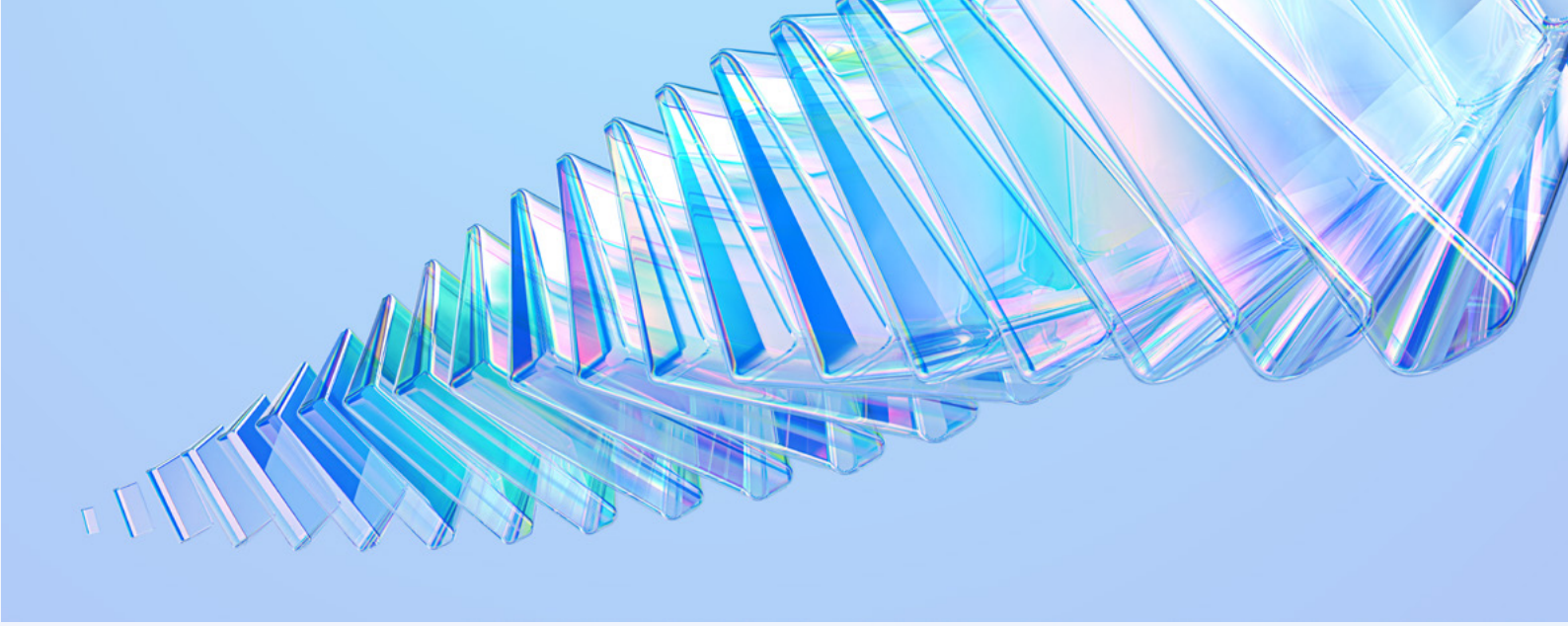
JET
SECURITY
TEAM

ОБЗОР РЫНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗА 2024

Инфосистемы Джет
JET.SU



ВВЕДЕНИЕ

Как и многие другие сферы, рынок информационной безопасности подвергся существенной трансформации за последние три года. Если 2022 год и начало 2023-го были временем «тушения пожаров» — спешным импортозамещением в тех областях, где это было возможно, — то начиная со второй половины 2023 года рынок перестроился и перешел к более системному, осмысленному подходу.

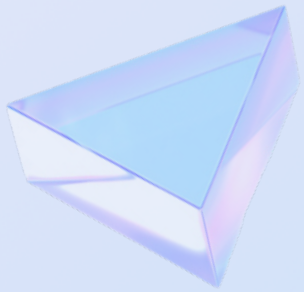
Накопив статистику по реализованным нами проектам за 2023 и 2024 годы, мы подготовили обзор рынка, чтобы показать, какие направления информационной безопасности пользуются наибольшим спросом, а также продемонстрировать динамику этого спроса.

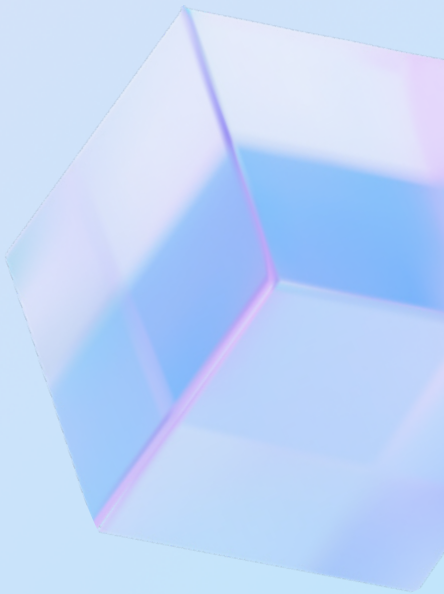
Глобальный тренд, который мы фиксируем на рынке, заключается в явном желании организаций реализовать у себя систему обеспечения ИБ, внедренную «не для галочки», а обеспечивающую реальную защищенность бизнес-процессов. Первоочередной становится задача обеспечения непрерывности бизнеса. Тенденция сохраняется с 2010-х, однако разница между периодами 2019–2021 и 2023–2024 годов существенная.

Обозначим ключевые особенности рынка ИБ в текущий момент.

- Возрастающая вовлеченность топ-менеджмента организаций в вопросы ИБ, осведомленность СМИ и коллег о возможных катастрофических последствиях кибератак.
- Увеличивающаяся доля расходов на ИБ, рост влияния подразделений ИБ на жизнь организаций.
- Более тесная кооперация между ИТ-подразделениями и ИБ.
- Смена парадигмы с «если нас взломают» на «когда нас взломают», рост внимания к построению работающего мониторинга ИБ, разработка планов реагирования.
- Нацеленность на результат в проектах, повышение требований со стороны заказчиков и к самим решениям, и к сопутствующим работам по внедрению и эксплуатации.

- Усложнение процесса выбора технических решений. Более тщательные пилотные тестирования и сравнение имеющихся на рынке альтернатив.
- Качественное развитие отечественных средств защиты информации и взрывной рост их числа.
- Значительное увеличение спроса на различные сервисы ИБ вследствие кадрового голода и необходимости оперативно усилить защищенность.
- Рост интереса к киберразведке, проверке подрядчиков и другим методам защиты вне ИТ-периметра.
- Устойчивое проникновение технологий машинного обучения в сферу ИБ — как в составные части вендорских решений, так и в операционную деятельность отдельных специалистов (использование больших языковых моделей для выполнения рутинных задач).

