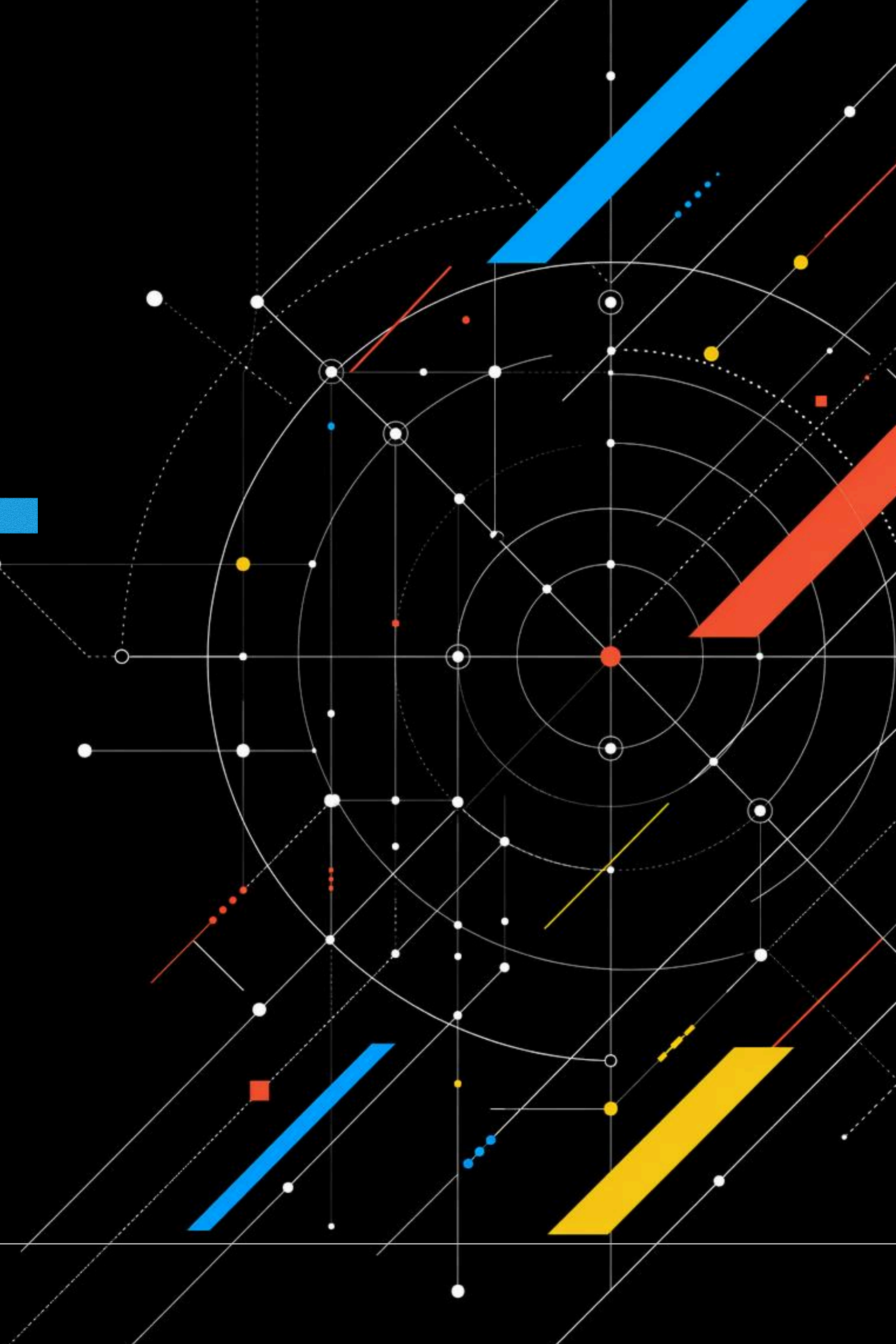


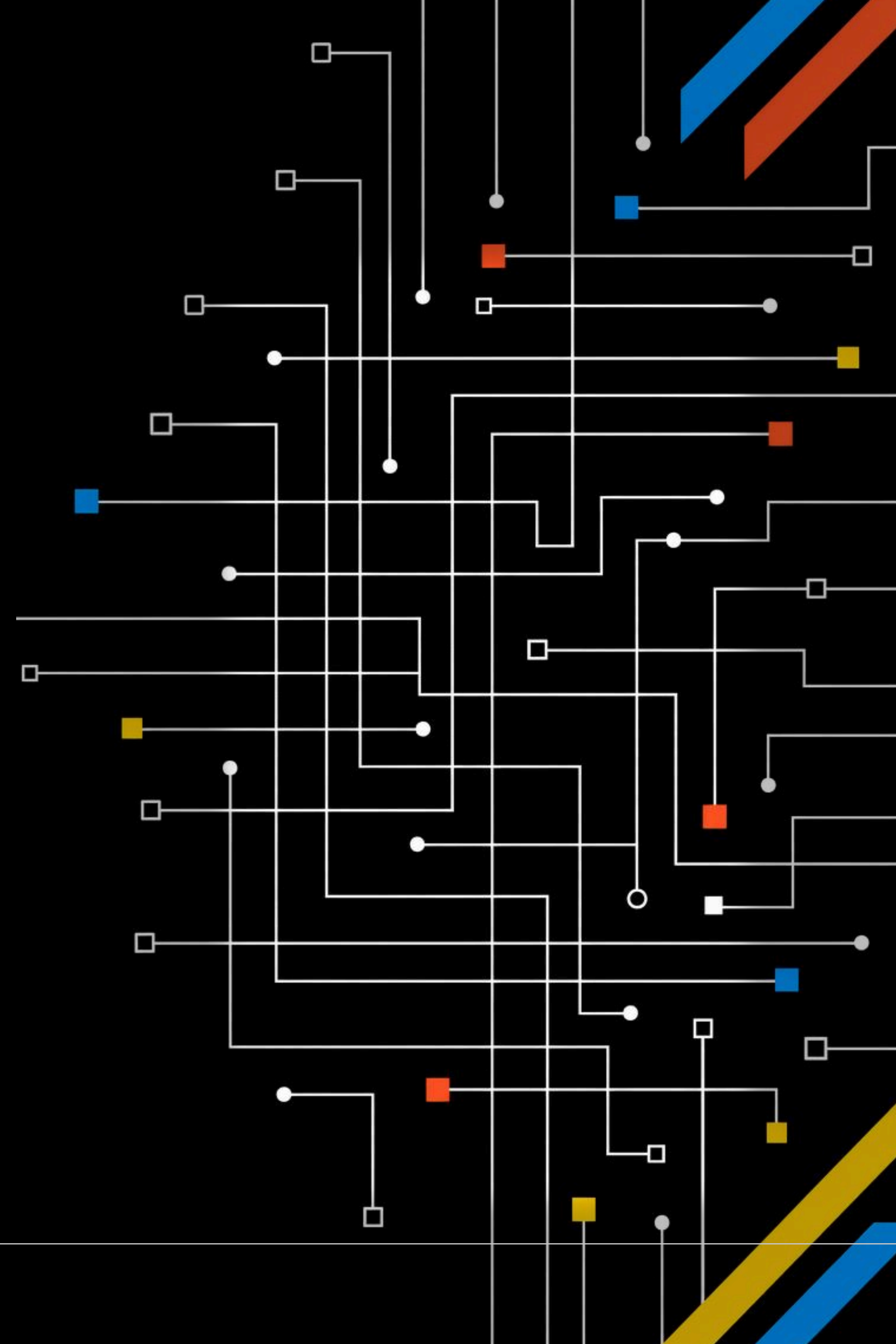
Дайджест рынка ИБ

июнь 2026



Оглавление

03.....	Резюме
04.....	Рекомендации
05—06	Регулирование
07—08	Новости компаний
09—14	Тенденции
15—16	Реестры Минцифры
17.....	Реестр ФСТЭК



03 Резюме

Банк России перевел ИИ в финансовом секторе в плоскость ИБ-рисков

Рекомендации Банка России №3-МР от 16 июня задают для финансового рынка рабочую рамку ИИ-безопасности. Исследование K2 и «Лаборатории Касперского» показывает, что 59% крупных компаний используют несколько типов ИИ-сервисов, но управляемые процессы защиты собственной ИИ-разработки есть только у 18%. На стороне продуктов в июне появились AIDR для контроля корпоративных LLM, PT Naira для SOC и AppSec, MOLOT для поиска вредоносного поведения в коде, ИИ-триаж и кодфикс в Solar appScreener.

Рост рынка ИБ поддерживают не только закупки СЗИ, но и эксплуатация, совместимость и сервисная модель

ЦСР оценивает российский рынок ИБ в 2025 году более чем в 364 млрд руб., рост - 16,1% год к году. СЗИ формируют около 74% рынка, услуги - около 26%.

Антифрод и авторизация — часть архитектуры цифровых каналов

Федеральный закон №210-ФЗ расширяет антифрод-обязанности банков, операторов связи и цифровых сервисов. Федеральный закон №199-ФЗ добавляет ответственность за нарушения правил авторизации пользователей на российских сайтах и в приложениях, а также за нарушения при применении рекомендательных технологий.

SOC и EDR требуют инвентаризации активов

Исследование «Гарды» фиксирует разрыв между быстрым первичным ответом и зрелым реагированием. Исследование ЦСР по Endpoint Security дополняет эту картину. EPP остается основным объемом сегмента, но EDR растет быстрее и чаще потребляется через MSS/MDR

AppSec расширяется до цепочки поставки ПО, CI/CD и подписи кода

Positive Technologies в отчете по веб-приложениям и инфраструктуре разработки включает в поверхность риска API, контейнеры, репозитории, open source, CI/CD, секреты, LLM-приложения и ИИ-агенты. Июньские продуктовые новости показывают тот же сдвиг на уровне функций: MOLOT ищет вредоносное поведение в коде, Solar appScreener развивает ИИ-триаж и работу с open source-компонентами, Kaspersky Container Security добавляет проверки политик и GitHub Actions

Промышленная ИБ зависит от ИТ, подрядчиков, учетных записей и доверенных каналов

BI.ZONE: за I кв.2026г. доля финансово мотивированных атак на российские промышленные компании выросла до 36%. Kaspersky: рост инцидентов в транспорте и промышленности

04 Рекомендации

Для заказчиков	Для интеграторов и MSSP	Для вендоров
Описать ИИ-сценарии, данные, роли, журналы и подтверждение критичных операций.	Собрать практики AI Security на стыке ИБ, данных, AppSec, SOC и архитектуры ИИ.	Показывать управляемость ИИ-функций: аудит, права, журналы, интеграция с SIEM/SOC.
