Исследование

Обзор рынка информационной безопасности 2025

Инфосистемы Джет

SECURITY TEAM

Оглавление

Введение

Год назад мы выпустили первый для нас обзор рынка ИБ, в котором привели сравнительные показатели нашей коммерческой деятельности в разрезе конкретных направлений информационной безопасности за 2024 год. В этом году повторяем подобный обзор, добавляя к нему результаты 2025 года.

Обзор рынка ИБ 2024

Несмотря на то, что результаты в части объемов бизнеса по различным направлениям не содержат в себе никаких сенсаций относительно результатов 2023 и 2024 годов, мы видим тенденции в развитии отрасли информационной безопасности, отчетливо проявившие себя в 2025-м.

ТРЕНД №1

Как и в 2024 году, глобальным трендом на рынке остается желание построить систему обеспечения ИБ, реализующую реальную защиту бизнес-процессов. Как достаточно новый тренд мы фиксируем интерес к реальной защищенности не только в сегменте крупного и крупнейшего бизнеса, но и в сегменте среднего бизнеса, который традиционно не инвестировал в информационную безопасность. Безусловно, это связано с рядом громких, резонансных случаев кибератак на крупные российские компании в 2025-м году.

Глобальная тенденция — синергия ИТ и ИБ

ТРЕНД №2

Другой глобальной тенденцией является ускоряющееся взаимопроникновение ИТ и ИБ друг в друга. Хотя это, конечно, не новая и достаточно очевидная мысль — что без правильно организованного ИТ не может быть эффективной ИБ — на практике долгие годы ИТ-службы и ИБ-службы в значительной доле организаций существовали изолировано друг от друга, в лучшем случае соблюдая нейтралитет, в худшем вовсе были антагонистами. Сейчас мы видим, что многие организации не спешат стартовать классические ИБ-проекты по внедрению СЗИ до тех пор, пока не устранят накопленный техдолг по повышению защищенности ИТ-инфраструктур.

Ключевые особенности рынка ИБ прямо сейчас

/01

Остающаяся высокой вовлеченность высшего руководства компаний к вопросам ИБ, сочетающаяся с прагматичным подходом к выделению бюджетов. **Бюджеты выделяются на проекты, связанные с реальной защищенностью.**

/02

Все чаще возникающие у заказчиков, в том числе из финсектора и сферы промышленности, требования к гарантии результата.

Возрастающий рост интереса к различного рода кибериспытаниям на данном фоне.

/03

Фокус на обеспечение киберустойчивости и непрерывности бизнеса с той поправкой, что в качестве основной угрозы рассматриваются не традиционные пожары / затопления ЦОДов, а шифровальщики и вайперы.

/04

Модернизация ИТ-инфраструктур в ходе «ИБ-проектов». Если тот факт, что любой новый проект по ИТ должен включать в себя ИБ, уже давно не новость, то реализация серьезных изменений в ИТ (харденинг, микросегментация, устранение уязвимостей, борьба с лишними полномочиями и другое) в ходе ИБ-проектов — относительно новый тренд.

Как вы докажете, что ваш проект по ИБ сделает нас защищеннее?

/05

Опережающий рост спроса на разного рода коммерческие сервисы.

Это одновременный ответ на два вопроса: кадровый голод и желание получить сервис здесь и сейчас, не тратя время на последовательное внедрение СЗИ и выстраивание процессов внутри.

/06

Существенный рост интереса к проектам по ИБ у организаций среднего бизнеса.

/07

Два классических драйвера рынка последних лет — импортозамещение и усиление регуляторных требований — нисколько не ослабевают, а в некоторых направлениях, наоборот, превалируют.

/08

Несмотря на значительное внимание к этой теме, **использование ИИ еще не стало критическим образом определять подходы к нападению и защите.** Количество пока не перешло в новое качество, и, по нашей оценке, не перейдет в ближайшие два–три года. Хотя рост использования ИИ в ИБ безусловен.

ИИ пока не определяет подходы к нападению и защите

Методика составления обзора

Для того чтобы результаты по годам были соизмеримы между собой, при подготовке обзора мы решили не менять методику его составления. Единственная правка, которую мы внесли, заключается в том, что мы разделили объем по подсистеме «XDR» на части и отнесли их к различным направлениям. Если в 2024-м году объем по XDR был сравнительно небольшим, то в 2025-м он вырос в пять раз. С учетом того, что разные вендоры понимают под XDR разное, и зачастую это не отдельное решение, а просто набор из классических продуктов, некорректно было бы относить этот объем к какому-то одному направлению.

Ниже приводится методика составления обзора без изменений относительно 2024 года.

Информационная безопасность — чрезвычайно обширная сфера, включающая в себя сотни различных решений в рамках десятков подсистем. Это затрудняет задачу создания обзора рынка, одинаково понятного как для специалистов по ИБ, так и для других заинтересованных лиц.

Безусловно, любая группировка конкретных решений в подсистемы достаточно условна и в деталях может быть проведена по-разному. В рамках данного обзора мы предлагаем ориентироваться на следующий ландшафт средств защиты информации и связанных с ними сервисов.

С нашей стороны было бы непоказательно давать статистику в разрезе каждой отдельной подсистемы или сервиса, так как сравнение выручки за 2023 и 2024 годы было бы нерелевантным для ряда подсистем из-за статистически небольшого количества реализованных по ним проектов.

С этой точки зрения приведенные ниже подсистемы ИБ и различные сервисы были сгруппированы в направления, исходя из схожести решаемых задач.

Направление	Подсистемы
Сетевая безопасность	NGFW, криптографическая защита каналов связи, NAC, NTA, Web Proxy, Firewall Management, пользовательский VPN, однонаправленные шлюзы
Защита АСУ ТП	Проекты по комплексной защите АСУ ТП
Антифрод	Проекты и решения по автоматическому обнаружению признаков внутреннего и внешнего мошенничества
Мониторинг, реагирование и управление ИБ	SIEM, SOAR, TI/TIP, sGRC, XDR (в части мониторинга). Не включая в себя услуги коммерческого SOC Jet CSIRT
Защита от вредоносного кода и целенаправленных атак	Сетевые песочницы, EDR, XDR (в части сетевой и хостовой защиты), антиспам, антивирусы, СЗИ от НСД, Deception Tools, решения по защите виртуализации, EMM.
Управление доступом	IdM, многофакторная аутентификация, VDR, PIM, менеджеры паролей
Защита данных	DLP, решение по маркированию данных, DCAP, решения по маскированию данных, DAM
Защита приложений (AppSec)	WAF, Anti-DDoS, проекты по DevSecOps
Управление уязвимостями	VM, контроль конфигураций, BAS
Консалтинг	Проекты по выполнению требований законодательства (не включая стоимости необходимых решений), а также по пентестам и экспертному консалтингу

Экспертные сервисы	Услуги коммерческого SOC (Jet CSIRT), проекты по киберразведке, кибер-криминалистике и киберучениям. Услуги по оказанию технической под-держки и поддержанию работоспособности СЗИ (не включая стоимости вендорской поддержки и продлений)
Криптографическая защита	УЦ/PKI, СКЗИ (не включая криптошлюзы)

Другой практической пользой подобной группировки является то, что иногда достаточно трудно определить, к какому классу решений отнести тот или иной продукт. Например, полноценное NGFW-решение в конкретном проек-те может быть использовано под задачу проксирования пользовательского трафика и применяться только для этой цели. Соответственно, проект фор-мально может быть отнесен как к NGFW, так и к Web-Proxy.

Отдельно стоит отметить направление «Защита АСУ ТП». Оно может быть рассмотрено как в узком смысле, включая в себя только специализирован-ные решения по защите промышленных сетей и хостов, так и в широком, когда вне зависимости от применяемых средств защиты информации, если соответствующий проект реализовывался с целью защиты конкретных АСУ ТП, весь проект целиком отнесен к данному направлению. В рамках нашего обзора был применен «широкий» подход.

Чтобы снизить объем искажений статистики, из расчетов мы исключили стоимость сетевого и серверного оборудования, СХД, которые внедряются для обеспечения функционирования средств защиты, а также работы по их внедрению и поддержке.

Пояснение к методике подсчета финансовых показателей:

2023 год
795
проектов

2024 год
970
проектов

2025 год
905
проектов

Каждый проект, исходя из реализован-ных решений, был отнесен к одному или нескольким направлениям информаци-онной безопасности. Далее направления сравнивались по совокупной выручке.

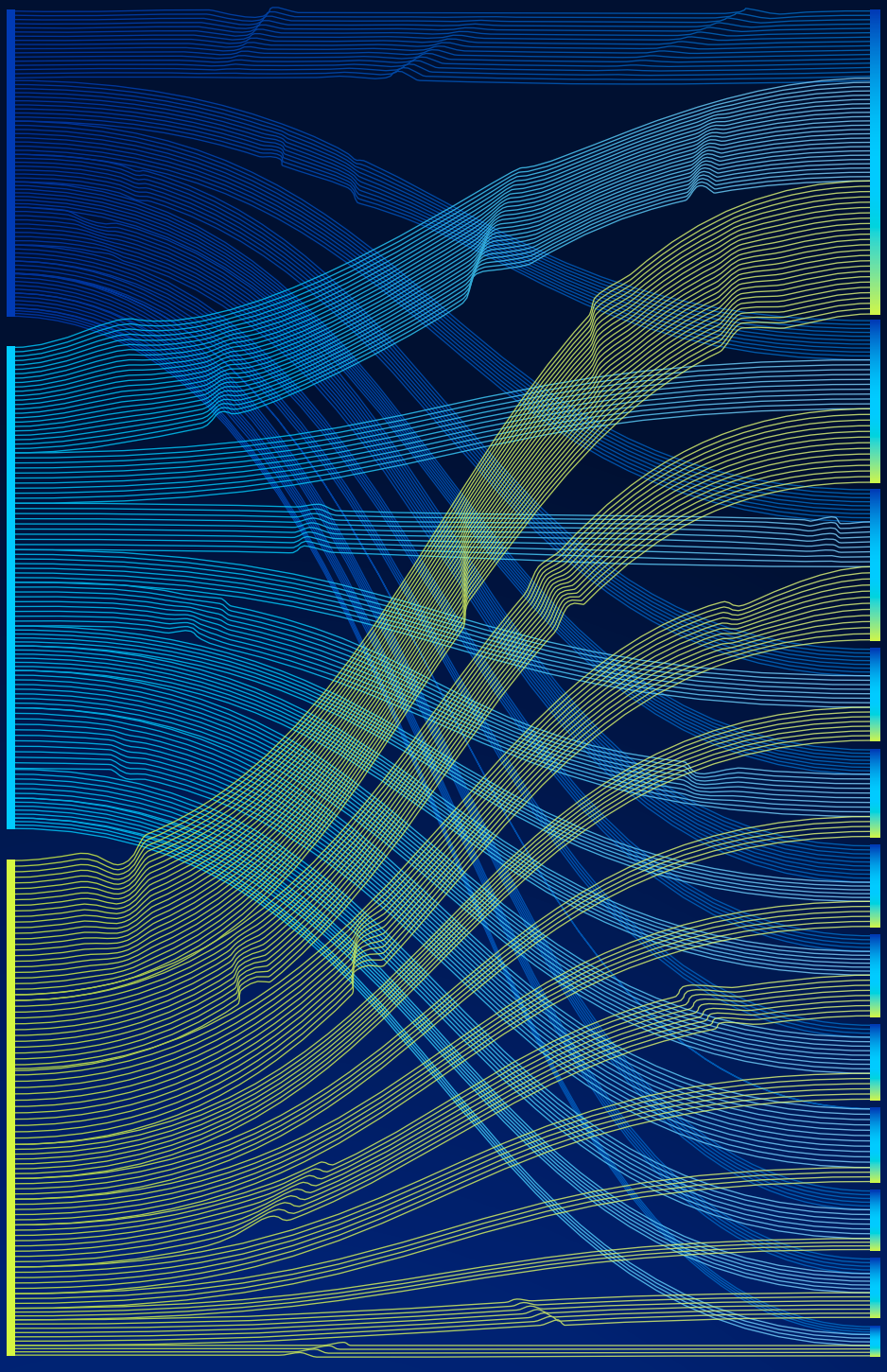
Проекты рассматривались в целом, включая стоимость лицензии и оборудо-вания, а также ассоциированных с ним интеграционных, консалтинговых и аналитических работ.