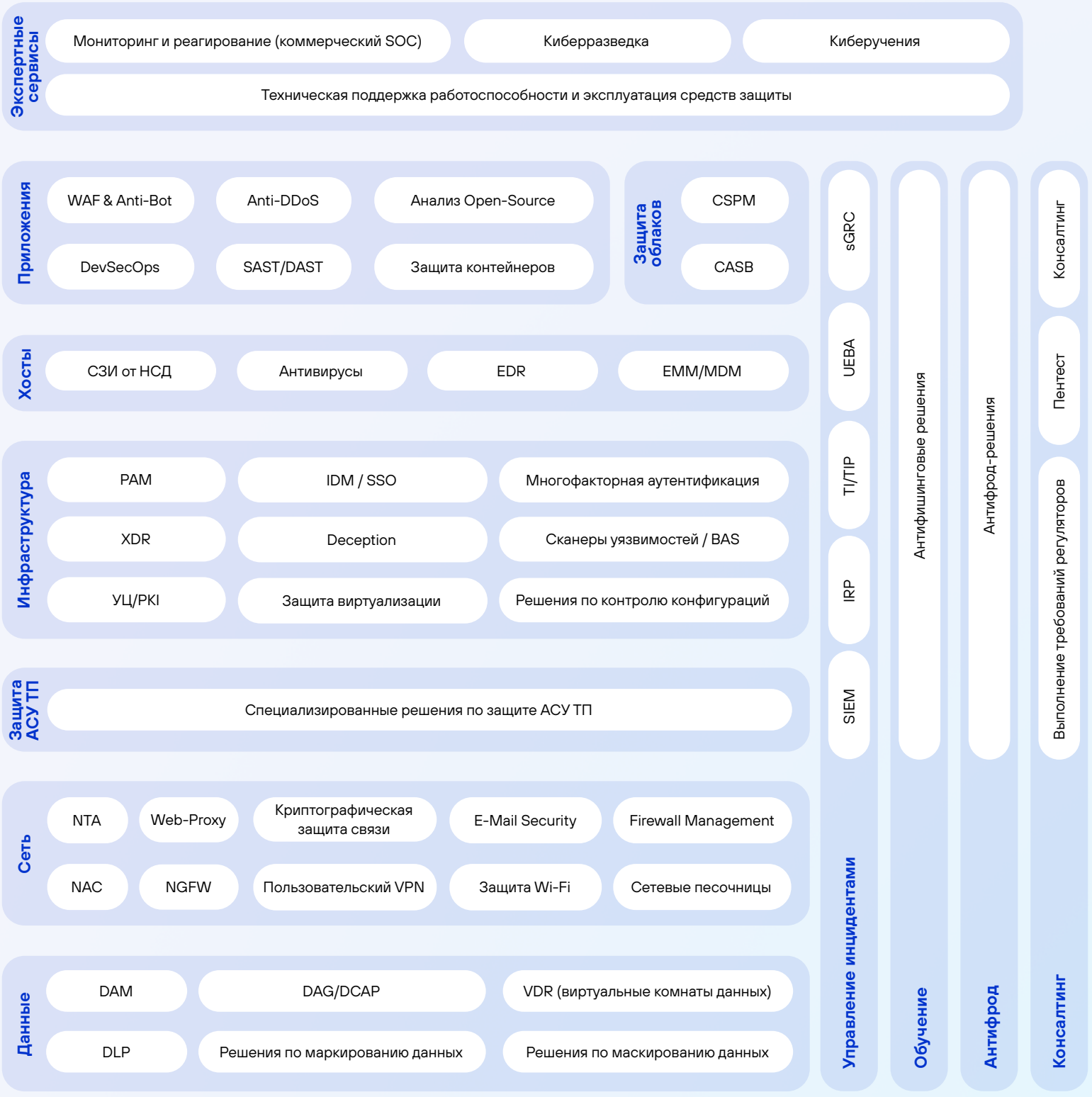




МЕТОДИКА СОСТАВЛЕНИЯ ОБЗОРА

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 обзора мы предлагаем ориентироваться на следующий ландшафт средств защиты информации и связанных с ними сервисов:


Экспертные сервисы
Мониторинг и реагирование (коммерческий SOC)
Киберразведка
Киберучения
Техническая поддержка работоспособности и эксплуатация средств защиты
Приложения
WAF & Anti-Bot
Anti-DDoS
Анализ Open-Source
DevSecOps
SAST/DAST
Защита контейнеров
Защита облаков
CSPM
CASB
Хосты
СЗИ от НСД
Антивирусы
EDR
EMM/MDM
Инфраструктура
PAM
IDM / SSO
Многофакторная аутентификация
XDR
Deception
Сканеры уязвимостей / BAS
УЦ/PKI
Защита виртуализации
Решения по контролю конфигураций
Защита АСУ ТП
Специализированные решения по защите АСУ ТП
Сеть
NTA
Web-Proxy
Криптографическая защита связи
E-Mail Security
Firewall Management
NAC
NGFW
Пользовательский VPN
Защита Wi-Fi
Сетевые песочницы
Данные
DAM
DAG/DCAP
VDR (виртуальные комнаты данных)
DLP
Решения по маркированию данных
Решения по маскированию данных
Управление инцидентами
sGRC
UEBA
TI/TIP
IRP
SIEM
Обучение
Антифишинговые решения
Антифрод
Антифрод-решения
Консалтинг
Консалтинг
Пентест
Выполнение требований регуляторов

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

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

Направление	Подсистемы
Сетевая безопасность	NGFW, криптографическая защита каналов связи, NAC[1], NTA[2], Web Proxy, Firewall Management[3], 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[4], SOAR[5], TI[6]/TIP, sGRC[7]
Защита от вредоносного кода и целенаправленных атак	Сетевые песочницы, EDR[8], XDR, антиспам, антивирусы, СЗИ от НСД, Deception Tools[9], решения по защите виртуализации, EMM[10]

[1] **NAC (Network Access Control)** — Комплексный контроль доступа к сети. Включает безопасный доступ к бизнес-данным на основе контекста, оптимизированный гостевой доступ, самостоятельную регистрацию устройств пользователей в сети, автоматическую проверку соответствия подключаемых устройств политикам безопасности.

[2] **NTA (Network Traffic Analysis)** — Системы анализа сетевого трафика для выявления атак на периметре и внутри сети. Также применяется при расследовании инцидентов ИБ и выявлении нарушения регламентов ИБ.

[3] **Firewall Management** — Системы управления межсетевыми экранами, позволяющие реализовать единую точку контроля изменений в сетевой инфраструктуре, а также автоматизировать ресурсоемкие процессы внесения изменений в конфигурации.

[4] **SIEM (Security Information and Event Management)** — Система, предназначенная для мониторинга и анализа событий из ИТ- и ИБ-систем, анализа событий по действиям пользователей и оперативного информирования об инцидентах ИБ.

[5] **SOAR (Security Orchestration and Response)** — Решения по выстраиванию workflow по обработке инцидентов ИБ; автоматизация реагирования на инциденты; контроль исполнения задач в рамках реагирования и оперативное получение отчетов.

[6] **TI (Threat Intelligence)** — Оперативное детектирование инцидентов ИБ за счет использования данных киберразведки, управление данными киберразведки, ретроспективный поиск угроз и оперативное реагирование на инциденты ИБ.

[7] **sGRC (Security Governance, Risk Management and Compliance)** — Системы автоматизации разных процессов ИБ. Учет активов, связь активов и процессов, автоматизация процесса управления рисками. Отслеживание выполнения требований законодательства.

[8] **EDR (Endpoint Detection and Response)** — Продвинутая (по сравнению с антивирусом) защита конечных станций. Включает анализ поведения рабочей станции, обнаружение бесфайловых атак, инструменты для проведения расследований и карантин скомпрометированного девайса.

[9] **Deception Tools** — Использование техник активного обмана атакующих с применением специализированных ловушек, приманок и других методов дезинформации.