Пересмотреть антифрод, авторизацию и клиентские цифровые каналы.	Делать проекты IAM/MFA, антифрода, защиты ДБО, телеком-сигналов и юридически значимых событий.	Развивать объяснимость антифрода, поведенческую аналитику, графы связей и SOC-интеграции.
Навести порядок в активах, внешнем периметре, SOC/EDR/MDR и планах восстановления.	Продавать готовый процесс: активы, правила, плейбуки, метрики, EASM, WAF, Anti-DDoS, API Security и IR.	Улучшать телеметрию, расследование, API, отчеты, приоритизацию и передачу контекста в SOC.
Проверить CI/CD, open source, секреты, контейнеры, подпись кода, подрядчиков и КИИ-среду.	Выделить AppSec / supply chain и отраслевую ИБ в отдельные практики.	Поддерживать разработческие процессы, промышленные протоколы, российские платформы и сертификацию.

05 Регулирование

Банк России: Рекомендации по использованию ИИ

16 июня Банк России выпустил методические рекомендации №3-МР по обеспечению ИБ при разработке и применении ИИ на финансовом рынке. Документ описывает риски ИИ-систем, тактики атак, меры защиты, внутренние документы, роли участников процесса и дополнительные меры для критически важных операций. Для операций с высоким ИБ-риском регулятор рекомендует подтверждение сотрудником.

Для финансовых организаций практический старт — реестр ИИ-сценариев. Без него невозможно понять, какие модели используются в платежах, антифроде, скоринге, клиентских сервисах, обработке обращений и внутренних процессах. После инвентаризации нужно проверять данные, поставщиков, доступы, журналы, модель угроз и точки, где требуется ручное подтверждение.

Законопроект о больших моделях ИИ задает будущую рамку доверия к моделям

25 июня в Госдуму внесен законопроект №1271570-8 «О поддержке развития технологий искусственного интеллекта в Российской Федерации». Документ определяет понятийный аппарат и принципы регулирования отношений в сфере разработки, внедрения, использования и применения больших фундаментальных моделей ИИ. В проекте появляются категории суверенных и национальных больших фундаментальных моделей.

Законопроект пока не создает новых обязанностей для организаций. Его значение для ИБ-повестки — в будущих вопросах доверия: где размещается модель, какие данные используются, кто владеет моделью, как подтверждается статус, кто контролирует обновления и какие сценарии применения могут быть ограничены суверенными или национальными моделями.

ФСТЭК: обзоры правоприменительной практики

ФСТЭК утвердила два обзора правоприменительной практики за 2025 год. Приказ №184 от 17 июня касается контроля за соблюдением участниками ВЭД законодательства в области экспортного контроля. Приказ №194 от 30 июня относится к лицензионному контролю деятельности по технической защите конфиденциальной информации и разработке и производству средств защиты конфиденциальной информации.