Для проектов, в которых реализовывались комплексные системы обеспечения ИБ, выделяли долю выручки для каждого из направлений.

Проекты по проектированию или, например, настройке соответствующих подсистем также относились к ним и не выделялись отдельно.

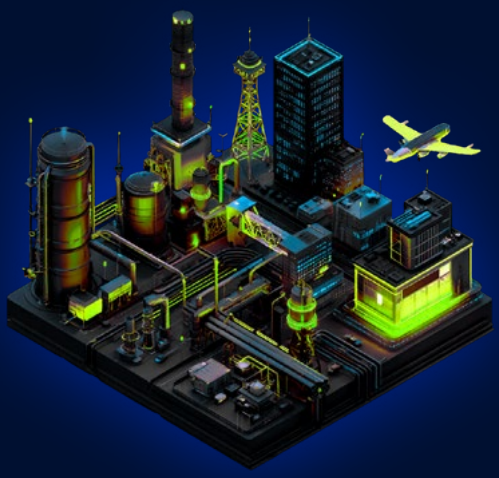
Структура рынка информационной безопасности

Совокупный рост нашей выручки по проектам в области информационной безопасности составил 12%. С 20,47 млрд рублей в 2024 году до 22,99 млрд рублей в 2025 году. При этом, разумеется, финансовые показатели по разным направлениям менялись по-разному.



/01 Сетевая безопасность

2025 год в очередной раз подтвердил, что сетевая безопасность — совокупно самое крупное направление на рынке. Объемы ни по NGFW, ни по гостовым криптошлюзам не снижаются, а только растут. И будут расти далее, поскольку процесс импортозамещения в NGFW далек от своего завершения. Хороший рост показывает NTA, который все чаще позиционируется как составная часть SOC, и NAC для обеспечения защиты от атак с физическим проникновением. Кроме этого, проекты по NAC-решениям все чаще включают в себя не только решение ИБ-шных задач, но и ИТ-шных. Например, организация гостевого Wi-Fi-доступа.



Сетевая безопасность — самое крупное направление на рынке

/02 Защита от вредоносных кодов и целенаправленных атак

Один из лидеров роста, драйвером в котором является необходимость защиты от шифровальщиков. Отдельное внимание стоит уделить EDR. Раньше EDR воспринимались как некая «вишенка на торте», требующая очень зрелой и экспертной команды, и поэтому доступная не всем. Сейчас и с ростом зрелости рынка, и с развитием продуктов, и с их все возрастающей ролью в рамках процессов SOC, EDR становится неотъемлемой частью комплексных систем ИБ.

/03 Мониторинг и реагирование

Направление, которое, наверное, наиболее тесно связано с обеспечением реальной защищенности, один из лидеров роста в 2025 году. Если раньше ядром комплексных проектов была сетевая и хостовая безопасность, то сейчас фокус смещен в сторону обязательного наличия SOC, неважно, in-house или коммерческого. Тезис, что без процесса мониторинга 24x7 внедренные средства защиты, по сути, бесполезны, не просто декларируется, но и находит устойчивое отражение в проектах.

/04 Управление доступом

Одно из самых стабильных направлений в нашем бизнесе, устойчиво пользующееся спросом. Его ключевым драйвером являются крупные, долгосрочные проекты по внедрению IDM, а также достаточно новая тема защиты биометрических данных.

/05 Экспертные сервисы

Лидер роста, главным образом в части услуг по мониторингу и реагированию (наш коммерческий SOC — Jet CSIRT). Особо следует отметить изменение парадигмы проектов по SOC. Если раньше чаще встречались проекты, в которых заказчик сначала строит КСОИБ, а потом на второй или третий год развития отдельным проектом строит свой SOC либо передает процесс мониторинга на аутсорсинг, то сейчас все чаще встречаются проекты, когда строительство КСОИБ включается внутрь построения SOC. Иными словами — различные средства защиты рассматриваются в первую очередь как сенсоры для SOC. В подтверждение этого мы наблюдаем спрос на ранний запуск SOC на малых объемах, например, только на базе телеметрии и алертов EDR. Такая тенденция характерна прежде всего для компаний малого и среднего бизнеса. Кроме этого, сервисы мониторинга внешних цифровых угроз и киберучений стабильно растут, что в целом неудивительно с учетом их значительной практической пользы в соотношении с размером затрат на них.

JET CSIRT

Экспертные сервисы растут быстрее всех

/06

Управление уязвимостями

Для нас было некоторым удивлением увидеть по итогам года снижение по данному направлению, можно отметить две причины для этого — аномальный результат 2024 года (в нашем бизнесе) и, по-видимому, общее насыщение рынка продуктами, конкуренция между которыми ведется не только в части функциональности, но и в части ценовой политики. Если измерять в штуках, количество проектов по теме управления уязвимостями не уменьшилось, однако их средний чек стал меньше. Аналогичную картину мы прогнозируем и на 2026 год: высокий интерес рынка ко всему, что связано с управлением уязвимостями и конфигурациями (что вполне объяснимо в разрезе общей востребованности темы реальной защищенности), но вместе с этим и снижение среднего чека проекта. Также можем отметить высокий интерес к работам, связанным с харденингом ИТ-инфраструктуры как базовой меры защиты.

/07

Защита АСУ ТП

Тема защиты АСУ ТП ощутимо росла для нас в 2025 году. Связано это с тем, что жизненный цикл комплексного проекта существенно превышает календарный год и приближается к двум годам. Где в первый год производится обследование и проектирование, а внедрение средств защиты перетекает на второй год. Если в 2024 году мы в основном занимались проектированием, то в 2025 было больше проектов по внедрению.

/08

Защита приложений

Защита приложений показывает устойчивый рост, это связано с нормативным регулированием и с общим повышением зрелости заказчиков в данном вопросе. Сравнительно небольшой (относительно наиболее крупных) объем данного направления связан как с тем, что в части безопасной разработки (DevSec) во многом применяются opensource-решения, так и с тем, что многие продукты реализуются по сервисной схеме (WAF/AntiDDoS как сервис), не включающей в себя больших капитальных затрат.

/09

Антифрод

Несмотря на некоторое падение в финансовых результатах (вызванное, скорее, особенностью реализации наших проектов, нежели снижением интереса рынка), антифрод остается одним из важнейших элементов комплексной защиты организации. Хоть и не от угроз, связанных с компьютерными атаками, но от реальных финансовых потерь, причем не только в финансовой, но и других отраслях экономики.

/10

Криптографическая защита

Как мы и ожидали, в наших цифрах направление криптографической защиты информации уменьшилось по сравнению с 2024 годом, но отнюдь не до показателей 2023 года. Драйвер роста здесь — корпоративные центры сертификации под отечественные Linux-системы. Мы предполагаем, что данное направление будет все больше увеличиваться и в количестве проектов, и в объеме денег.

/11

Защита данных

Направление, показавшее наиболее значительный спад по итогам 2025-го года. Можно предположить, что это связано с общим насыщением рынка (DLP-системы очень давно присутствуют на рынке и реализованы в большинстве крупных заказчиков) и с тем, что в борьбе за фокус внимания тема защиты от инсайдеров существенно проигрывает теме защиты от взломов и разрушения инфраструктуры.

/12

Консалтинг

Результат нужен здесь и сейчас

Традиционное направление, включающее в себя всевозможные аудиты, пентесты, а также разработку планов по развитию функции ИБ. Ключевым изменением здесь можно назвать то, что доля проектов по чистому аудиту снижается. Рынок существенно ускорился, результат в части реальной защищенности нужен здесь и сейчас. В этих условиях заказчики не готовы до полугода ждать результатов классического аудита, после которого необходимо защищать стратегию и только потом выходить на этап проектирования. С другой стороны, существенно растет спрос на консалтинговые сервисы, связанные с непосредственным повышением уровня защищенности. Различные table-top-учения, red-team-пентесты, кибериспытания и так далее.