[10] **EMM (Enterprise Mobile Management)** — Решения, позволяющие защищать мобильные устройства — смартфоны, планшеты, ноутбуки — и централизованно ими управлять. Включают механизмы для непосредственной защиты и механизмы, упрощающие доступ к корпоративным приложениям.

Управление доступом	IdM, многофакторная аутентификация[1], VDR[2], PIM[3], менеджеры паролей
Защита данных	DLP[4], решение по маркированию данных, DCAP[5], решения по маскированию данных, DAM[6]
Защита приложений (AppSec)	WAF[7], Anti-DDoS[8], проекты по DevSecOps
Управление уязвимостями	VM, контроль конфигурации[9], BAS
Консалтинг	Проекты по выполнению требований законодательства (не включая стоимости необходимых решений), а также по пентестам и экспертному консалтингу
Экспертные сервисы	Услуги коммерческого SOC[10] (Jet CSIRT), проекты по киберразведке, киберкриминалистике и киберучениям. Услуги по оказанию технической поддержки и поддержанию работоспособности СЗИ (не включая стоимости вендорской поддержки и продлений)
Криптографическая защита	УЦ/PKI[11], СКЗИ (не включая криптошлюзы)

[1] **Многофакторная аутентификация** — усиление защиты систем с помощью нескольких факторов аутентификации, снижение риска несанкционированного доступа к корпоративным системам, защита от социальной инженерии (фишинга).

[2] **VDR(Virtual Data Room)** — виртуальные комнаты данных. Корпоративные системы для безопасного обмена «большими» файлами как между работниками организации, так и с третьими лицами.

[3] **PIM Privileged Identity Management)** — решения по контролю действий пользователей с повышенными правами, обеспечивают подотчетность действий привилегированных пользователей и подрядчиков.

[4] **DLP (Data Loss Prevention)** — классическое ядро комплекса защиты информации от утечек. Включает решения, позволяющие контролировать каналы передачи информации, обнаруживать защищаемую информацию по ее содержимому и блокировать утечки.

[5] **DCAP (Data-Centric Audit and Protection)** — решения, позволяющие анализировать большие объемы неструктурированных данных при хранении на файловых ресурсах. Включают аудит и анализ прав доступа, аудит файловых хранилищ, классификацию данных и поведенческую аналитику при доступе к данным.

[6] **DAM (Database Activity Monitoring)** — защита систем управления базами данных (СУБД) от несанкционированного доступа, защита от атак на СУБД, контроль доступа к СУБД со стороны администраторов, обеспечение соответствия требованиям регуляторов.

[7] **WAF (Web Application Firewall)** — решения по обеспечению защиты веб-приложений от атак прикладного уровня, противодействие злонамеренной активности бот-сетей, защита от DDoS-атак и оперативное блокирование уязвимостей.

[8] **Anti-DDoS** — Решения по своевременному обнаружению DDoS-атак на ИТ-ресурсы и фильтрация вредоносного трафика.

[9] **Контроль целостности** — контроль неизменности конфигурационных, системных, исполняемых и других файлов операционной системы.

[10] **SOC (Security Operation Center)** — центр мониторинга и реагирования на инциденты ИБ. Люди, процессы и технологии, обеспечивающие мониторинг событий ИБ в режиме реального времени и оперативное реагирование на инциденты.

[11] **PKI (Public Key Infrastructure)** — набор служб и сервисов для издания, хранения, проверки, приостановки действия, обновления и отзыва цифрового сертификата открытого ключа подписи.

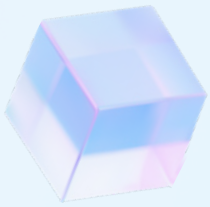
Благодаря подобному группированию можно сразу определить, к какому классу решений отнести тот или иной продукт. Например, полноценное NGFW-решение в конкретном проекте может быть использовано под задачу проксирования пользовательского трафика и применяться только для этой цели. Соответственно, проект формально 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 специализированные 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 этому направлению. Мы применяли «широкий» подход.

Чтобы снизить объем искажений статистики, мы исключили из расчетов 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.

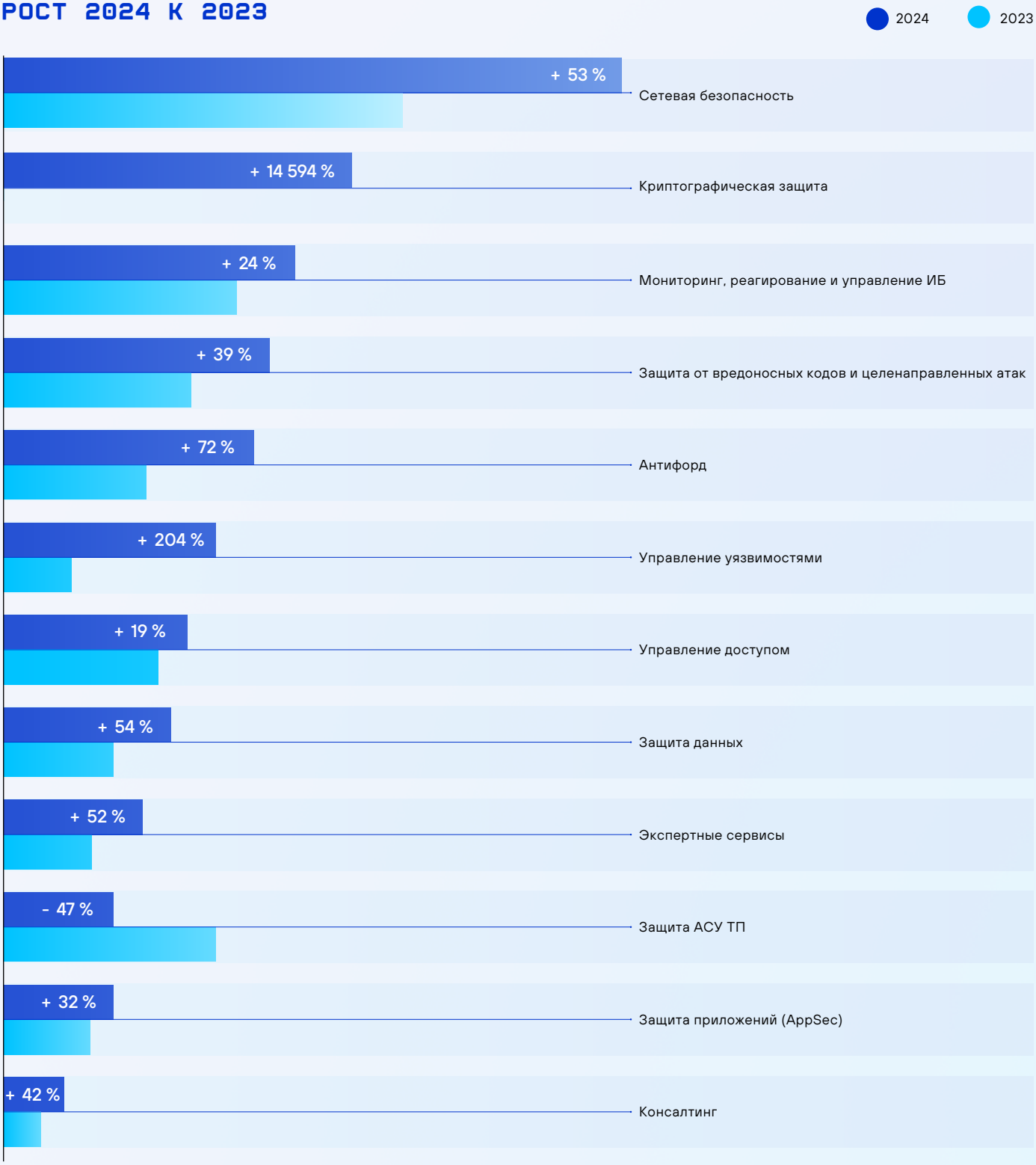
- В 2023 году «Инфосистемы Джет» реализовала 795 проектов по информационной безопасности, в 2024-м — 970.
- Мы относили проекты к одному или нескольким направлениям информационной безопасности, исходя из реализованных решений. Далее направления сравнивались по совокупной выручке.
- Проекты рассматривались в целом, включая стоимость лицензии и оборудования, а также ассоциированных с ним интеграционных, консалтинговых и аналитических работ.
- Для проектов, в которых реализовывались комплексные системы обеспечения ИБ, была выделена доля выручки для каждого из направлений.
- Проекты по проектированию или настройке соответствующих подсистем также относились к ним и отдельно не выделялись.