В экспортном контроле ФСТЭК выделяет операции без лицензий или разрешений, непроведение идентификации контролируемых товаров и технологий, нарушения учета внешнеэкономических сделок и слабое внимание к внутренним программам экспортного контроля. В лицензионном контроле по ТЗКИ и СЗКИ отдельно видна тема повышения квалификации специалистов.

06 Регулирование

Инициативы Минцифры

Минцифры предложило поэтапный переход значимых объектов КИИ на российское ПО: общий срок — с 1 января 2028 года, а для отдельных случаев — сдвиг до 2031 или 2036 года

Минцифры РФ считает ключевой задачей на 2026 год подготовку нормативной базы для введения "серьезных" штрафов для компаний за несоблюдение сроков перевода значимых объектов КИИ на российское ПО

Антифрод-2

26 июня опубликован Федеральный закон №210-ФЗ — второй пакет антифрод-мер. Среди заметных положений — ограничение количества банковских карт, новые обязанности банков и операторов связи, база IMEI, самозапрет на международные звонки и механизм компенсаций при отдельных нарушениях порядка противодействия мошенническим переводам.

Закон №199-ФЗ: авторизация и рекомендательные технологии получили штрафной контур

26 июня опубликован Федеральный закон №199-ФЗ о внесении изменений в КоАП. Он вводит ответственность за отдельные нарушения в сфере связи и информации, включая нарушения правил авторизации пользователей на российских сайтах и в приложениях, а также нарушения при применении рекомендательных технологий. Для организаций штрафы за нарушения авторизации составят от 500 тыс. до 700 тыс. руб., при повторном нарушении - от 1 млн до 1,4 млн руб.

Владельцам сайтов и приложений нужно проверить сценарии входа пользователей: какие способы авторизации используются, есть ли внешние сервисы входа, как работают MFA, сессии, восстановление доступа и журналы подозрительных действий.

Хостинг ГИС и требования к провайдерам

ТПП просила отложить расширение требований к хостинг-провайдерам для государственных систем. Сейчас требования затрагивают только ограниченный круг провайдеров, допущенных к работе с основными ИТ-госсистемами

Российская подпись кода

Крупнейшие российские разработчики создают систему защиты отечественного софта, которая сможет обеспечить защиту в условиях массового отзыва сертификатов для подписи программного кода западными удостоверяющими центрами. Это следует из презентации рабочей группы «Единое пространство доверия», которая действует на базе Национального технологического центра цифровой криптографии во взаимодействии с ФСБ, Минцифры и ФСТЭК

07 Новости компаний

Информзащита



«Информзащита» подтвердила статус Российского морского регистра судоходства на проведение проверки кибербезопасности судовых компьютеризированных систем и сетей.

14%

организаций имеют инструменты, позволяющие выявить манипуляцию ИИ-агентом и заблокировать опасный сценарий без ручной реакции. Доля проектов, где агенты получают доступ к письмам, документам, сайтам и обращениям, за год выросла с 18% до 34%.

42%

рост обращений по проверке prompt-зависимостей и расследованию активности в цепочках поставки ПО в январе-мае 2026 г/г

Positive Technologies

ИИ переходит из экспериментальной функции в рабочие инструменты SOC, AppSec и управления внешним риском

PT Naira

Positive Technologies выпустила ИИ-помощника на базе больших языковых моделей. Первые точки применения - MaxPatrol SIEM и PT BlackBox. В пилотах компания заявила ускорение расследования инцидентов на 50-60%, а подготовку правил для новых источников событий в MaxPatrol SIEM - почти на 90%.

Киберпогода

Компания представила платформу для прогнозирования внешних угроз и интерпретации бизнес-рисков. Продукт анализирует головную организацию, дочерние компании, партнеров, поставщиков, подрядчиков и производителей ПО. Positive Technologies оценивает формирующийся российский рынок таких решений в 5,5-6,6 млрд руб. на горизонте трех лет.

MOLOT

Positive Technologies обучила нейросеть MOLOT находить вредоносный код по последовательности действий программы. Модель используется в PT Application

Innostage выпустила AIDR - продукт для защиты корпоративных LLM и ИИ-сервисов. Решение работает как прозрачный прокси между пользовательским ИИ-приложением и языковой моделью: фильтрует входящие запросы, блокирует prompt injection и jailbreak, проверяет ответы на персональные данные, коммерческую тайну и другую критичную информацию, а события безопасности передает в SIEM

Innostage

AIDR закрывает контроль запросов и ответов корпоративных LLM

08 Новости компаний

ГК «Солар»

Solar appScreener 3.16 смещает AppSec к ИИ-триажу и ускорению исправлений

ГК «Солар» выпустила обновление Solar appScreener 3.16. Главный акцент сделан на SAST: ускорение анализа кода, ИИ-триаж результатов и автоматическую подготовку исправлений. По заявлению компании, ИИ-плагин работает в закрытом контуре, показывает более 90% точности на этапе триажа и до 85% на этапе исправления уязвимостей.

Интеграция	Что подтверждено	Практический эффект
<u>Solar SafeInspect</u> + «Ятоба»	Поддержка контроля привилегированных сессий при работе с отечественной СУБД на базе PostgreSQL.	Заказчик сохраняет видимость действий администраторов и подрядчиков при переходе на российскую СУБД, без разрыва РАМ-контроля.
<u>Solar SafeInspect</u> + Tantor Postgres	Технологическая совместимость в рамках программы Ready for Astra.	Для госсектора и КИИ это упрощает миграцию на отечественную СУБД с сохранением аудита, расследования и контроля привилегированных учетных записей.

Kaspersky

В Kaspersky Container Security добавлены собственные политики и benchmark-проверки, импорт и экспорт конфигурации, аудит control plane и правила выявления ошибок в GitHub Actions. Контейнерная безопасность все сильнее связывается с DevSecOps и supply chain.

R-Vision + УЦСБ

R-Vision и УЦСБ заключили соглашение о сотрудничестве для реализации комплексных проектов ИБ на базе платформы R-Vision EVO. Соглашение предусматривает, среди прочего, ранний доступ УЦСБ к платформенным решениям R-Vision.