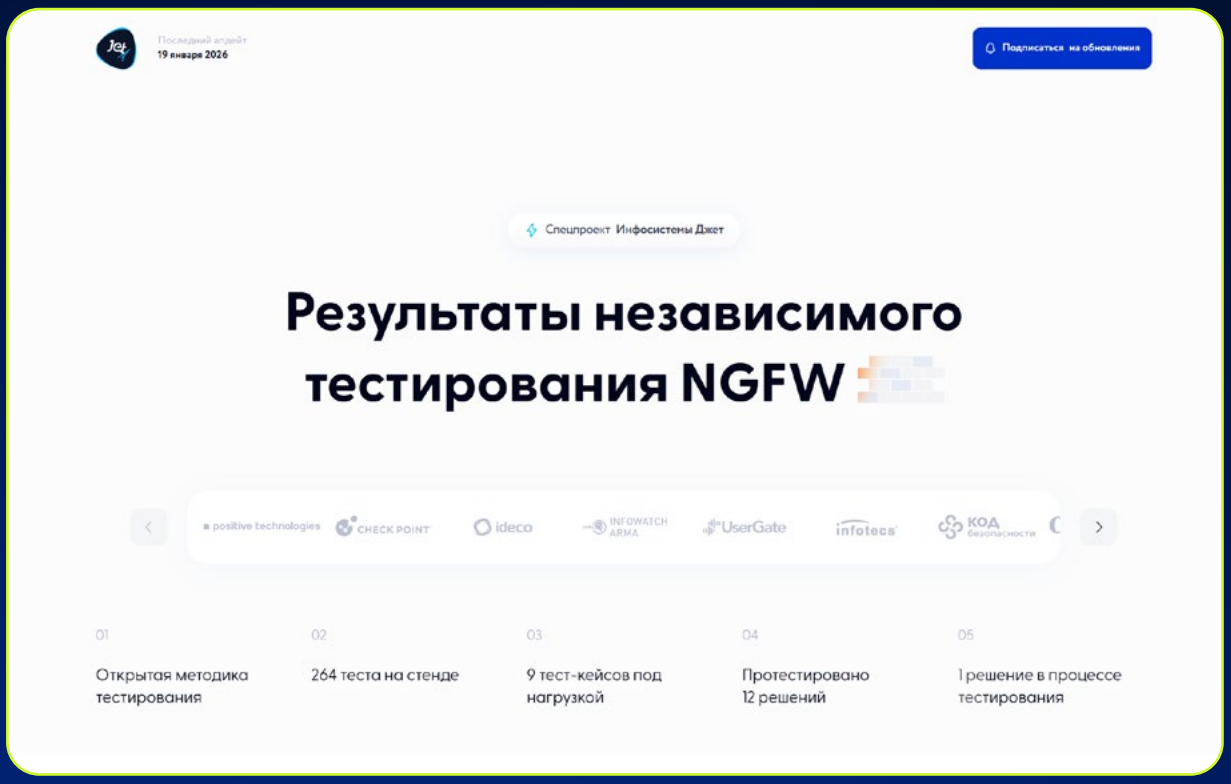
Сетевая безопасность

Несмотря на то, что в 2025 году несколько крупных вендоров, ранее заявлявших намерение выпустить на рынок свой NGFW, отказались от этих планов, рынок NGFW остается крайне конкурентным.

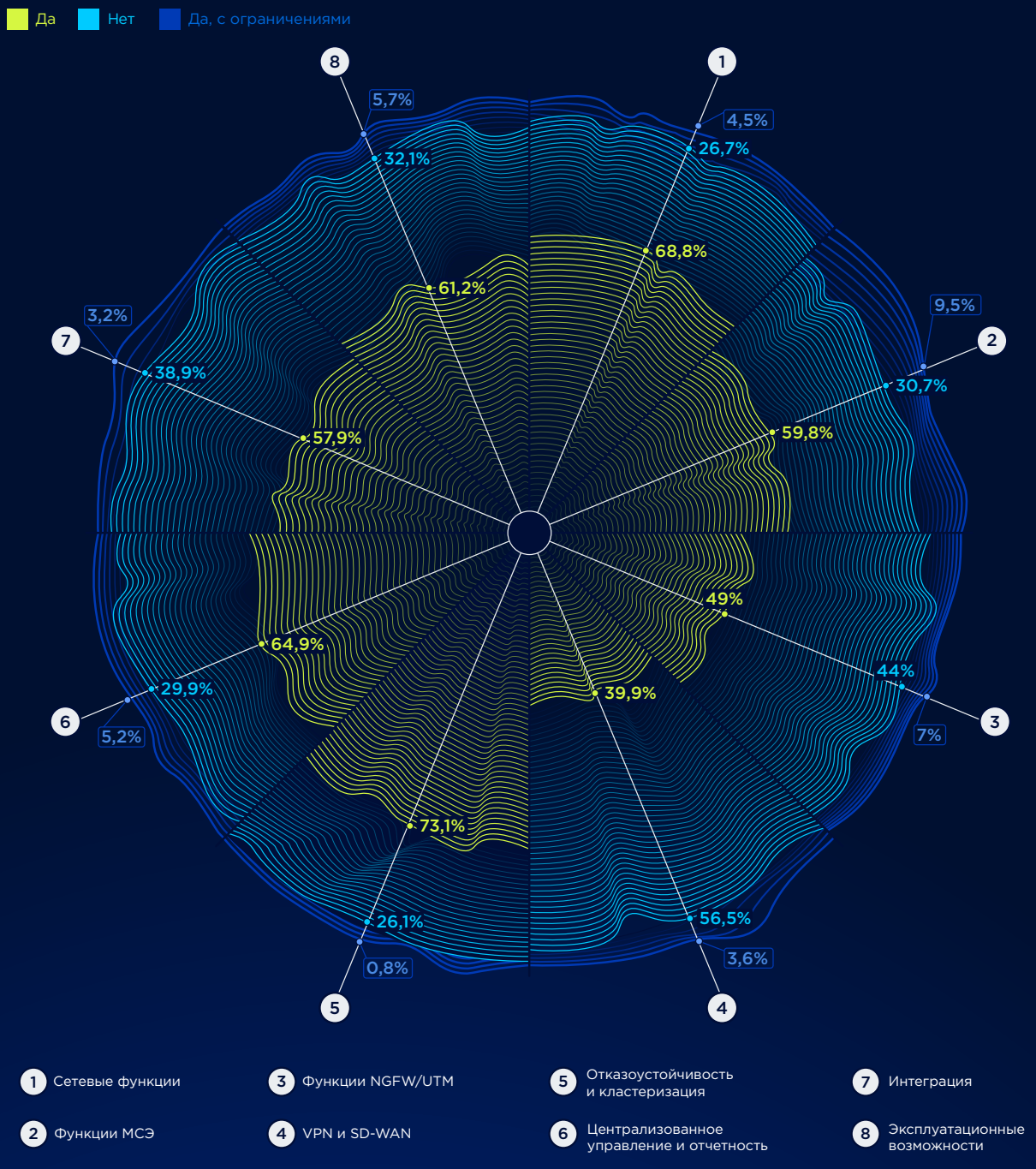
В рамках нашей лаборатории ngfw.jet.su мы продолжаем тестировать по открытой методике представленные на российском рынке продукты, в том числе доступны результаты для:

- PT NGFW 1.7.2
- C-Терра Экран-М
- Ideco NGFW v18 и v16
- Континент 4.1.9 и 4.1.7
- Check Point R81.2
- InfoWatch ARMA Стена (NGFW)
- UserGate 7.1.0 RC
- VipNet Coordinator HW 5.3
- Решение китайского производителя (7000 series, v.8.0)

ngfw.jet.su



Совокупные результаты тестирования приведены на графике ниже

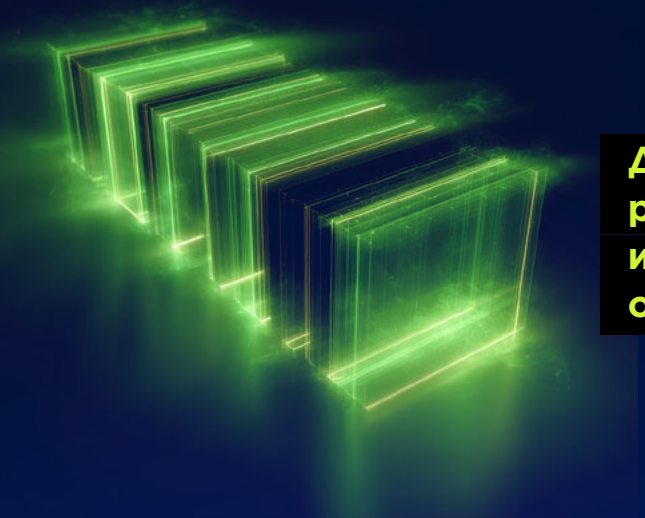


К сожалению, все еще можно констатировать, что отечественные продукты по совокупности функций отстают от мировых лидеров, по некоторым параметрам — существенно. При этом с точки зрения реализации проектов в сегменте крупного бизнеса ключевой блок-фактор, препятствующий импортозамещению, меняется. Если раньше это в первую очередь была недостаточная производительность (существующие аппаратные платформы не выдерживали требований крупного бизнеса), то сейчас, после выхода ряда продуктов High-End-класса, блок-фактором, скорее, является их надежность. Причем как надежность аппаратных платформ, так и наличие багов в программном обеспечении. Все производители NGFW, с которыми мы работаем, отмечают, что их ключевой приоритет на 2026 год — стабильность работы устройств.

Тем не менее, доля российских решений в сегменте NGFW неуклонно увеличивается. По нашей внутренней статистике, до 90% из крупнейших российских компаний уже имеют у себя в инфраструктуре отечественные решения.

Другим сдерживающим фактором для рынка NGFW является традиционная проблема с Remote Access VPN для российских решений. Безусловно, за 2025 год ситуация стала значительно лучше, однако эти количественные улучшения не перешли еще в новое качество. Можно констатировать, что вопрос RA VPN является одним из наиболее больных для NGFW и требует для своего решения набора продуктов, что усложняет общую архитектуру и эксплуатацию.