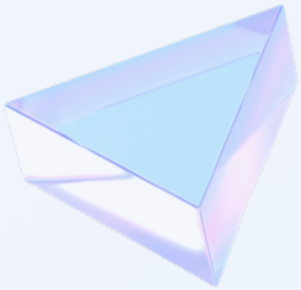
СТРУКТУРА РЫНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Совокупный рост нашей выручки по проектам в области информационной безопасности составил 43% — с 14,295 млрд руб. в 2023 году до 20,472 млрд руб. в 2024 году. При этом финансовые показатели направлений менялись по-разному.

РОСТ 2024 К 2023



- **Сетевая безопасность.** Самое крупное направление на рынке, показывающее устойчивый рост. В первую очередь, это связано с импортозамещением зарубежных NGFW. Особенно актуально для сегмента крупного enterprise. Несмотря на большое количество российских решений (не всегда, правда, достаточно зрелых) и требования законодательства, значительное количество организаций еще только планируют миграцию.



- **Криптографическая защита.** Беспрецедентный рост и в абсолютных, и в относительных цифрах обусловлен эффектом низкой базы 2023 года. Как и в случае с сетевой безопасностью, основной интерес рынка сейчас состоит в импортозамещении зарубежных HSM на отечественные аналоги. Также прогнозируется существенный рост спроса на корпоративные центры сертификации под Linux в связи с использованием отечественных Linux-систем.

- **Мониторинг и реагирование.** Стабильно растущее направление, рост которого обусловлен запросом на реальную безопасность. Особенностью и 2023-го, и 2024-го является постоянное увеличение доли и сложности интеграционных работ в проектах. Рынок становится более требовательным к настройкам SIEM и SOAR, к реализации в ходе проектов глубоких и сложных логик обнаружения и реагирования, релевантных актуальным техникам и тактикам злоумышленников.

- **Защита от вредоносных кодов и целенаправленных атак.** Направление, которое в свое время в меньшей степени требовало импортозамещения за счет наличия зрелых и широко распространенных российских решений. Стабильный рост обеспечивается общим ростом рынка ИБ и актуальностью задачи защиты от вирусов-шифровальщиков.

- **Антифрод.** Направление, связанное с непосредственной защитой от финансовых убытков, сейчас переживает бурный рост. Традиционные для финансовой отрасли антифрод-решения все чаще начинают использовать в других отраслях.

- **Управление уязвимостями.** Классическое направление в информационной безопасности, переживающее ренессанс. Мы фиксируем всплеск интереса, вызванный желанием обеспечить реальную защищенность инфраструктур как с точки зрения отсутствия программных уязвимостей, так и сточки зрения безопасной настройки (харденинг).

Недостаточно просто проводить сканирования на наличие уязвимостей, требование рынка — выстраивание процесса управления уязвимостями, инвентаризация ИТ-активов, патч-менеджмент и сквозная интеграция с SOC. Решения по контролю конфигураций, которые ранее внедрялись в основном для соответствия требованиям регуляторов, теперь рассматриваются как неотъемлемый элемент комплексной системы обеспечения ИБ. Зарубежные сканеры уязвимостей были замещены практически сразу, так как без обновлений они фактически не работают. В 2024-м рынок снова оживился в связи с выходом нескольких новых отечественных продуктов и необходимостью замены MaxPatrol 8 на актуальную версию сканера или аналог.

- **Управление доступом.** Направление, проекты в рамках которого связаны с изменениями в ИТ-ландшафте организации, а также с эксплуатационными процессами. Драйвером роста являются комплексные проекты по внедрению масштабных IdM-систем с разработкой регламентов доступа и ролевых моделей для бизнес-систем.

- **Защита данных.** Несмотря на то, что в медийном поле первоочередная задача ИБ определяется как противодействие внешним злоумышленникам, защита от инсайдеров и случайных сливов информации остается актуальной для рынка. Основным драйвером роста является управление неструктурированными данными (DCAP).

- **Защита АСУ ТП.** Единственное направление, не показавшее роста вопреки ожиданиям и прошлым прогнозам. Обусловлено это скорее не падением интереса рынка, а особенностью самих проектов (большая длительность, когда только проектирование может длиться год). В 2023 году мы реализовали ряд крупных проектов, включающих в себя внедрение большого количества средств защиты, а в 2024-м реализовывали проекты по проектированию и разработке рабочей документации.

- **Защита приложений.** Еще два-три года назад защита процессов разработки в рамках DevSecOps была наиболее распространена в финтехе. Сейчас же мы фиксируем повсеместный (вне зависимости от отрасли) спрос на подобные проекты. Идея об обязательном включении ИБ на каждом этапе разработки ПО все чаще идет от самой разработки или бизнес-владельцев разрабатываемых систем.

- **Экспертные сервисы.** Один из лидеров роста, выросший во всех своих составляющих. В первую очередь, в услугах коммерческого центра мониторинга и реагирования Jet CSIRT. Все больше организаций приходят к тому, что SOC является абсолютно необходимым элементом системы обеспечения ИБ. Также следует отметить кратный рост запросов и проектов по киберразведке и киберучениям. В абсолютных цифрах направление не выглядит большим на общем фоне — это связано с отсутствием в его составе поставок СЗИ, а не с числом или масштабом проектов.

- **Консалтинг.** Традиционное направление, включающее в себя всевозможные аудиты, пентесты, а также разработку планов по развитию функции ИБ. Мы отмечаем изменение запроса рынка в этой части с проведения работ «для галочки», для выполнения внутренних требований или требований законодательства на осознанный запрос, когда с помощью консалтинга организация хочет решить конкретные проблемы и детально спланировать развитие функции ИБ.

СЕТЕВАЯ БЕЗОПАСНОСТЬ

После ухода зарубежных вендоров с российского рынка спрос на отечественные NGFW существенно превысил предложение, что привело к появлению новых решений и серьезной конкуренции среди российских производителей. Потребности бизнеса выстраивать новые и масштабировать существующие инфраструктуры с использованием поддерживаемых вендорами решений сильно повлияли на рост рынка сетевой безопасности.

Чтобы помочь с выбором оптимального NGFW, в 2024 году мы запустили независимое тестирование представленных на российском рынке решений в собственной лаборатории «Инфосистемы Джет». Мы стремились дать наиболее полное представление о доступных в России решениях класса NGFW, их функциональных возможностях и реальной производительности. Тестирования производились по единой методологии, в формате vendor-agnostic в условиях, максимально приближенных к реальным. Нами были протестированы Check Point R81.20, Ideco NGFW v16, InfoWatch ARMA Стена (NGFW), UserGate 7.1.0 RC, ViPNet Coordinator HW5 5.3, Континент 4.1.7 и 4.1.9, решение китайского производителя (7000 series, v.8.0).