SolidLab + R-Vision:

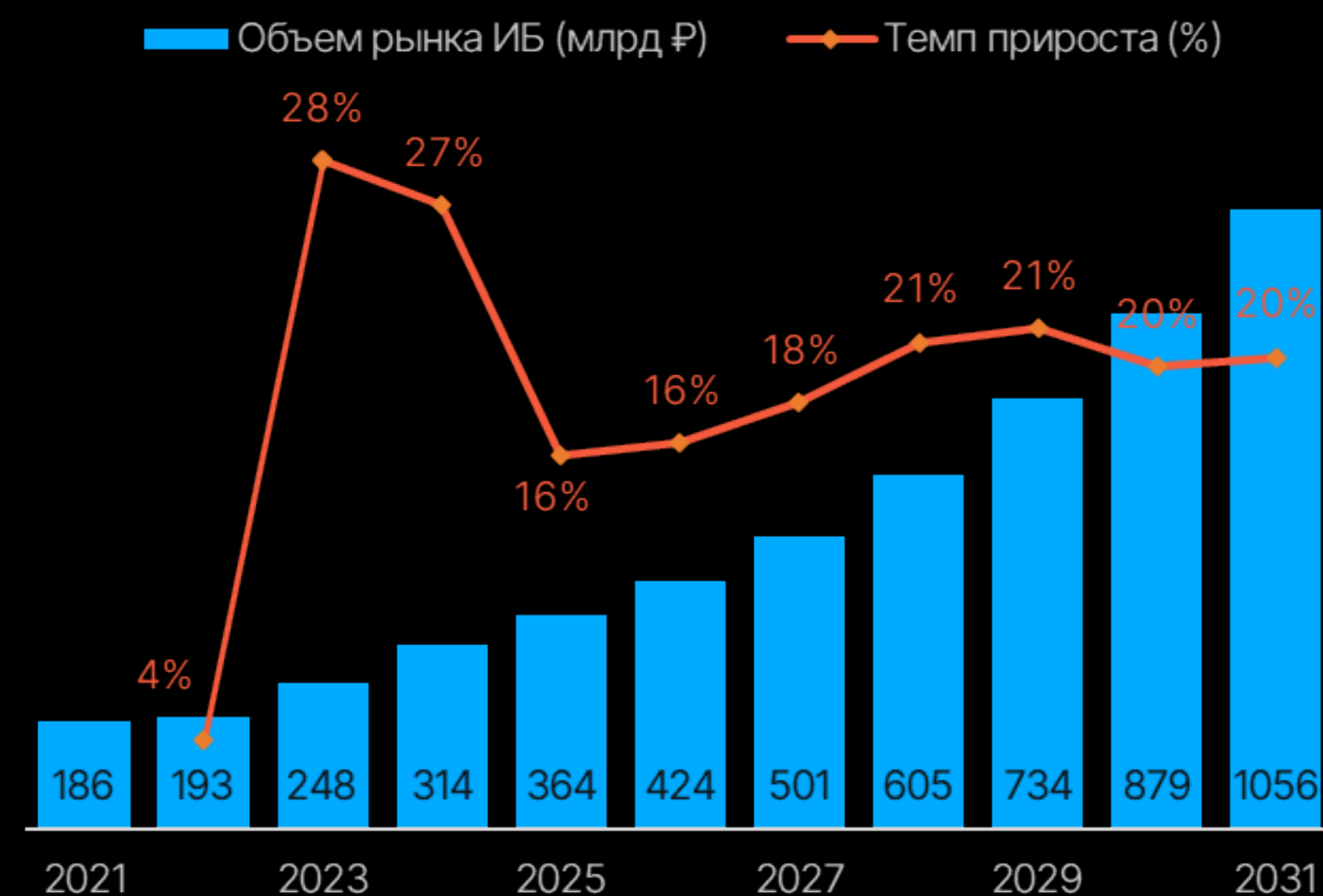
SolidLab и R-Vision подтвердили технологическую совместимость SolidLab VMS и R-Vision SOAR. Интеграция позволяет передавать данные об уязвимостях в SOAR, формировать и обновлять инциденты, связывать их с активами, обогащать контекстом и запускать сценарии обработки.

09 Тенденции

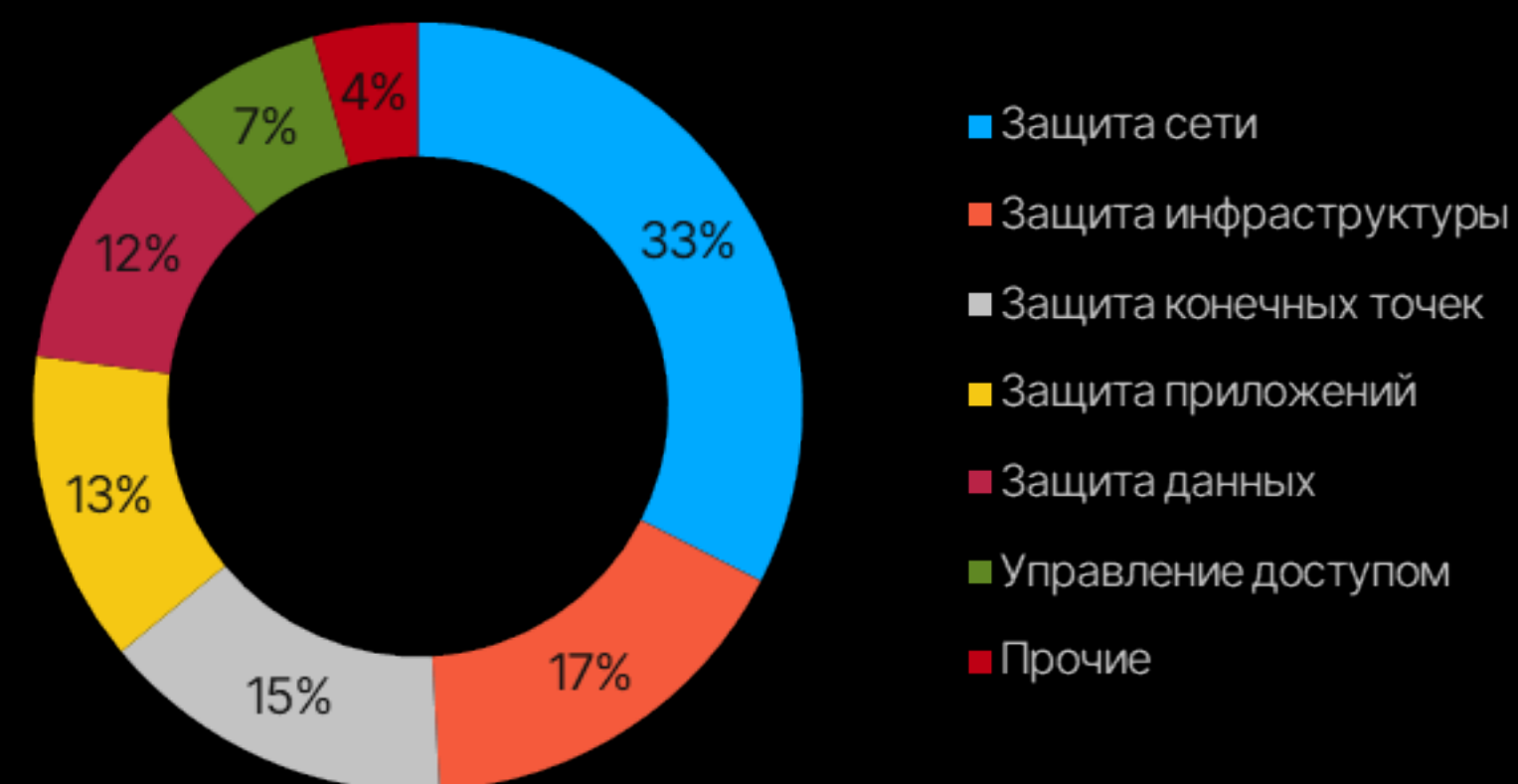
Центр стратегических разработок (ЦСР)