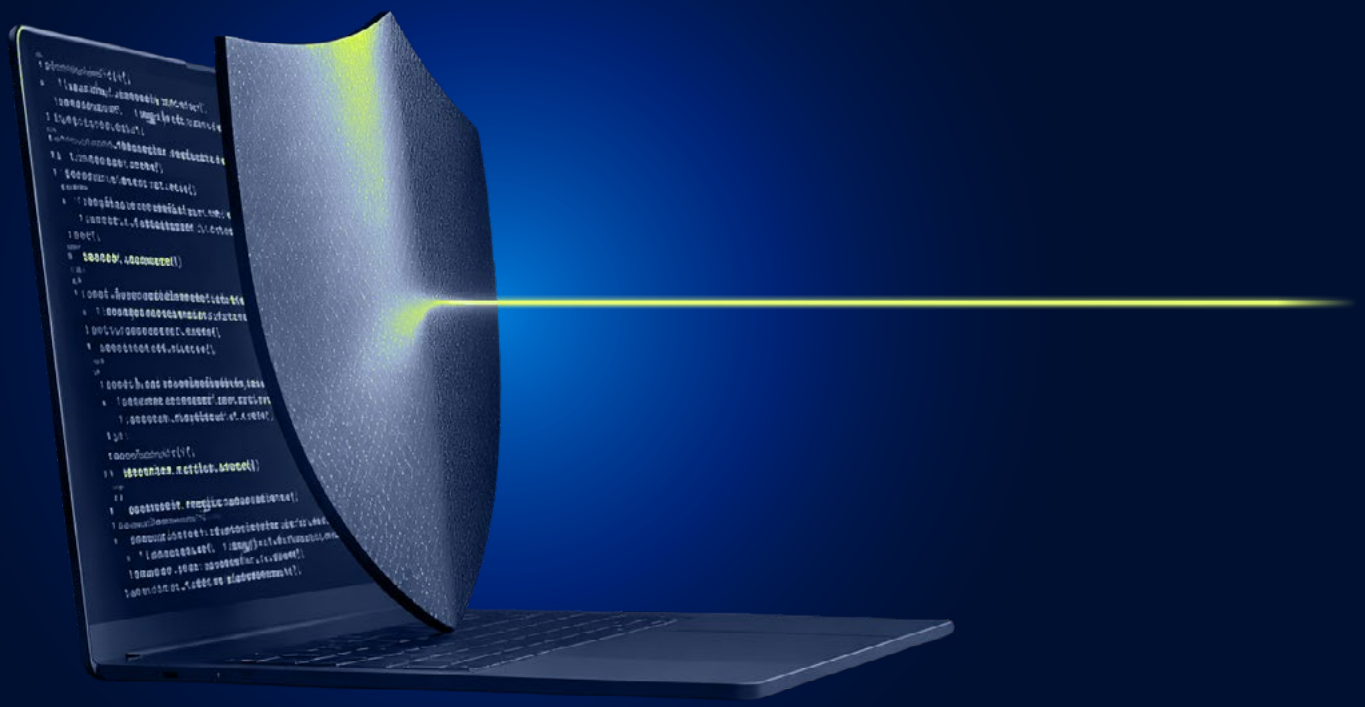
В нашей статистике серьезно выросли классические гостовые криптошлюзы, но это, скорее, особенность реализованных проектов в конкретный год, а не общая тенденция рынка, все-таки данные решения присутствуют на рынке очень давно, и ниша их применения крайне понятна.



До 90% из крупнейших российских компаний уже имеют у себя в инфраструктуре отечественные решения

А вот существенное увеличение проектов по теме NTA/NDR заслуживает отдельного упоминания, так как связано не непосредственно с вопросом сетевой безопасности, а с вопросом безопасности глобальной. NTA-решения все чаще внедряются не как отдельная подсистема, а как естественный (наряду с EDR, о чем будет сказано далее) источник событий для SOC.
В этой связи значительно увеличивается доля брокеров сетевых пакетов (для обеспечения обработки значительных объемов трафика в разных местах инфраструктуры) в проектах, по сути превращая проект по внедрению NTA в сложную инфраструктурную задачу.

Хорошими темпами растет подсистема NAC, что можно связать и с чисто эксплуатационными ИТ-шными запросами, например, по организации систем гостевого Wi-Fi-доступа.



Защита от вредоносного кода и целенаправленных атак

Это один из лидеров роста и в относительных, и в абсолютных значениях среди наших направлений. Мы фиксируем существенное увеличение проектов по всем подсистемам ИБ в данном направлении, которое в первую очередь ассоциируется с защитой от вирусов-шифровальщиков. Песочницы, защита почты, защита виртуализации — все эти подсистемы растут опережающими темпами.

Самый бурный период роста переживают EDR-решения

Ранее одно из самых экспертных, сложных в эксплуатации решений превращается в де-факто обязательный элемент комплексной системы обеспечения ИБ, неотъемлемый источник событий и инструмент реагирования для SOC.

Если раньше под технологическим ядром SOC понималась связка SIEM/SOAR/TIP, то уже сейчас в нее смело можно добавить EDR.

Кроме этого, функционал EDR-решений постоянно расширяется. С учетом планируемого выхода на рынок нескольких новых антивирусных продуктов происходит по сути слияние классических антивирусов и EDR в единую платформу хостовой защиты, условно называемую Endpoint Protection Platform. Это подтверждает тезис, что все новое — хорошо забытое старое, так как решения, называемые EPP, существовали на рынке еще лет 15 назад.

Здесь мы тоже наблюдаем устойчивую тенденцию к платформизации, roadmap различных вендоров содержат в себе идеи по добавлению к EDR (EPP) дополнительного функционала, нехарактерного для классических EDR: управление уязвимостями, RA VPN, хостовый deception и так далее. По сути, в будущем нас ждет слияние всей хостовой защиты в единый агент.

В 2025 году мы увидели существенный коммерческий спрос на XDR-решения. Каждый вендор подразумевает под XDR что-то свое, обычно набор своих классических продуктов из коробки, работающих в логике взаимообогащения событий ИБ друг от друга. И если в самом позиционировании XDR обновлений, наверное, не произошло, то в части интереса рынка мы увидели существенное изменение. Организации, которые впервые стали серьезно уделять внимание информационной безопасности, скорее, выберут единую экосистему (XDR) одного вендора, нежели будут последовательно проводить пилоты и выбор решений в каждой из соответствующих подсистем.

Мониторинг, реагирование и управление ИБ

2025 не принес серьезных качественных изменений в направление мониторинга, реагирования и управления ИБ. Напомним, к данному направлению мы относим проекты по SIEM, SOAR, TI/TIP, sGRC, не включая услуги нашего коммерческого центра мониторинга и реагирования Jet CSIRT. Изменения были, скорее, количественными, но тем не менее — существенными.

Рынок SIEM-решений продолжает насыщаться, хотя, казалось бы, что для такого старого направления состав решений должен быть более консервативным. Однако практика показывает обратное. Все больше вендоров выпускают или планируют к выпуску в ближайшее время новые SIEM, соревнуясь не только в классическом функционале, но и в новых походах.

Рынок идет по пути «экосистемности» и «платформенности», что в первую очередь затрагивает SIEM, превращая их в комбайны, объединяющие в себе SIEM/SOAR/TIP. Сейчас это отчасти маркетинг, но тенденция видна явно.

Стоит отметить, что производители SIEM-решений стали обращать внимание на совокупную стоимость владения. SIEM-решения традиционно требуют немалое количество вычислительных ресурсов, при этом с высокими запросами к производительности, для обработки и хранения собираемой телеметрии. Вопрос экономии стоит остро и требует от вендоров пересмотра архитектурных подходов и используемых технологий.

Казалось бы, техническое отставание новых решений от грандов рынка должно быть существенным, но зачастую это не совсем так. Новые решения, построенные на современных технологиях хранения и обработки данных, а также масштабирования нагрузки, лишены многих врожденных ограничений, которые характеры для решений, давно присутствующих на рынке. Это особенно актуально с учетом того, что средний объем событий ИБ в SOC неуклонно растет.

Из года в год мы фиксируем устойчивое усложнение проектов по SIEM/SOAR, часто именно тут происходит взаимопроникновение ИТ и ИБ. Вопрос ставится уже не просто «Внедрите SIEM и подключите к нему источники», а скорее как «Внедрите SIEM, определите необходимый и достаточный набор источников, настройте безопасным образом источники в части ИТ-инфраструктуры и подключите их к SIEM». Устойчиво растет количество интеграций и EPS для средней инсталляции in-house SOC, а также сложность корреляционного контента и требования к скорости его адаптации к изменяющимся атакам. В проектах по SOAR из года в год растет количество интеграций для автоматизации ручных операций команды SOC. Если раньше интеграции ограничивались только средствами защиты, то сейчас SOAR активно интегрируют со многими внутренними ИТ-сервисами, ускоряя возможности SOC-команды по обогащению и реагированию. Фактически, если у ИТ-сервиса есть описанный API или иные возможности интеграции, то такой ИТ-сервис может нести ценности для процессов мониторинга и реагирования на инциденты ИБ.

Из интересных новинок можно отметить существенный рост интереса, который пока не превратился в коммерческий спрос, на все, что связано с использованием ИИ для обработки событий и инцидентов ИБ.

Практически каждый крупный SOC, неважно, In-house или коммерческий, так или иначе экспериментирует с ИИ, в первую очередь для решения задач, связанных с сокращением ручных операций

Управление доступом

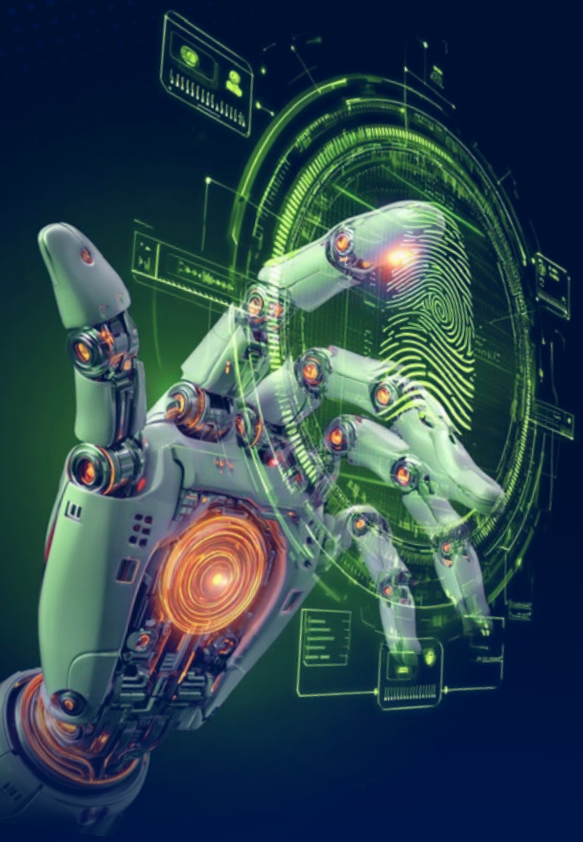
Если говорить про тренды, за последний год на рынке IDM появился ряд новых игроков на перспективу. Но на нынешней стадии зрелости они не составляют реальную конкуренцию лидерам в enterprise-сегменте, и пока их целью является, скорее, формальное закрытие требований ИБ. Помимо закрытия требований по сертификации (интерес к open-source же снизился существенно, что закономерно), ключевыми факторами выбора продуктов всегда были и остаются гибкая функциональность и возможности кастомизации, а на их развитие требуется время.