Ключевые вендоры 2024

UserGate

CHECK POINT

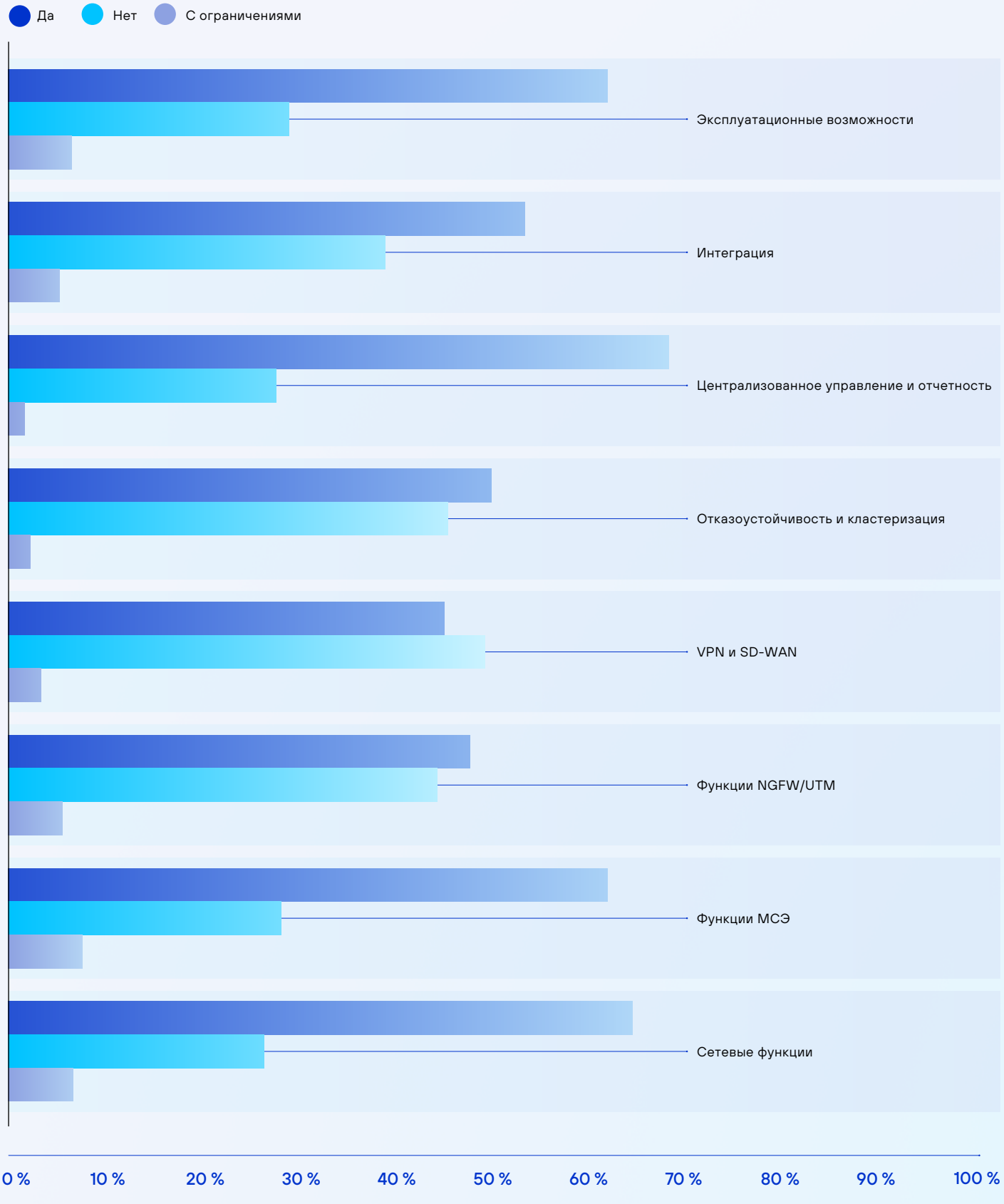
КОД безопасности

positive technologies

AxeL pro

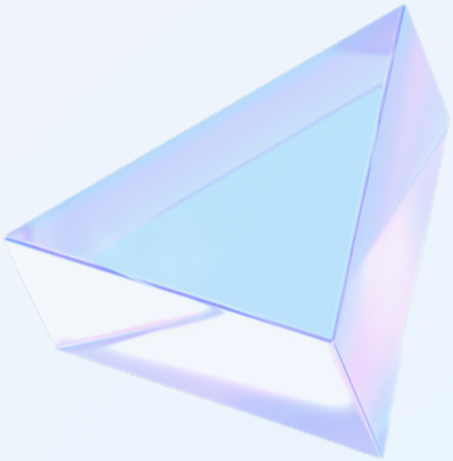
Совокупные результаты функционального тестирования российских решений представлены на графике:

Процент выполнения группы функционала российскими решениями



Исходя из результатов тестов российские NGFW-решения демонстрируют максимальные показатели выполнения для функций централизованного управления и отчетности, сетевых функций и эксплуатационных возможностей. К блоку функционала, который в среднем меньше всего реализован, относятся функции VPN и SD-WAN.

Что касается производительности устройств, то существующие аппаратные платформы не выдерживают требований, выдвигаемых бизнесом, поэтому в 2024 году мы наблюдали гонку за производительностью среди вендоров. Новые игроки, ранее не занимавшиеся сегментом NGFW, презентуют высокопроизводительные решения сразу, а традиционные вендоры начинают добавлять в линейку высокопроизводительные платформы. В рамках нагрузочного тестирования, при котором мы сравнивали заявленные вендором параметры производительности с фактическими (полученными в лаборатории «Инфосистемы Джет») данными, для большинства протестированных решений мы получили сопоставимые результаты. Это стало для нас некоторой неожиданностью, потому что западные вендоры традиционно довольно сильно завышали в документации производительность своих решений.



В 2025 году бурное развитие решений NGFW и борьба производителей продолжатся. С 1 января вступил в силу указ Президента РФ №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», который подразумевает запрет на использование средств защиты информации, «странами происхождения которых являются недружественные иностранные государства», при этом не все организации успели перейти на отечественные аналоги. К тому же помимо импортозамещения есть задачи по созданию новых и масштабированию существующих инфраструктур, для которых также необходимо подобрать надежное и соответствующее требованиям бизнеса решение NGFW.

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

Беспрецедентный рост в абсолютных и относительных цифрах, который показало это направление в нашей статистике, обусловлен процессами импортозамещения. В первую очередь, это импортозамещение платежных HSM.

До 2022 года рынок платежных HSM в России практически полностью занимали зарубежные решения — в основном решения компании Thales. Сложилась ситуация, при которой, с одной стороны, импортозамещение в данной области является обязательным в силу важнейшей роли платежных HSM в бесперебойном функционировании платежных операций по банковским картам, а, с другой стороны, не первоочередным, ведь с уходом вендора из России внедренные HSM не потеряли в своей функциональности. В 2023 году банки только присматривались к отечественным решениям и не инициировали проекты по миграции, однако со второй половины 2024 года мы фиксируем интерес к теме, который будет расти в 2025-м.