Рынок ИБ России: текущее состояние и перспективы развития до 2031г

Динамика объема рынка ИБ в 2021-2031гг



Долевое распределение продаж различных категорий СЗИ в 2025 году, %



364
млрд ₽

Объем рынка ИБ РФ в 2025г. Рост 16% к 2024 г.

93.5
млрд ₽

Объем рынка услуг ИБ в РФ, ≈ 26% рынка ИБ

94%

Доля российских поставщиков СЗИ

19%

Прогнозируемый совокупный среднегодовой рост рынка ИБ в 2025-2031 гг.

10 Тенденции

Центр стратегических разработок (ЦСР)

Рынок средств защиты конечных точек

40.1 Объем рынка защиты конечных точек в РФ в 2025 г.
млрд ₽ Рост 15% к 2024 г.

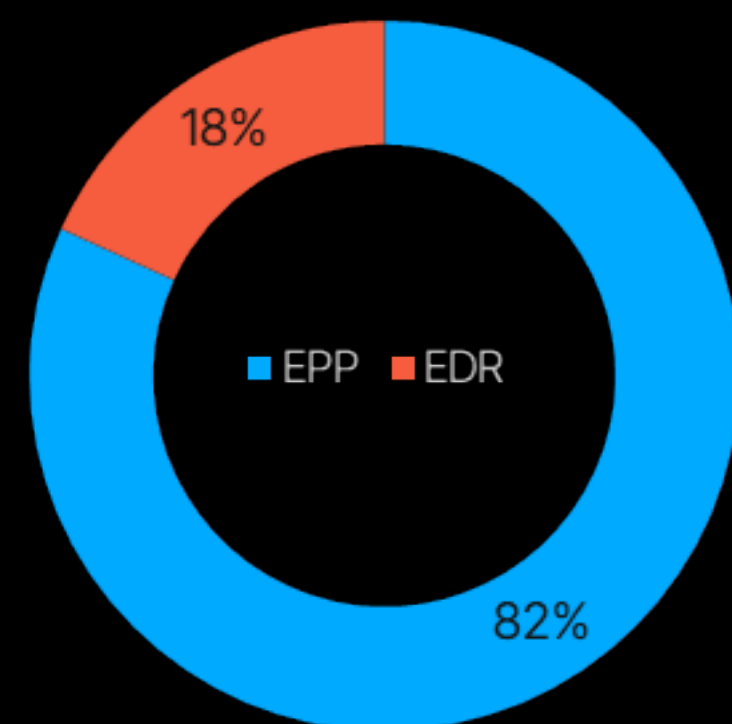
8% Прогнозный CAGR EPP в 2026-2031 гг.

22% Прогнозный CAGR EDR в 2026-2031 гг.

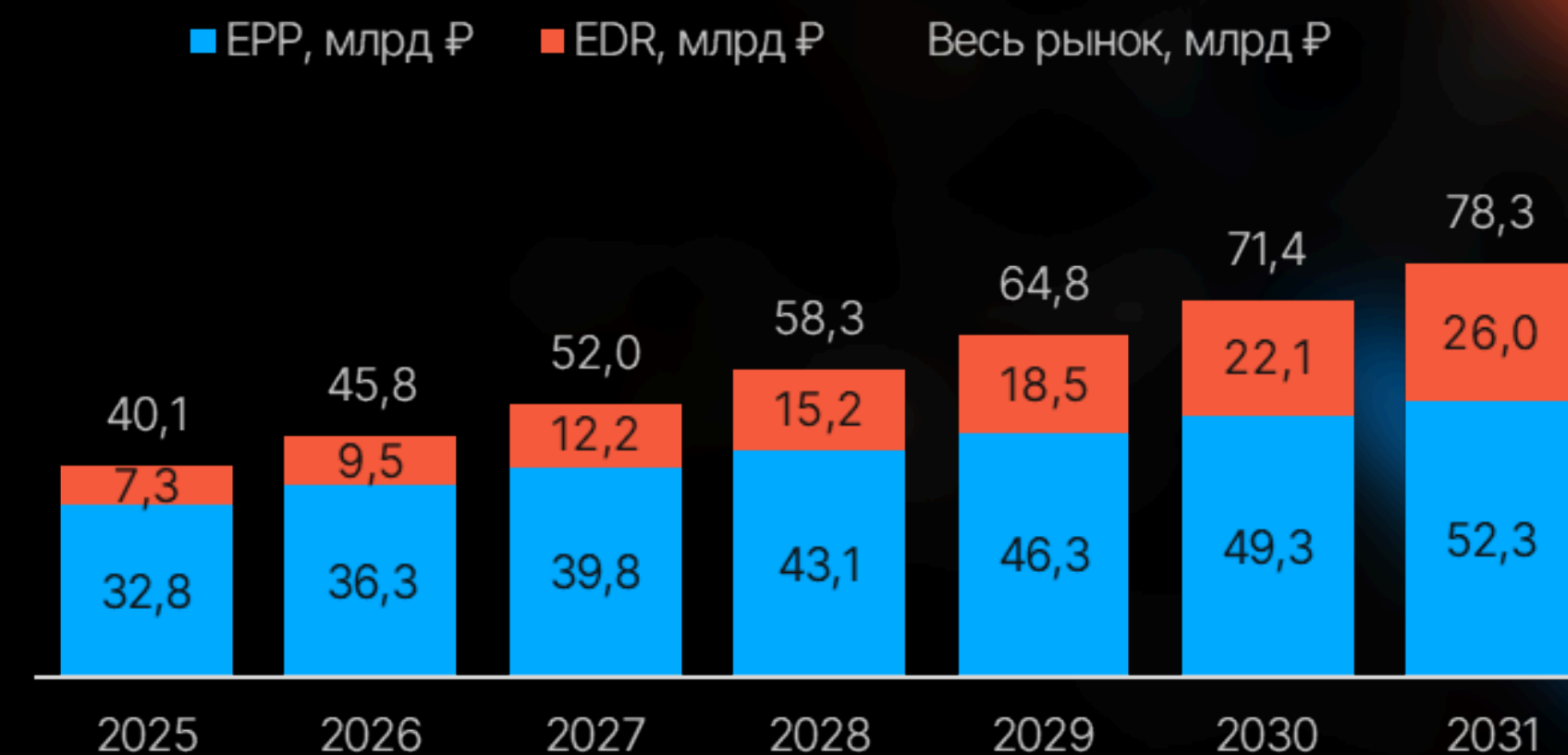
Динамика рынка защиты конечных точек в РФ, 2021-2025, млрд ₽