В 2026–2027 годах тренд роста будет связан с задачами автоматизации и оптимизации в крупных компаниях. Такие задачи сейчас возникают во всех направлениях, а внедрение IDM в крупных компаниях как раз дает ощутимый экономический эффект за счет сокращения трудозатрат на операционную деятельность.

Ключевыми факторами развития систем IAM в 2025 году, которые сохранят свою актуальность и в 2026, являются:

- импортозамещение;
- замена open-source (самый распространенный open-source — Keycloak);
- локализация (бывшие российские филиалы глобальных компаний продолжают строить свою инфраструктуру и отделяться от глобальных сервисов);
- использование IAM для государственных платформ;
- использование многофакторной аутентификации при доступе к бизнес-приложениям.

Если ранее 2FA в основном требовалось при подключении к инфраструктуре, то теперь учащается запрос на многофакторную аутентификацию и в бизнес-приложениях, что реализуется решениями IAM в связке с решениями 2FA.



Отдельно стоит отметить рынок биометрических систем управления доступом. В 2025 году продолжилась адаптация рынка биометрических технологий к требованиям № 572-ФЗ, основные положения которого вступили в силу в 2024 году. Увеличилось количество аппаратных и программных продуктов, работающих в соответствии с данным ФЗ. Также наблюдалось увеличение количества аккредитованных коммерческих биометрических систем (КБС). Кроме этого, расширилось число сервисов, доступных по биометрии с помощью Единой Биометрической Системы. Основным «двигателем» изменений является Центр Биометрических Технологий (оператор Единой Биометрической Системы — ГИС ЕБС).

На современном этапе развития технологий можно выделить следующие реализованные решения в сфере биометрии на 2025 год:

- оплата биометрией («улыбкой»);
- проход в метро (помимо Москвы, например, запущено в Екатеринбурге, Новосибирске);
- идентификация нерезидентов при оформлении сим-карты;
- сдача биометрии иностранцами при въезде через пункты пропуска в аэропортах.

В 2025 году начались пилотные проекты с применением лицевой биометрии:

- сервис МИГОМ (без предъявления документов, по лицу):
  - > регистрация на рейс, предполетные проверки;
  - > посадка на ж/д поезда;
  - > заселение в гостиницы;
  - > регистрация на стойках самообслуживания в МФЦ;
  - > подтверждение возраста при покупке товаров 18+;
- программа обязательной регистрации домашних животных по биометрии начала действовать в Ленинградской области с 1 января 2025 года.

Государство активно продвигает биометрию через законотворчество. Например, биометрия для микрозаймов в России становится обязательной с 1 марта 2026 года для дистанционного оформления. По результатам анализа текущей ситуации и оценки тенденций развития можно составить прогноз, согласно которому в 2026 году можно будет наблюдать:

- увеличение использования биометрии во всех сферах жизни;
- основным двигателем останется ЦБТ;
- новые аккредитованные КБС;
- запуск некоторых пилотов (см. выше 2025 год) в прод;
- запуск новых пилотов.

Кроме этого, обсуждаются и новые возможности, которые можно будет осуществлять при помощи биометрии:

- оформление дистанционных сделок с недвижимостью;
- проход в госучреждения и школы.

Рынок биометрических технологий ожидает анонсированное изменение № 572-ФЗ в части ст. 13, определяющей возможность использования собственных или сторонних аккредитованных коммерческих биометрических систем (КБС) для построения СКУД.

На стороне ЕБС продолжается проработка увеличения количества биометрических модальностей. Ведется проработка и для того, чтобы к имеющимся в ЕБС лицу и голосу добавить «Отпечаток ладони» и «Рисунок вен ладони».

Экспертные сервисы

Как и ранее, основным драйвером роста любых сервисов является кадровый голод, но кроме простого кадрового голода на рынке ИБ следует отметить серьезно возросший к вопросам защиты информации интерес у организаций среднего масштаба. Для них в принципе отсутствует возможность построить свой in-house SOC и обеспечить мониторинг 24x7.

Проекты нашего коммерческого центра мониторинга и реагирования Jet CSIRT растут не только в количестве, но и в объеме (среднем чеке). Зачастую речь идет уже не только о вполне стандартных услугах по мониторингу, а о полном аутсорсинге значимых функций ИБ в заказчике под ключ под эгидой SOC. SOC уже рассматривается рынком не просто как функция мониторинга, а как центральное звено, обеспечивающее функционирование различных процессов (управление уязвимостями, управление рисками, управление осведомленностью, управление требованиями, харденинг и так далее) и в целом осуществляющее развитие функции ИБ в организации.

Иными словами, происходит существенная трансформация запроса рынка. Еще лет пять назад фраза «Сделайте мне безопасность под ключ» обозначала, скорее, классический поход (обследование / проектирование / внедрение десятка подсистем / техподдержку), сейчас же она зачастую означает именно подключение к стороннему SOC, внутри услуг которого будет обеспечиваться комплексная безопасность защищаемой организации.

Если раньше к SOC подходили уже после построения комплексной системы обеспечения ИБ, то после недавней череды резонансных кибератак, поставивших пострадавших на грань выживания, SOC — это однозначно базовый набор мер ИБ, и он часто входит в первый этап повышения уровня защищенности.

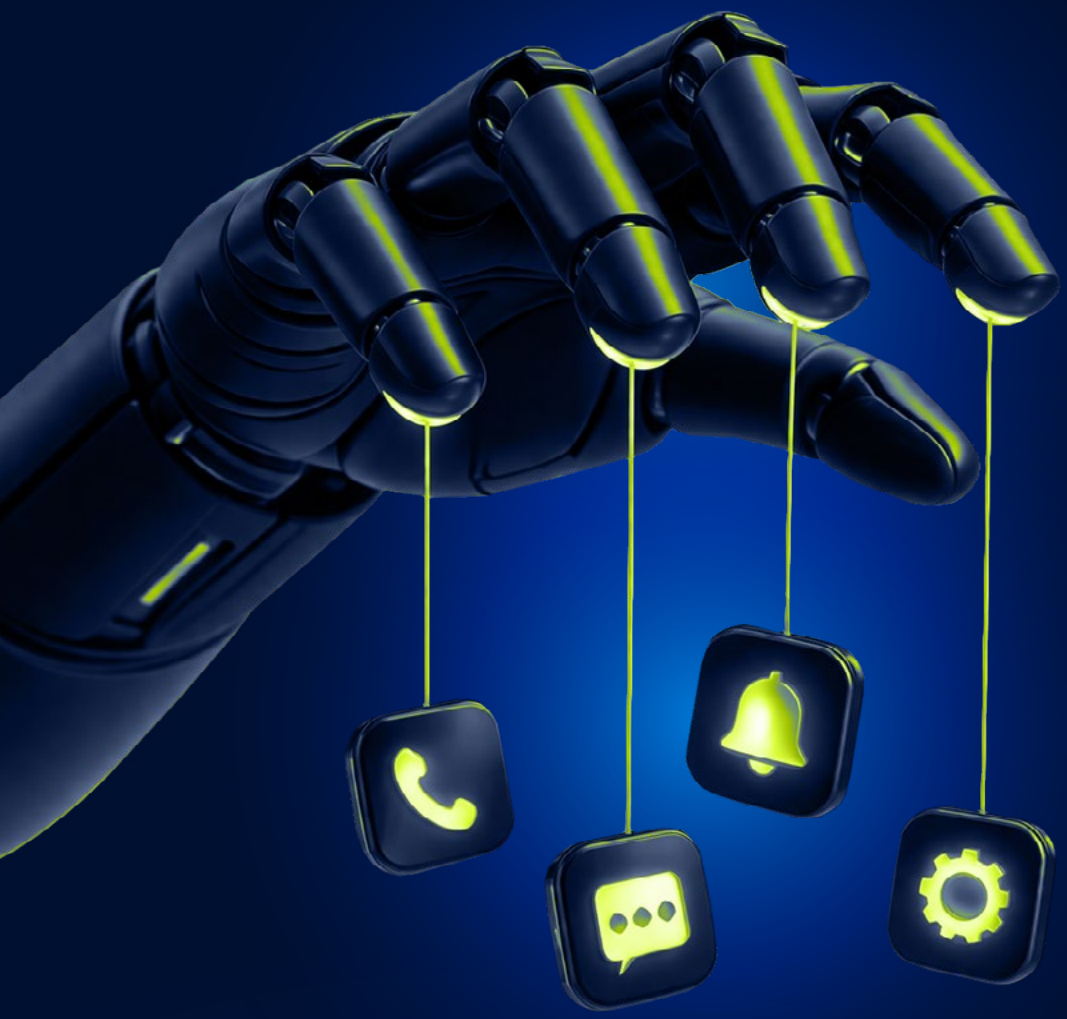
Такую тенденцию мы особо отмечаем у компаний, переживших кибератаки. Такие компании готовы подключаться к SOC-сервисам практически сразу после проведения расследования и устранения последствий.

С другой стороны, что удивительно, 2025 год стал прорывным наоборот для концепции «оптимизированных» SOC, когда вместо использования SIEM и подключения к нему значительного количества источников услуга по мониторингу и реагированию оказывается исключительно на EDR-агентах. Такая схема, безусловно, значительно более дешевая, отлично подходит организациям среднего бизнеса либо организациям, которые пока не готовы существенно инвестировать в ИБ, но хотят повысить свой уровень защищенности здесь и сейчас. Другой тенденцией можно считать запрос на гарантированность результата — все чаще подключение к SOC сопровождается серьезной юридической работой в отношении взаимных обязательств и гарантий, которые провайдер услуги предоставляет заказчику. Одним из возможных ответов на запрос гарантированности защиты может являться страхование киберрисков, интерес к которому все больше возрастает. Однако полная синхронизация подходов между игроками рынка ИБ и страховыми компаниями еще предстоит, во многом из-за традиционного скепсиса по отношению к услугам страхования у людей, которые не использовали их ранее.

Актуальным остается вопрос поддержки работоспособности все еще эксплуатируемых зарубежных средств защиты информации, в том числе — обеспечение ремонтного фонда, оперативной замены вышедшего из строя оборудования и эксплуатации в части доработки настроек и политик.