Другими важными элементами ИТ-инфраструктуры, требующими импортозамещения, являются корпоративные центры сертификации, которые обеспечивают работоспособность ИТ-инфраструктуры. Ранее задача решалась с помощью Microsoft Certificate Authority (MS CA). Как и в случае с HSM, уход Microsoft из России не повлиял на функциональность MS CA, поэтому многие организации не спешили с заменой, однако здесь в силу вступает другая тенденция — постепенное импортозамещение самой операционной системы Windows как на серверах, так и на АРМ. Переход на отечественные ОС на базе Linux остро ставит вопрос поиска замены MS CA, без которой полноценная миграция не может быть эффективно реализована.

Ключевые вендоры 2024

Аладдин

КРИПТОПРО

МОНИТОРИНГ, РЕАГИРОВАНИЕ И УПРАВЛЕНИЕ ИБ

В 2024 году наблюдалось явное повышение интереса к теме TI-данных для небольших SOC и к полноценным TI-платформам в зрелых с точки зрения ИБ организациях — количество таких проектов выросло в два раза. Это кажется закономерным, ведь увеличение числа атак вынуждает применять средства проактивного обнаружения угроз ИБ.

Наряду с TI продолжает развитие и рынок SIEM-систем — появляются новые игроки, составляющие конкуренцию признанным лидерам рынка. Это расширяет возможности выбора для заказчиков по импортозамещению, которое еще не завершилось в целом по рынку.

С ростом среднего количества событий ИБ в SOC, что само по себе является трендом, мы также видим смещение фокуса с классического SOC вокруг SIEM-систем в сторону систем класса LM (Log-Manager-решений), которые позволяют эффективно агрегировать, фильтровать и хранить огромные объемы событий ИБ в течение долгого времени. Стоимость таких систем существенно ниже, чем у SIEM, но они не имеют столь развитых возможностей по корреляции и автоматическому анализу событий. Мы ожидаем рост продаж в этом направлении в 2025 году.

В части направления SOAR-систем наблюдается усложнение проектов. Это связано с тем, что заказчики чаще смотрят в сторону автоматизации процессов и реализации множества кастомных интеграций с внешними системами и СЗИ. Стремясь к автоматизации процессов ИБ (в том числе по причине дефицита кадров), выбирают SGRC-системы, которые позволяют централизованно управлять активами, аудитами и рисками ИБ.

Большинство компаний уровня Enterprise уже имеют в своей структуре SOC, но зачастую у них нет уверенности в том, что в условиях серьезного инцидента SOC сработает эффективно. Из-за этого растет количество проектов по аудиту SOC: анализ текущих процессов, оценка достаточности используемого технологического стека и корректность его настройки, RedTeam и PurpleTeam. Также велик спрос на проведение киберучений для инженеров 1-й и 2-й линий.

Ключевые вендоры 2024

kaspersky

positive technologies

R-Vision

Security Vision

ЗАЩИТА ОТ ВРЕДОНОСНОГО КОДА И ЦЕЛЕНАПРАВЛЕННЫХ АТАК

Самое стабильное из всех направлений с точки зрения ежегодного роста. Во-первых, в рамках направления традиционно широко использовались отечественные решения — соответственно, уход зарубежных вендоров не сильно повлиял на ситуацию на рынке. Во-вторых, с учетом того, что ключевой угрозой являются вирусы-шифровальщики, спрос на решения по защите от вредоносных кодов только растет.

Ключевой точкой роста здесь являются технически продвинутые решения: сетевые песочницы и EDR, использование которых стало обязательным элементом для построения комплексной системы обеспечения ИБ, эффективно противостоящей целенаправленным атакам.

Существенно развивается рынок EDR и с точки зрения функциональности имеющихся решений, и с точки зрения выхода на рынок новых игроков. EDR рассматривается не просто как источник дополнительной информации для SOC, а как полноценное средство защиты информации, на котором осуществляется и мониторинг, и непосредственное реагирование.

Стабильно растет спрос на решения класса Deception Tools, о полезности которых мы наблюдаем диаметрально противоположенные мнения на рынке. Часть наших заказчиков считает данные решения избыточными и не несущими реальной полезности, другая часть (и она растет), наоборот, рассматривает их как хоть и не первоочередную, но обязательную часть экосистемы ИБ.

Также одной из ключевых тенденций рынка является развитие вендорских экосистем, оформленных в виде единых XDR-решений, которые работают как единое целое от уровня сетевых и хостовых сенсоров до верхнеуровневой аналитики. С одной стороны, это является существенным плюсом, в том числе с точки зрения автоматизации рутинных операций, с другой стороны, ни одна из существующих экосистем не покрывает весь ландшафт необходимых средств защиты, что приводит к необходимости реализации нескольких экосистем (или их элементов) в рамках одной инфраструктуры и усложняет их интеграцию.

Ключевые вендоры 2024

kaspersky

positive technologies

F6

АНТИФРОД

Традиционно сложилось, что банковская сфера является двигателем развития направления противодействию мошенничеству. Однако в 2024 году значительный рост количества и объемов проектов случился в «небанках».

Совокупность высокого уровня автоматизации бизнес-процессов и потребности в сокращении издержек предоставила возможность многим крупным компаниям в различных отраслях подойти к задачам противодействия мошенничеству и хищениям в производстве, закупочной деятельности, логистике, складской деятельности.

Если раньше противодействие мошенничеству и хищениям в части бизнес-процессов было автоматизировано «на коленке», а по большей части не было автоматизировано вовсе, то в 2024-м мы встречаемся с большим количеством запросов на автоматизацию: многие организации стали относиться к системам противодействия мошенничеству как к быстро окупающим себя инвестициям, а не как к тратам. По нашим прогнозам, количество таких проектов вырастет в разы в ближайшие пару лет.

Что касается банковской сферы, в ней произошли изменения, заставившие выделить в 2024 году значительные ресурсы на развитие систем противодействия мошенничеству. Драйвером стал вступивший 25 июля 2024 года в силу Федеральный закон №369-ФЗ, согласно которому банки обязаны приостанавливать переводы, если информация о получателе денег содержится в базе данных Банка России о случаях и попытках мошеннических операций. В противном случае кредитной организации придется вернуть клиенту деньги в течение 30 календарных дней. Это привело к росту запросов на доработку и настройку функционирующих систем, а также на внедрение новых систем для тех заказчиков, которым из экономических соображений не было смысла в таких системах, так как потери были несоизмеримы со стоимостью внедрения и эксплуатации.

При этом традиционный для ИТ-рынка тренд на импортозамещение мало коснулся банков, поскольку многие либо уже заменили системы противодействия мошенничеству на российские (отечественные решения давно занимают ведущие позиции на рынке), либо настолько эти системы кастомизировали, что они стали «собственной разработкой». Тем не менее проекты по замене антифрод-движка на российский аналог с переносом существующих правил все еще встречаются.

Ключевые вендоры 2024

JET DETECTIVE

Если говорить о цифрах, мы фиксируем, что рост направления в 2024 году составил ~70%. В 2025-м, принимая во внимание объем запросов от небанковского сектора, мы прогнозируем еще больший рост.

По нашим прогнозам, рост направления в 2025-м обеспечат следующие факторы:

- рост количества проектов по противодействию мошенничеству и хищениям в небанковском секторе;
- предполагаемый ввод в действие закона об обязательном периоде охлаждения по потребительским кредитам и займам между заключением договора и получением денег, который, по аналогии с законом о приостановке переводов, будет возлагать на банки финансовую ответственность и, как следствие, приведет к необходимости доработки и настройке систем противодействия мошенничеству;
- развитие темы цифрового рубля, что приведет к необходимости обеспечения банками безопасных финансовых операций с его использованием. После полномасштабного запуска потребуется разработка правил и контрольных процедур для обеспечения безопасных операций.