Долевое распределение категорий в 2025 году, %



Прогноз развития рынка защиты конечных точек



11 Тенденции

Гарда

Как российские компании реагируют на ИБ-инциденты

72% Среднее время реагирования на ИБ-инциденты — менее суток

57% Компаний без полной автоматизированной инвентаризации активов

Типы инцидентов, требующие наибольших ресурсов для реагирования



Инструменты для выявления и реагирования на ИБ-инциденты



Отчет показывает ограниченную зрелость полного цикла реагирования на инциденты. Компании умеют обнаруживать и выполнять базовые действия. Слабое место в более сложных процедурах: расследование, контекст, классификация активов, эскалация, восстановление и измерение результата.

Главные проблемы, замедляющие реагирование



12 Тенденции

К2 + «Лаборатория Касперского»

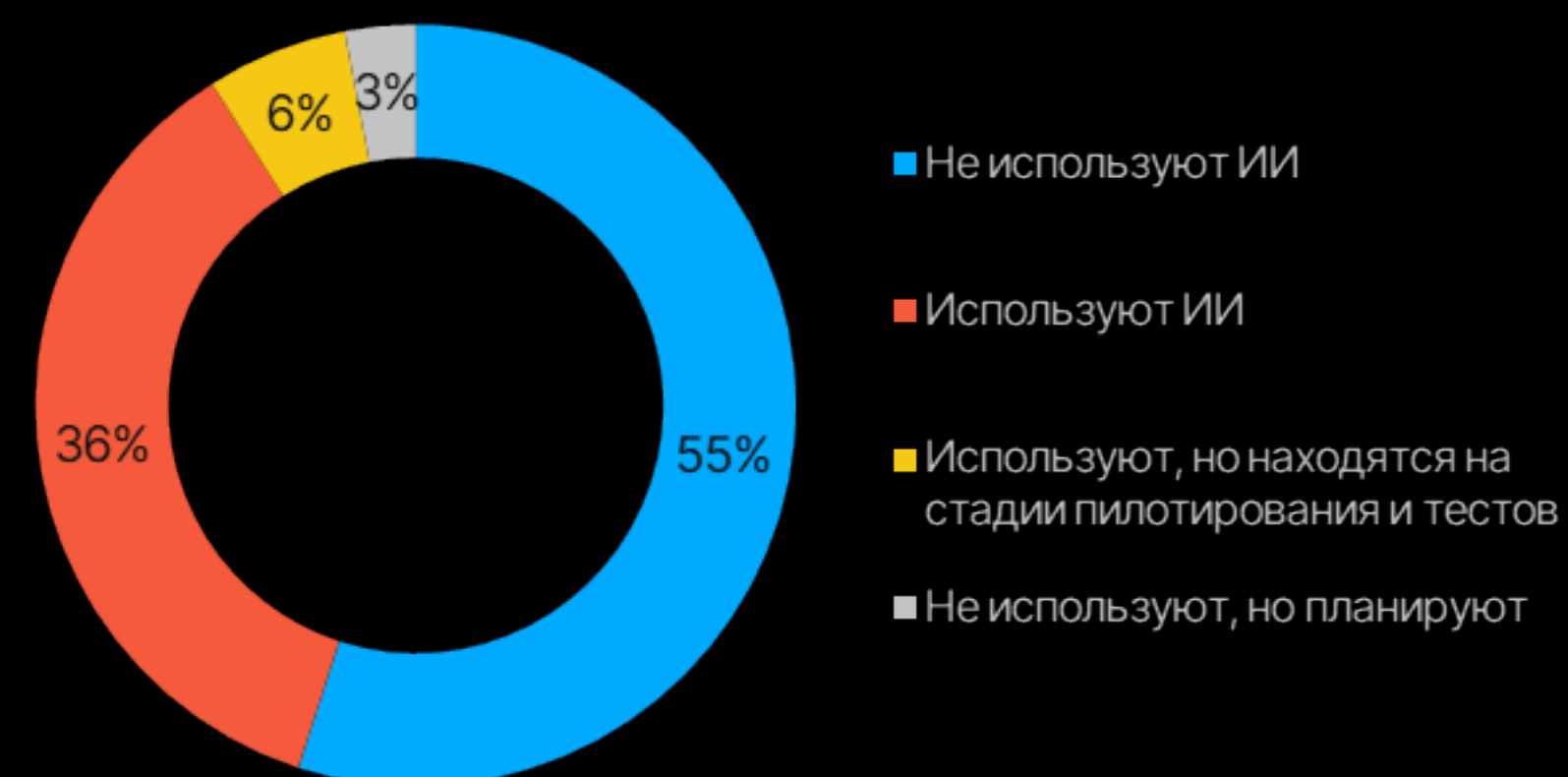
Безопасность ИИ в России: практика, риски, зрелость

59% Компаний, использующих ИИ, работают с несколькими типами ИИ-сервисов

38% Имеют собственные команды ИИ-разработки

61% Стремится контролировать использование внешних ИИ-сервисов

Применение ИИ в компаниях



Насколько ИИ важен компаниям



Отчет показывает разрыв между внедрением и контролем ИИ. Компании уже используют российские, зарубежные, собственные и заказные ИИ-сервисы одновременно. Без реестра моделей, правил доступа, контроля данных, проверки внешних сервисов и ответственности между ИБ, ИТ и разработкой такой ландшафт быстро становится неуправляемым