Как и в 2024 году, хорошо растут и в части выручки, и в части количества проекты по мониторингу внешних цифровых угроз и киберучениям. С ростом зрелости сервисов мониторинга внешних цифровых угроз они все больше рассматриваются заказчиками не как некая «вишенка на торте» SOC, а как его неотъемлемая часть, позволяющая команде ИБ посмотреть на свою инфраструктуру глазами злоумышленников. Аналогичное происходит и с киберучениями. Если еще два–три года назад большинство заказчиков хоть и признавали их полезность, но не были готовы тратить на них бюджеты, сейчас картина меняется в лучшую сторону.

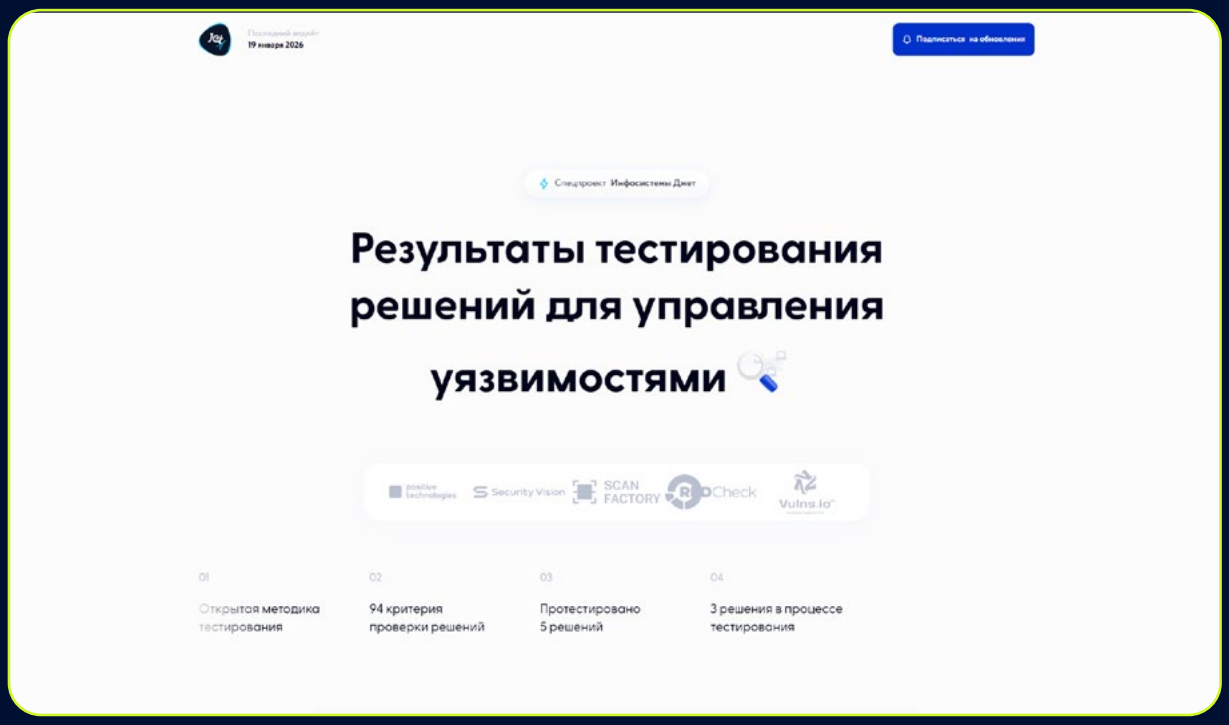
Подробнее аналитику по нашим экспертным сервисам можно прочитать в нашем исследовании «Курс на антихрупкость. Стратегический обзор киберугроз 2025».



Управление уязвимостями

Еще большее, нежели в SIEM, насыщение рынка происходит в части управления уязвимостями. Количество решений по управлению уязвимостями, которые представлены на рынке («сканер уязвимостей» — уже реже употребляемый термин), приближается к двадцати. Это с учетом размытого позиционирования некоторых из них создает в известной степени маркетинговый хаос в данном направлении.

Тем не менее, вся индустрия сходится в одном — недостаточно просто выявить уязвимости и недостатки конфигураций на конкретных хостах, необходимо обеспечить процесс их устранения. И, если в теории понятно, как это сделать, то на практике в крупных инфраструктурах эта задача крайне сложно решаемая. В итоге при выборе решений по управлению уязвимостями зачастую предпочтение отдается не решениям, показывающим лучший детект, а решениям, которые внутри себя содержат более удобную «процессную обвязку», позволяющую контролировать процесс устранения.

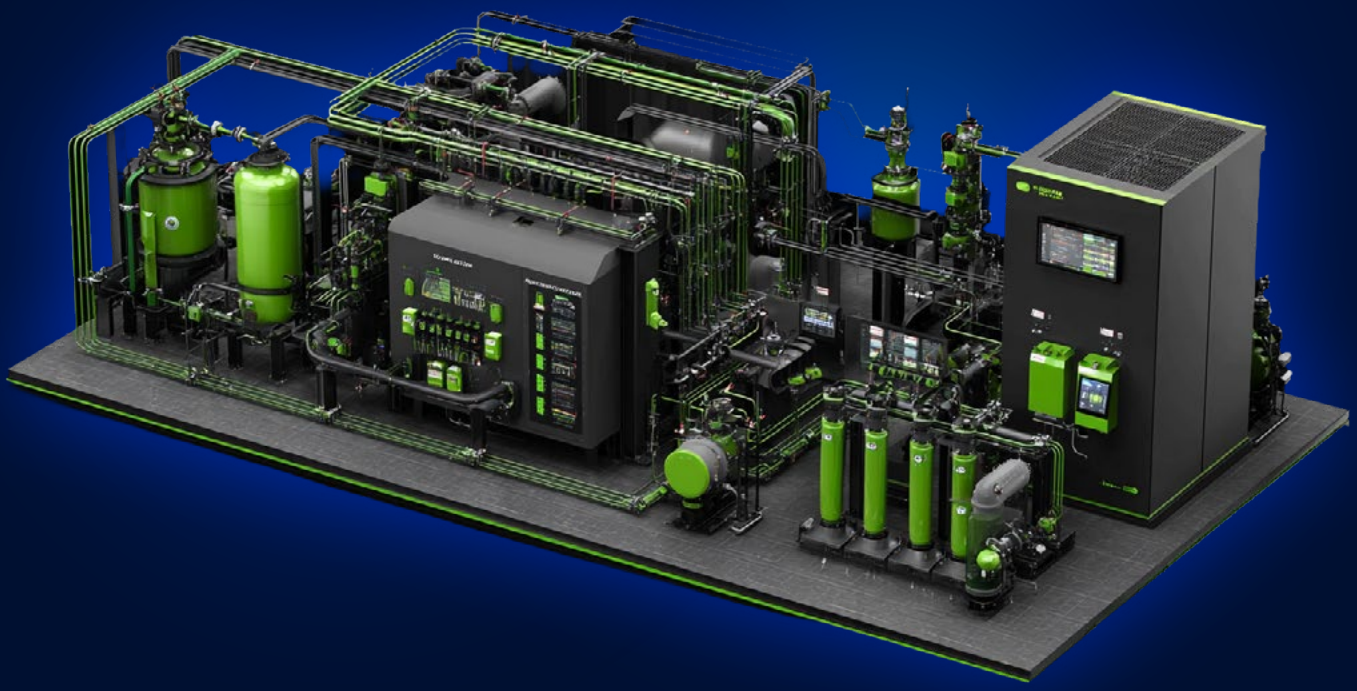


Открытый проект по публичному тестированию решений по управлению уязвимостями

Чтобы помочь с выбором VM-решений, мы создали открытый проект по публичному тестированию решений по управлению уязвимостями, в рамках которого по открытой методике проводим последовательное тестирование различных представленных на рынке продуктов.

Одним из следствий глобального тренда на взаимодействие ИТ и ИБ является крайне возросшее внимание к теме харденинга, то есть безопасной настройке элементов ИТ-инфраструктуры. Понимание того, что с накопленным за годы техническим долгом по безопасной настройке внедрение любых средств защиты если не бессмысленно, то в значительной степени неэффективно, отчетливо приходит к участникам рынка. Но так как, к сожалению, не существует решений по автоматическому харденингу ИТ-инфраструктуры, эта задача по-прежнему должна решаться вручную, что делает её крайне сложно реализуемой для хоть сколько бы то ни было крупных инфраструктур.

Прогнозируемого нами в прошлом году возрастания спроса на BAS-решения, к сожалению, пока не произошло. BAS-решения все так же остаются достаточно эксклюзивной покупкой для наиболее зрелых организаций, реализовавших значительную часть остальных подсистем ИБ.



Защита АСУ ТП

В 2025 году продолжились активное развитие данной сферы и рост интереса промышленных компаний к увеличению уровня своей защищенности. Наблюдается тренд на использование компенсирующих мер в АСУ ТП, однако их доля относительно технических мер (СрЗИ) постепенно уменьшается. Это происходит как за счет совершенствования средств защиты различных классов, так и за счет процессов импортозамещения АСУ ТП с уже встроенными механизмами безопасности.

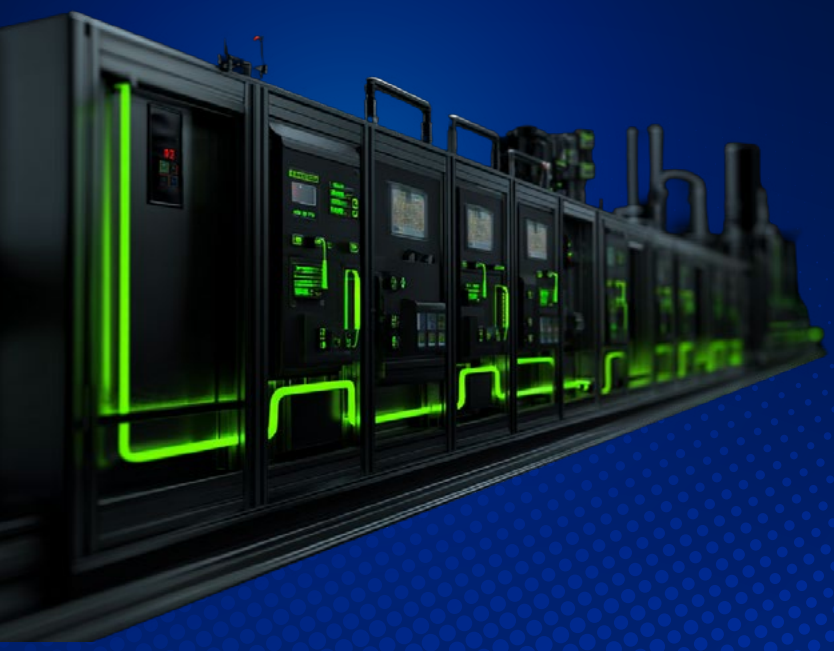
Постепенно в промышленных компаниях растет зрелость процессов ИБ АСУ ТП, а в соответствии с этим идет смещение фокуса от более простых подсистем (антивирусная защита, сегментирование сети) к более продвинутым (EDR, SIEM, PAM)

Толчком к этому служит как ужесточение законодательной базы в сфере КИИ, так и моральное устаревание использующихся западных систем автоматизации.