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

С учетом требований импортозамещения 2024 год стал знаковым для тематики управления уязвимостями и пережил значительную трансформацию за счет постоянного выхода новых отечественных продуктов. Количество решений на рынке перевалило за десяток .

Ключевые вендоры 2024

positive technologies

INC SECURITY

ALTEX SOFT

GIS ГАЗИНФОРМ СЕРВИС

Важно отметить, что развитие направления управления уязвимостями не ограничивается только классическими сканерами уязвимостей. Стандартом становится использование систем контроля конфигураций, которые позволяют обеспечить постоянный мониторинг и поддержку целевых состояний параметров ИТ-инфраструктуры, что существенно снижает вероятность возникновения новых уязвимостей. В целом, мы фиксируем растущий тренд на харденинг ИТ-инфраструктуры, сокращение поверхности атаки и непрерывный контроль параметров безопасности. Кроме того, популярность набирают решения для автоматизированного тестирования безопасности (BAS) и

решения по автоматизации пентестов, которые обеспечивают более глубокий анализ потенциальных точек проникновения злоумышленников.

Решения класса BAS станут еще более универсальными, охватывая не только сетевую безопасность, но и защиту приложений, облачных сред и систем автоматизированного управления технологическими процессами (АСУ ТП). Автоматизированные пентесты продолжат набирать популярность, особенно среди компаний, испытывающих дефицит квалифицированных специалистов. Эти технологии позволяют снизить зависимость от человеческого фактора и обеспечить регулярные проверки безопасности без значительных затрат времени и ресурсов.

В 2025 году ожидается усиление тренда на автоматизацию процессов управления уязвимостями, что выходит за рамки их простого выявления. В условиях высокой конкуренции на рынке VM, успех будет зависеть от способности вендоров создавать решения, которые обеспечивают полный цикл управления уязвимостями — от обнаружения до устранения — в рамках одного продукта.

УПРАВЛЕНИЕ ДОСТУПОМ

Учитывая действующие регуляторные ограничения (Указ Президента РФ №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Приказ ФСТЭК №77 об «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»), предсказуемо растет спрос на замену продуктов классов IDM, IAM, SSO зарубежных вендоров отечественными решениями.

Также наблюдается интерес к решениям по управлению доступом с открытым исходным кодом. Они, как правило, проигрывают вендорным решениям по техническим параметрам и требуют серьезной доработки, но в определенных случаях могут выглядеть привлекательнее с точки зрения экономики.

Ключевые вендоры 2024

Сегодня рынок делят:

- вендоры, которые развивали свои продукты в течение последних семи-десяти лет и вывели их на высокий технический уровень;
- новые игроки, решения которых, возможно, начнут воспринимать более серьезно после проверки временем;
- Open-Sourse-решения, которые, несмотря на недостатки в части функциональности и удобства эксплуатации, предоставляют широкие возможности для кастомизации (при условии, что за внедрение берутся опытные профессионалы).

Описанная ситуация наиболее релевантна для IDM-решений в силу их особенностей, разница между отечественными и зарубежными IAM и SSO исторически была меньше.

Всеобщий тренд на импортозамещение отчасти задает направление развития продуктов отечественных вендоров. При выборе решения по управлению доступом все чаще приходится учитывать совместимость с отечественными продуктами, приходящими на замену зарубежным операционным системам, службам каталогов, почтовым, кадровым и интегрируемым системам. Наличие штатных коннекторов к большому количеству отечественных систем или хотя бы простота их разработки и кастомизации являются если не ключевым, то весомым параметром при выборе продукта.

Отдельно стоит отметить рынок биометрических систем управления доступом. В этом направлении 2024 год прошел под эгидой адаптации решений для соответствия 572-ФЗ, который говорит о том, что для распознавания по лицу система должна быть интегрирована с государственной биометрической системой (ГИС ЕБС). Если в 2023 году ввод нового требования вызвал некоторый спад на рынке биометрии, то за 2024 год решения основных крупных вендоров адаптировались для взаимодействия с ГИС ЕБС, и ситуация пришла в норму. К тому же за 2024 год появился ряд аккредитованных коммерческих биометрических систем.

В 2025-м ожидается рост направления на 40—50%, наиболее значимыми факторами для которого станут импортозамещение для крупных компаний и подключение к ЕБС.

Что касается финсектора, то в этой сфере специалисты отмечают незначительный рост запросов на решения по управлению доступом, однако в 2025 году ожидается увеличение спроса

до 50%. Прогноз обусловлен вступлением в силу ГОСТ Р 71753-2024 «Системы автоматизированного управления учетными записями и правами доступа» 20 декабря 2024 года, который устанавливает требования к автоматизации процессов, связанных с управлением доступом и используемыми системам. Наиболее востребованы сегодня и в будущем будут решения класса IdM и SSO отечественных производителей.

ЗАЩИТА ДАННЫХ

Несмотря на то, что внешние киберугрозы продолжают доминировать в медийном поле, задачи защиты от внутренних угроз и случайных сливов информации остаются критически важными для бизнеса.

Ключевые вендоры 2024

INFOWATCH®

СОЛАР

ГАРДА

CYBERPEAK
системы защиты данных

Интерес обусловлен несколькими ключевыми факторами. Прежде всего, наблюдается значительное увеличение объемов неструктурированных данных, требующих эффективной защиты. Это стимулирует компании переходить от базовых DLP-систем к более совершенным комплексным решениям по управлению данными, обеспечивающим детальный контроль и мониторинг. Кроме того, активное развитие отечественных продуктов в условиях импортозамещения предоставило рынку новые конкурентоспособные решения, способные успешно заменить зарубежные аналоги.

Основные технологические изменения, которые мы заметили в 2024 году, следующие:

1. Появление решений, работающих на уровне систем хранения данных, которые позволяют более эффективно контролировать доступ и предотвращать утечки;
2. Использование машинного обучения для автоматической классификации данных и выявления аномалий;
3. Добавление автоматического маркирования документов (функция, изначально нехарактерная для традиционных DCAP-систем, успела получить положительный отклик у наших заказчиков, способствуя более эффективной и оперативной категоризации данных).

Дальнейшее развитие направления будет зависеть не только от технологических достижений, но и от регуляторных изменений. В 2024 году вступили в силу важные изменения в законодательстве, касающиеся ответственности за утечки данных.

Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 30.11.2024 №420-ФЗ и Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 30.11.2024 №421-ФЗ значительно повысили размеры оборотных штрафов за нарушение требований по защите данных. Компании вынуждены адаптироваться к изменениям, что стимулирует поиск более эффективных решений для защиты данных.

ЭКСПЕРТНЫЕ СЕРВИСЫ

Одним из основных драйверов роста любых сервисов является кадровый голод, крайне обострившийся в последние годы. По сути, значительная часть организаций просто не может укомплектовать свой штат для закрытия необходимых потребностей, особенно в экспертных областях — мониторинг и реагирование, киберразведка, эксплуатация средств защиты в режиме 24x7.

Другой группой новых пользователей отечественных сервисов являются бывшие дочерние предприятия зарубежных компаний, которые раньше получали соответствующие сервисы от своих головных подразделений. Привыкшие жить по сервисной модели обеспечения ИБ, они переориентировались на российских сервис-провайдеров, создав существенный спрос на услуги по мониторингу и реагированию и технической поддержке.