14% Хорошо знакомы с методологией MLSecOps

42% Не внедрили защиту датасетов

30% Не используют контроль доступа и доставки

22% Не используют ролевую модель доступа к ИИ-сервисам и наборам данных

13 Тенденции

Positive Technologies

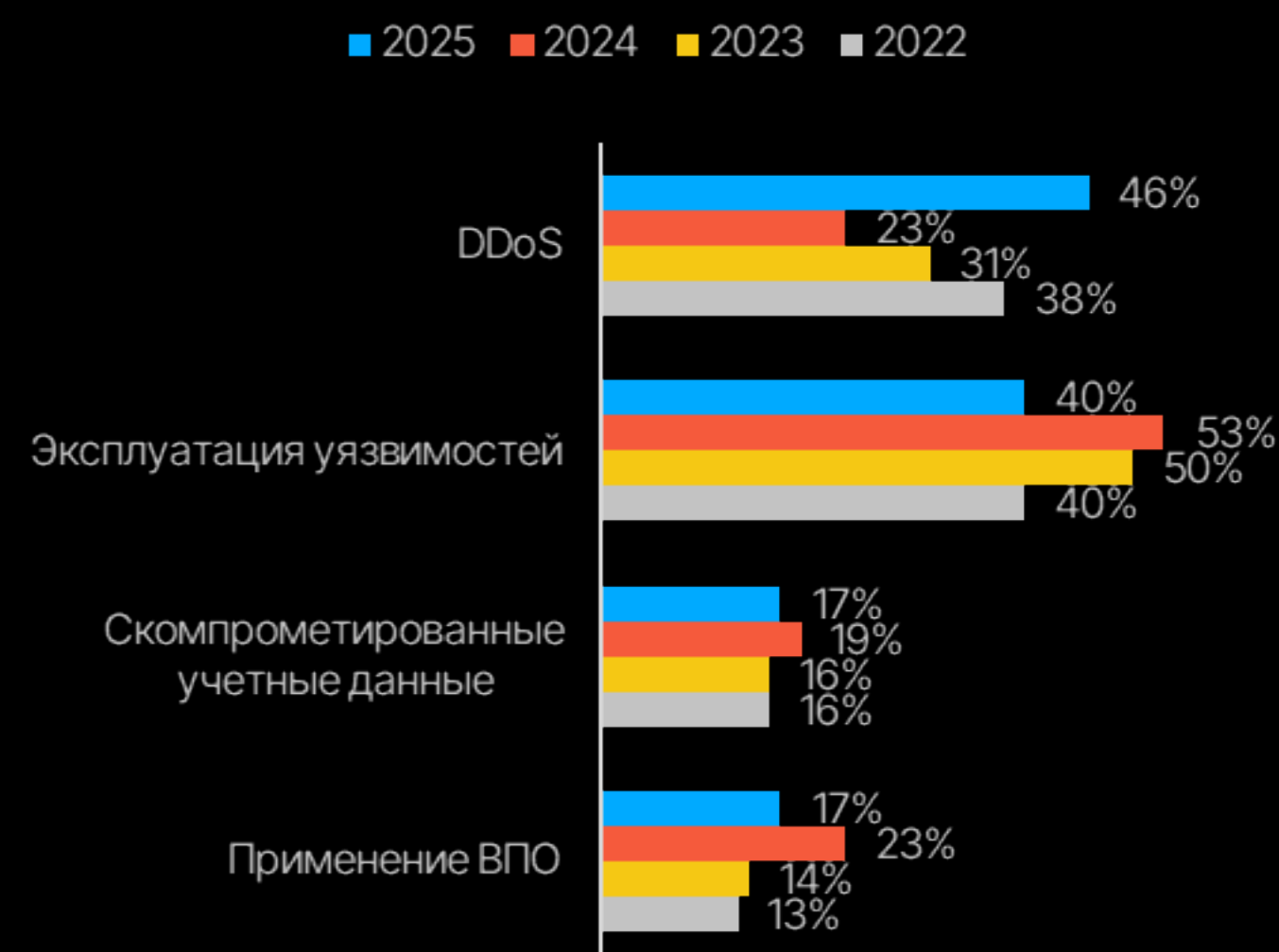
Киберугрозы веб-приложений и инфраструктуры разработки: тренды и прогнозы 2026–2027

20% В 2025 году каждая пятая успешная атака на организации была направлена на веб-ресурсы

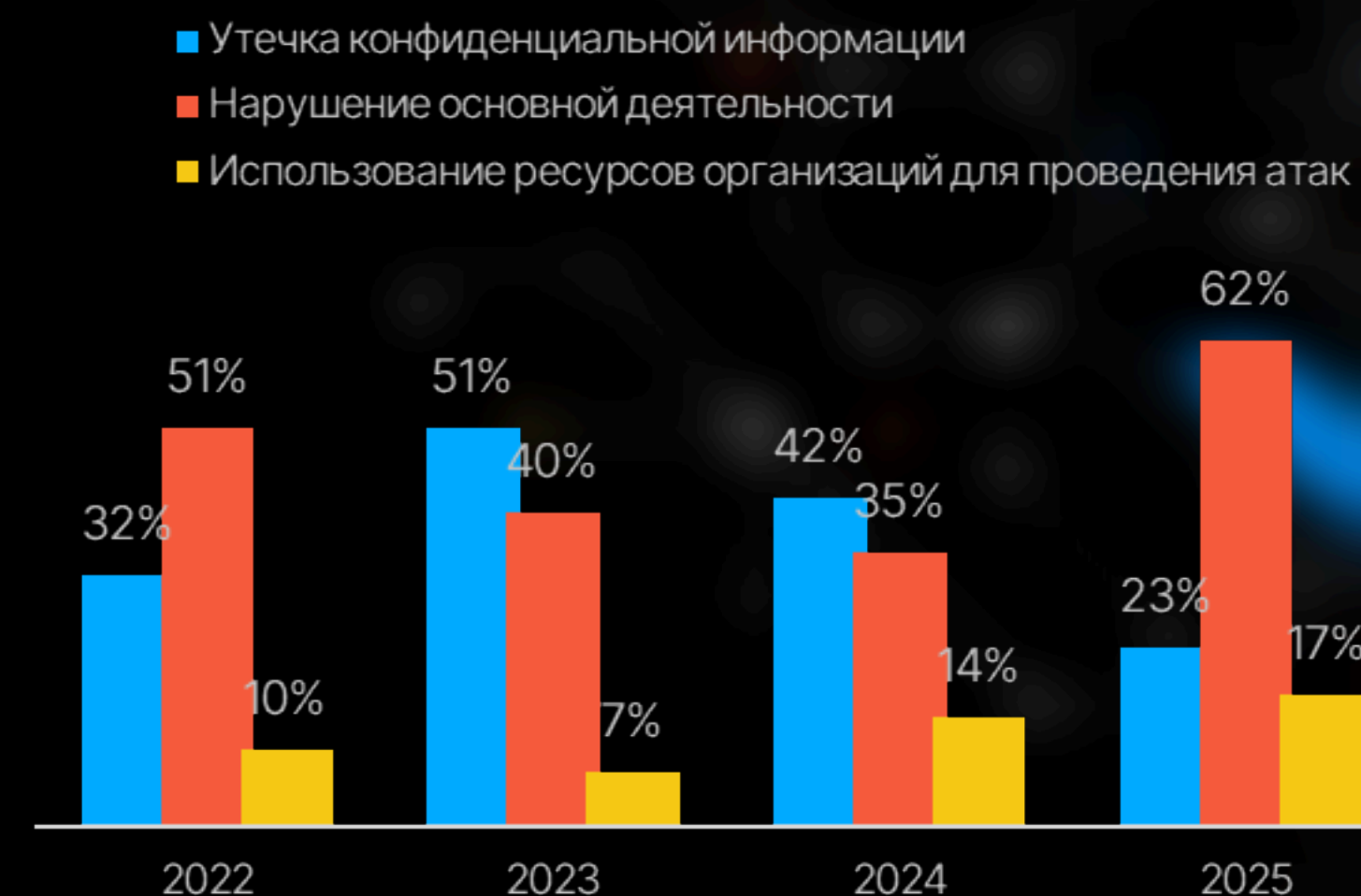
75% успешных атак на веб-приложения российских организаций в 2025 г. привели к нарушению основной деятельности