Отдельно стоит отметить повышение интереса к тематике защиты цепочки поставок как одного из самых эффективных способов ограничения поверхности атаки на промышленные предприятия. На это влияет и уже существующая судебная практика, когда при возникновении инцидентов на стороне подрядной организации ответственность за последствия несет конечный заказчик.

Ввиду усложнения и оптимизации условий производства на промышленных предприятиях существует огромное количество горизонтальных и вертикальных интеграций с внутренними и внешними подрядчиками, регулирующими организациями. При этом смежными могут быть не только технологические процессы, но и сетевая / вычислительная инфраструктура. В рамках аудитов промышленных предприятий до сих пор выявляются случаи, когда подрядчики имеют отдельный удаленный канал доступа напрямую через 3G-модемы, не учтенные в системе безопасности предприятия.

Для решения вопроса обеспечения защиты таких взаимодействий уже существуют общедоступные фреймворки, позволяющие разбить данную задачу на цепочку достаточно простых шагов. Но, учитывая функциональное и техническое разнообразие элементов этой инфраструктуры, принципиально сложно разработать универсальную схему взаимодействия с подрядными организациями для всех отраслей. Однако многие промышленные компании в 2025 году начали реализовывать первые шаги — инвентаризацию и ранжирование критичных подрядчиков.



Защита приложений (AppSec)

Основываясь на возросшем количестве запросов, проектов и событий в области AppSec в РФ, мы отмечаем сохранение тренда на повышенный интерес к этой области, что подтверждают прогнозы 2024 и 2025 годов. При этом факторы, способствующие росту интереса к AppSec, немного скорректировались:

- Увеличение числа взломов компаний и шифрования их инфраструктуры вынуждает рынок смотреть на ИБ комплексно, в том числе — более тщательно анализировать разрабатываемое как самостоятельно, так и с помощью подрядчиков ПО. Все больше компаний приходят к необходимости внедрения безопасной разработки в кратчайшие сроки.
- Регуляторы выпустили новые требования в области безопасной разработки:
  - > вышел Приказ ФСТЭК №117 (уже начал действовать с марта 2026 года), в котором есть явные отсылки к ГОСТ 56939-2024 о безопасной разработке;
  - > вышла новая редакция Профиля Защиты Прикладного программного обеспечения от ЦБ РФ. Основной лейтмотив обновления — синхронизация Профиля защиты с ГОСТ Р 56939-2024;
  - > в 2025 году ожидался к выходу ГОСТ по композиционному анализу, но этого не случилось. Ожидаем его в 2026 году.

- На рынке появились еще несколько SAST, DAST, SCA и ASPM-решений, теперь всего их более тридцати пяти.
- В ответ на запрос рынка о недостатке квалифицированных AppSec-специалистов сформировались сервисы по оказанию услуг в этой области — анализ кода можно осуществлять в формате аутсорса.

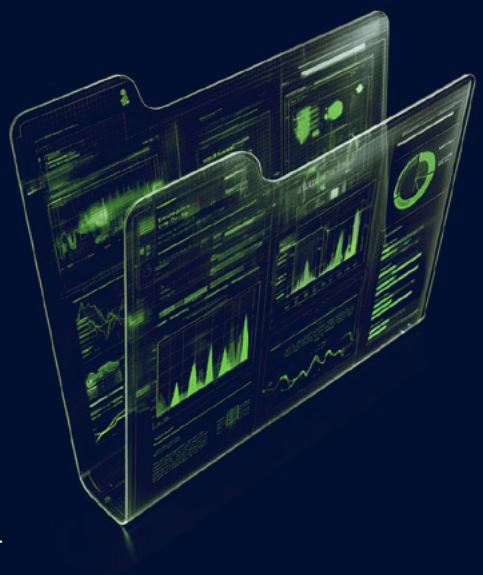
Важным трендом 2025 года отметим использование ИИ-инструментов и сервисов для анализа кода и триажа (разборов результатов анализа кода) — многие вендоры и ИИ-энтузиасты преуспели в этой области

На наш взгляд, использование общедоступных ИИ-сервисов и специально обученных нейросетей для анализа кода, триажа, формирования рекомендаций по исправлению и формирования исправлений будет приоритетным в ближайшие несколько лет. Именно использование ИИ в безопасной разработке позволит удовлетворить потребности бизнеса в части значительно увеличивающегося количества разработки ПО и крайне медленного появления новых квалифицированных Appsec-специалистов.

Появилась и новая область в AppSec — безопасная разработка и эксплуатация ИИ, MLSecOps. Всеобщий интерес к разработке, внедрению и использованию ИИ повлек за собой необходимость обеспечивать безопасность для ИИ. В этой области отметим выход огромного количества материалов в СМИ по теме MLSecOps, практически на каждой ИБ-конференции очень много внимания уделялось этой теме, в мире вышло множество фреймворков, в том числе не менее трех — в РФ (SAIMM, модель угроз от Сбера, дополнение к фреймворку DAF).

На рынке РФ появились первые рабочие инструменты в области MLSecOps, со стороны наших клиентов поступает много запросов на анализ (пентест) внедренных у них LLM и на внедрение инструментов защиты LLM (в первую очередь guardrails). Несмотря на тяжелую ситуацию на рынке вычислительных мощностей для нейросетей (в частности, видеокарт), проектами по внедрению ИИ в свои бизнес-процессы занимаются не менее половины наших крупных клиентов, что совершенно точно означает значительный рост проектов по внедрению процессов и инструментов защиты ИИ в ближайшие 2–3 года.

Антифрод



Банковская индустрия исторически занимает лидирующие позиции в разработке и внедрении передовых решений по борьбе с мошенничеством. Это обусловлено высокой стоимостью рисков и необходимостью защиты финансовых активов клиентов.

В 2025 году сохранился тренд на проникновение решений по противодействию мошенничеству в другие сферы: логистика, закупки, производство, телекоммуникации, страховые компании, электронная коммерция. Драйверами развития отмечаются потребность в сокращении издержек и автоматизация бизнес-процессов.

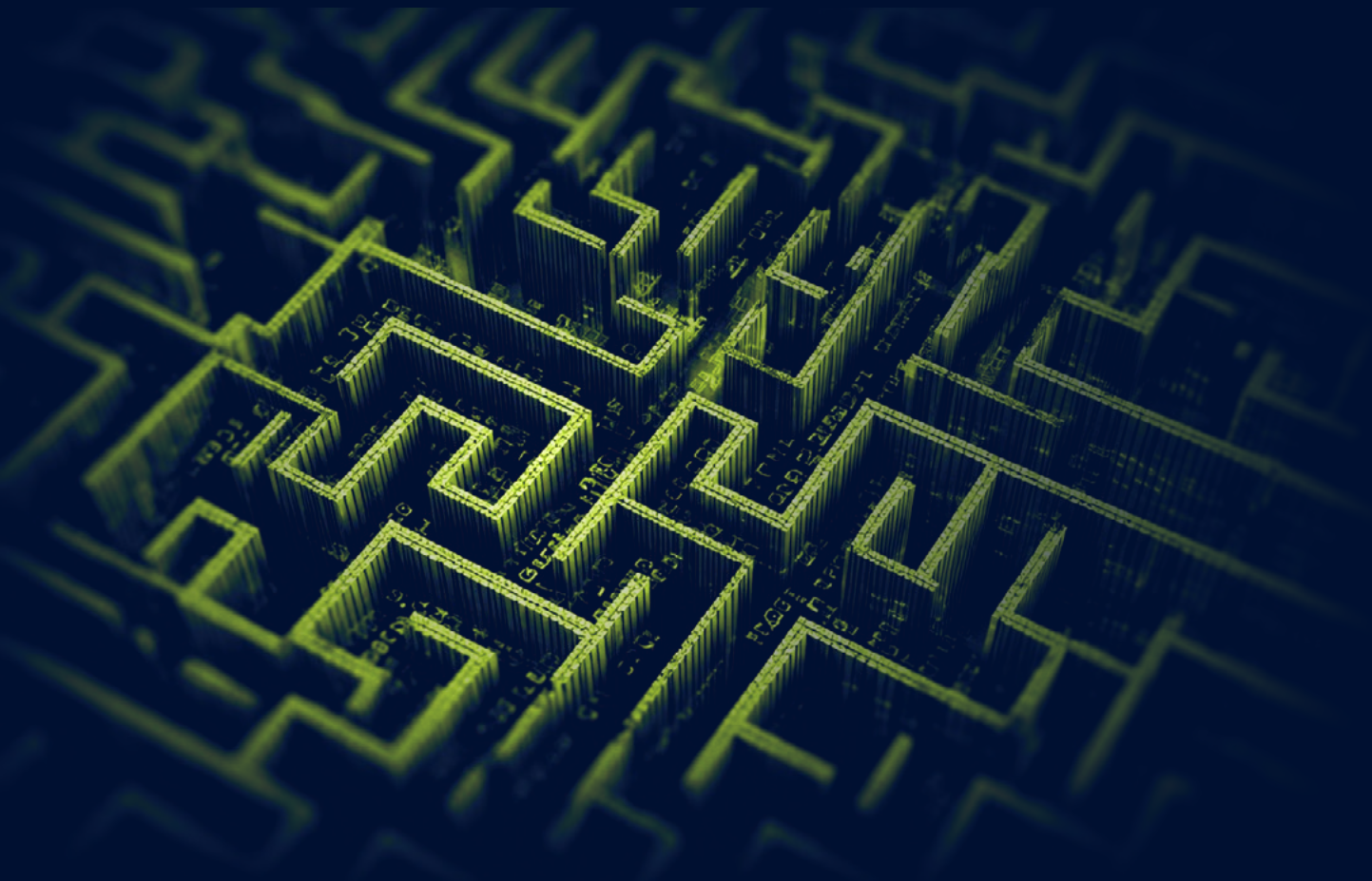
В последние годы произошел кардинальный перелом в подходе бизнеса к автоматизации процессов противодействия мошенничеству. Если еще недавно многие организации обходились либо кустарными решениями, либо вовсе полагались на ручной контроль, что было сопряжено с высокими рисками и существенными потерями, то к 2025 году ситуация значительно изменилась.