Существенный рост и в части выручки, и в части количества проектов показывают тематики киберразведки и киберучений. Киберразведка становится неотъемлемой частью современного SOC, основным элементом защиты. Киберучения, в свою очередь, рассматриваются как способ подготовиться к неминуемому столкновению с хакерами в рамках кибератак, что соответствует смене парадигмы с «будем защищаться, чтобы нас не взломали» на «нужно быть готовым к тому, как действовать, когда нас взломают».

Подробную аналитику по нашим экспертным сервисам можно прочитать в исследовании «Анализ ландшафта угроз кибербезопасности 2024».

ЗАЩИТА ПРИЛОЖЕНИЙ (APPSEC)

Мы наблюдаем повышенный интерес к теме безопасной разработки в последние два года. Этому способствует несколько факторов.

- Рост зрелости уровня ИБ в компаниях и осознание, что безопасная разработка важна, в том числе из-за регулярного освещения этой темы в СМИ.
- Изменения в нормативном регулировании. Уже вступило в силу требование к безопасной разработке ЗО КИИ, описанное в приказе ФСТЭК №239, ЦБ РФ сформировал требования к уровню доверия разрабатываемого ПО и регулярно проверяет финансовые организации на соответствие этим требования, готовятся новые ГОСТы в части безопасной разработки (а значит, появится правоприменительная практика для таких ГОСТов).
- Появляется все больше решений в части безопасной разработки. В этом году на рынок вышли несколько SAST[1], DAST[2], SCA и ASPM-решений, формируются сервисы для оказания услуг в этой области.
- Немалый вклад в популяризацию направления вносит обмен опытом и новыми тенденциями на ИБ-конференциях (как профильных, так и общих), а также в локальных сообществах CISO и владельцев бизнесов.

Ключевые вендоры 2024

СОЛАР

kaspersky

positive technologies

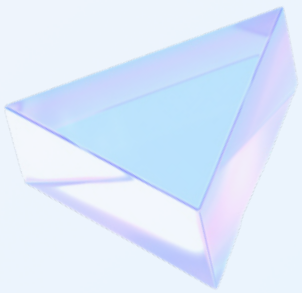
[1] SAST (Static Application Security Testing) — решения для повышения качества и надежности разрабатываемого ПО с помощью статического анализа кода на предмет ошибок и уязвимостей.

[2] DAST (Dynamic Application Security Testing) — метод тестирования безопасности приложений. Приложение проверяется во время его работы, без знания внутренних взаимодействий или структуры на системном уровне, а также без доступа или просмотра исходного кода.

Область защиты приложений (AppSec) и в целом направление DevSecOps наполнены доступными Open-Source-инструментами, позволяющими за относительно небольшие вложения обеспечить компаниям базовый уровень безопасной разработки и защиты разработанных приложений. Основным минусом в подходе построения защиты приложений на базе набора Open-Source-инструментов (помимо того, что придется мириться с некоторыми ограничениями в функциональности таких решений) является необходимость найма высококвалифицированных специалистов в штат, которых сейчас ощутимо не хватает на рынке ИБ. Использование enterprise-решений лишено таких недостатков и позволяет сократить и количество, и время специалистов AppSec и DevSecOps, затрачиваемое на обслуживание систем защиты приложений.

Последние два года запомнились также выходом нескольких важных документов и методологий в мире защиты приложений:

- ГОСТ Р 56939-2024 «Разработка безопасного программного обеспечения. Общие требования»;
- ГОСТ Р 71207-2024 «Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования»;
- фреймворк по безопасной разработке Appsec Table To от Positive Technologies;
- фреймворки по оценке зрелости процессов безопасной разработки DevSecOps Assessment Framework и по защите контейнерной инфраструктуры Jet Container Security Framework от «Инфосистемы Джет» (выложены в общий доступ).



По нашим оценкам, направления безопасной разработки, DevSecOps, защиты приложений будут активно развиваться, поскольку компании осознали важность этих направлений. Из-за новых требований законодательства в этой части рынок ожидает взрывной рост.

ЗАЩИТА АСУ ТП

В 2024 году направление информационной безопасности в автоматизированных системах управления технологическими процессами продолжало активно развиваться, что обусловлено ростом цифровизации промышленности, активным вводом в эксплуатацию и модернизацией новых промышленных объектов, а также увеличением числа киберугроз. Промышленные системы становятся все более привлекательной целью для киберпреступников и государственных хакерских группировок. Увеличилось число атак, направленных на критически важную инфраструктуру — энергетику, нефтегазовую отрасль, водоснабжение. Злоумышленники используют сложные методы, включая внедрение вредоносного ПО, атаки на цепочки поставок и эксплуатацию уязвимостей в устаревшем оборудовании.

В 2024 году продолжилось ужесточение нормативно-правовой базы в области ИБ для АСУ ТП. В России и других странах внедряются новые стандарты и требования, направленные на защиту критически важной инфраструктуры. Так, в России активно развивается регулирование в рамках ФЗ-187 «О безопасности критической информационной инфраструктуры» (КИИ), что требует от компаний внедрения комплексных мер защиты, включая аудит, мониторинг и реагирование на инциденты.

Продолжилась тенденция перехода промышленных предприятий на облачные платформы для управления производством. Это требует разработки новых подходов к обеспечению безопасности данных, передаваемых и хранящихся в облаке. Одновременно с этим многие промышленные объекты продолжают использовать устаревшее оборудование, которое не поддерживает современные стандарты безопасности. В 2024 году увеличился спрос на решения, позволяющие защитить такие системы, включая сетевую сегментацию, установку дополнительных средств мониторинга и обновление прошивок. Но, несмотря на развитие технологий, человеческий фактор остается одним из ключевых рисков в ИБ АСУ ТП. В 2024 году компании уделяли все больше внимания обучению сотрудников, проведению тренингов и симуляций кибератак в рамках киберучений. Этот подход позволяет снизить вероятность ошибок, связанных с недостаточной осведомленностью персонала.

Ключевые вендоры 2024

kaspersky

positive technologies

КОНСАЛТИНГ

Направление консалтинга всегда отличалось достаточной стабильностью с точки зрения финансовых показателей, что неудивительно, ведь основные услуги в виде аудитов и тестирований на проникновение давно известны рынку. Количество и объемы наших консалтинговых проектов, включая проекты по выполнению требований законодательства, пентесты и экспертный консалтинг, в 2024 году выросли относительно 2023 года на 42%, что практически точно совпадает с общими темпами роста.

Изменения заметны в тех целях, которые организации ставят себе при проведении аудитов и пентестов — сейчас это обеспечение реальной защищенности бизнес-процессов, связь информационной безопасности с непрерывностью бизнеса и выстраивание защищенной ИТ-инфраструктуры.

Не в последнюю очередь этому способствует громкое медийное освещение крупнейших кибератак в 2024 году. Такая публичность формирует у топ-менеджмента организаций запрос на независимую оценку уровня своей безопасности и готовности к восстановлению. Образно говоря, запрос заказчиков «проверьте, как работает моя ИБ» трансформируется в «проверьте, насколько мой бизнес защищен от остановки, как быстро в случае остановки он может быть восстановлен».

В 2025 году мы ожидаем усиление этого тренда, а также кратный рост проектов по теме непрерывности бизнеса и обеспечения восстановления.

JET
SECURITY
TEAM

security@jet.su
jetcsirt.su