для устойчивого развития сети центров мониторинга и обмена информацией об угрозах? Как включение генеративного искусственного интеллекта в практики защиты трансформирует образовательные программы и профессиональные траектории специалистов по безопасности?

Доклад Центра стратегических разработок дает плотную количественную и качественную основу и очерчивает контуры технологических и институциональных изменений, как возможность перейти от общих рассуждений о «рынке ИБ» к анализу конкретных траекторий, участников и практик, которые будут определять цифровую безопасность в России в ближайшее десятилетие.

Доклад «Рынок ИБ в России 2026–2031»