Сегодня рынок демонстрирует устойчивый рост спроса на Enterprise-платформу, а бизнес-сообщество полностью пересмотрело свое отношение к системам защиты от мошенничества. Организации больше не рассматривают внедрение таких систем как дополнительные издержки, а воспринимают их как стратегические инвестиции с быстрой окупаемостью и явной экономической эффективностью.

Такой поворот в сознании бизнеса обусловлен несколькими ключевыми факторами. Прежде всего — это взрывной рост числа мошеннических атак и связанных с ними финансовых потерь. Кроме того, значительное влияние оказало развитие технологий автоматизации и появление успешных кейсов внедрения антифрод-систем, наглядно демонстрирующих их эффективность.

К 2025 году компании активно инвестируют в комплексные решения. Внедрение современных технологий противодействия мошенничеству стало не просто желательным трендом, а необходимой мерой для сохранения конкурентоспособности и защиты бизнеса от финансовых потерь.

Этот переход к автоматизации антифрод-процессов свидетельствует о зрелости рынка и осознании бизнесом важности превентивных мер в борьбе с мошенничеством.



Криптографическая защита

Как и ранее, основной драйвер направления — импортозамещение. И если в части отечественных HSM оно идет все-таки не так быстро, как хотелось бы, то в части удостоверяющих центров под отечественные операционные системы процесс существенно ускорился в 2025 году. Несмотря на то, что в подавляющем большинстве организаций не произошла замена экосистем Microsoft, крупные организации, в большинстве своем попадающие под те или иные требования законодательства, постепенно «идут» в отечественные ОС.

Обычно это происходит методом выстраивания параллельной (к существующей Windows) экосистемы на базе российского вендора, внутри которой воспроизводится полный набор инфраструктуры и офисного прикладного ПО. Для функционирования такого импортозамещенного «острова» сразу встает необходимость наличия корпоративного центра сертификации взамен Microsoft Certificate Authority (MS CA). Другим драйвером, хоть и характерным только для финансовой сферы, являются проекты по цифровому рублю.

В 2025-м году мы фиксировали кратный рост пилотных проектов и даже пилотных внедрений отечественных продуктов на небольшой внутренний контур, на котором происходила отладка эксплуатационных процессов, а в будущем прогнозируем и увеличение таких проектов, и масштабирование уже реализованных.

Защита данных

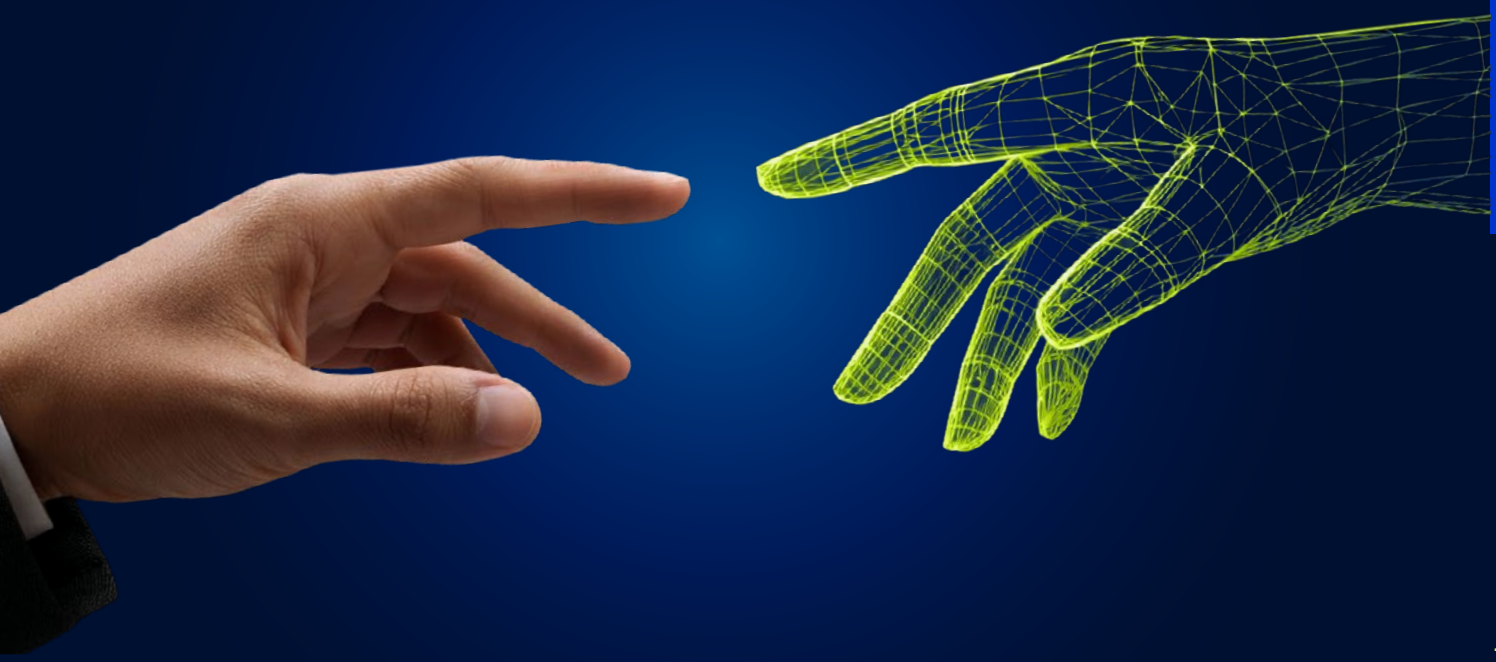
Направление, показавшее у нас наибольший спад в 2025 году. Трудно определить какую-то единую причину для этого, однако вопросы, связанные с защитой данных при их хранении и передаче (не включая средства защиты каналов связи), пользуются значительно меньшим интересом, нежели остальные направления ИБ.

Предполагаем, что это связано со значительной фактической разницей между финансовыми потерями от внешних компьютерных атак (шифровальщики и вайперы) и от инсайдерских атак (утечки данных). Безусловно, большинство организаций обеспокоены утечками и традиционно закрывают этот вопрос путем внедрения DLP-систем, но уровень финансирования и вообще внимания к проектам, связанным с защитой от инсайдеров, существо ниже, чем к проектам по защите от внешних атакующих.

Тем не менее, направление, конечно, чрезвычайно важное для комплексного обеспечения информационной безопасности, продолжает развиваться. Выходят новые продукты, развиваются комплексные подходы к защите от утечек, комбинирующие в себе не просто контроль почтового и веб-трафика, но и контроль данных при хранении (DCAP), защиту от съемки экрана (маркирование), контроль голосового трафика.

Интересным развитием направления является необходимость контроля над передаваемой в большие языковые модели (LLM) внутренней информацией. Повсеместное внедрение различных помощников, реализованных на базе внешних LLM, приводит к новому, неконтролируемому каналу утечки. Мы фиксируем значительный интерес к данной тематике, который пока имеет пилотный характер, но в горизонте 2026–2027 годов должен привести к росту количества проектов по теме защиты от утечек.

Другой, пока еще нераскрывшийся, драйвер для защиты от утечек — это оборотные штрафы за утечку персональных данных. Насколько сильное влияние на рынок он окажет, мы увидим в будущем.



Консалтинг

В 2025 году наблюдалось небольшое падение спроса на консалтинговые проекты. Отмечается перераспределение фокуса на проекты, связанные с проверкой киберустойчивости: резонансные атаки на крупнейшие российские компании и рост атак, направленных на шифрование и разрушение ИТ-инфраструктуры, продемонстрировали уязвимость даже зрелых компаний. На этом фоне значительно проявился тренд прошлого года — на усиление киберустойчивости и на её независимую оценку.

Фокус сместился с вопроса «Взломают или не взломают» на оценку способности компании сохранить операционную устойчивость в случае инцидента — «Сможем ли мы выжить, если нас взломают».

Регулярная независимая оценка уровня киберустойчивости является ключевым фактором реальной готовности к кибератакам. В связи с этим в число самых востребованных услуг вошли кибериспытания, позволяющие на практике проверить реальную эффективность системы защиты. Подход к проведению этих работ изменяется относительно классических пентестов — вместо поиска максимального количества уязвимостей компании хотят получить анализ действительно критичных сценариев, ведущих к полной остановке бизнеса, утечке персональных данных, ощутимого влияния на ключевые бизнес-процессы и так далее.

Регулярная независимая оценка уровня киберустойчивости является ключевым фактором реальной готовности к кибератакам

Одновременно растет спрос на проекты по обеспечению непрерывности бизнеса. Это направление поддерживает тренд, направленный на подготовку компаний к последствиям разрушительных кибератак. Компании все чаще интересуются практическими задачами: оценкой противодействия вирусам-шифровальщикам, безопасностью систем резервного копирования и способностью команды действовать в кризисной ситуации. Все больше организаций системно и зрело подходят к определению критичности информационных систем, что закономерно повышает спрос на проведение BIA как одного из наиболее точных инструментов такой оценки. В рамках услуг по непрерывности бизнеса наибольшей популярностью пользуются table-top (настольные тестирования реагирования на инциденты, например, распространение шифровальщика в инфраструктуре компании), позволяющие смоделировать и прожить кризис в спокойной обстановке и без реальных последствий.

Традиционно высоким остается спрос на услуги оценки соответствия требованиям законодательства и отраслевых стандартов (compliance). Наибольшей популярностью пользуются услуги по обеспечению соответствия требованиям ЦБ РФ и требованиям в области КИИ. При этом проекты по приведению в соответствие требованиям 152-ФЗ «О персональных данных» оказались менее востребованными, чем ожидалось. Ужесточение ответственности за утечки персональных данных повысило приоритет практических мер: внедрение специализированных средств защиты, повышение осведомленности, проведение пентестов и другое. Дополнительными сдерживающими факторами стали отсутствие сформировавшейся правоприменительной практики, а также механизм применения оборотных штрафов: значимые санкции предусмотрены лишь при повторной утечке.

JET

SECURITY
TEAM

security@jet.su
jetcsirt.su