- ⚡ Веб-приложения стали не отдельным ИТ-активом, а точкой воздействия на операционную устойчивость.
- ⚡ DDoS снова стал в 2025г одним из главных практических рисков для публичных сервисов: доля DDoS среди успешных инцидентов в мировом масштабе — 46%, в масштабе России — 48%
- ⚡ Эксплуатация уязвимостей остается системным каналом компрометации: 40% успешных атак на веб-приложения в мировом ландшафте и 43% в атаках на веб-ресурсы российских организаций.
- ⚡ Open source и CI/CD становятся частью периметра ИБ
- ⚡ Скомпрометированный веб-ресурс становится плацдармом для дальнейших атак

Методы, использованные в успешных атаках на веб-ресурсы (мир)



Динамика последствий успешных атак на веб-приложения (мир)



14 Тенденции

Лаборатория Касперского

Киберпульс.Россия

+68% Рост обнаруженных и предотвращенных ИБ-инцидентов в российских организациях в 1 кв. 2026 г/г

+24% Рост инцидентов в транспорте и промышленности

+39% Рост атак с эксплойтами

+39% Рост атак с банкерами

Аналитика по данным Kaspersky DDoS Protection, за период январь — май 2026 г.

+27% Рост числа DDoS-атак в России и странах СНГ к аналогичному периоду 2025 года

51% Увеличение доли атак уровня приложений до 51% в общей структуре DDoS против 31% годом ранее

+215% Рост атак свыше 200 Гбит/с

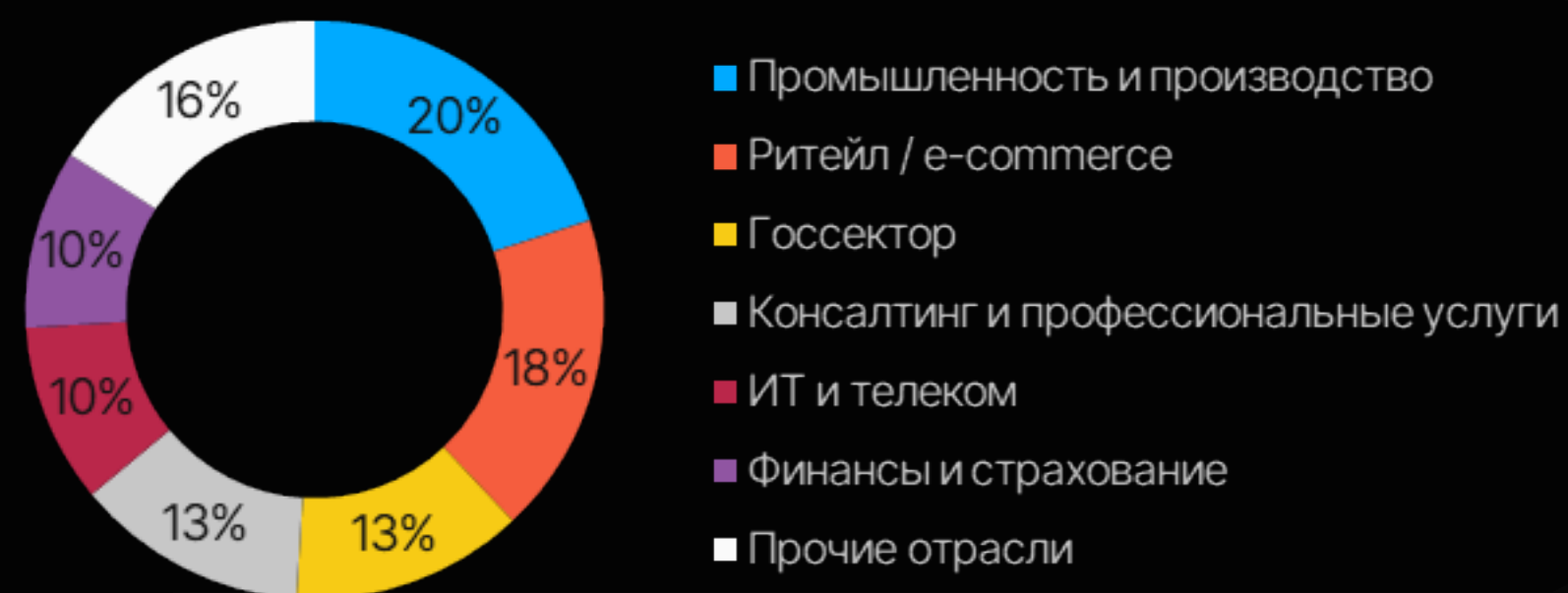
Инфосистемы Джет

Аналитика Jet CSIRT по ИБ-инцидентам за 2023-2025 годы

Сценарии атак



Распределение инцидентов по отраслям



15 Реестр Минцифры: ПО

UserGate SWG

Шлюз веб-безопасности корпоративного класса. Контролирует доступ сотрудников к веб-ресурсам и веб-сервисам, проверяет HTTP / HTTPS-трафик, применяет политики, блокирует фишинговые, вредоносные и нежелательные сайты.

Avanpost DAG

Инвентаризирует неструктурированные данные, права пользователей и группы доступа. Помогает находить избыточные права, контролировать политики доступа и готовить аудит по файловым ресурсам и хранилищам.

КриптоАРМ ID

Решение для доступа клиентов, партнеров и сотрудников к информационным системам, сайтам и приложениям.

Гарда DBF

Контролирует операции с СУБД и бизнес-приложениями, фиксирует запросы к данным, выявляет подозрительные действия и может блокировать нелегитимные обращения.

SDLPlatform

Собирает результаты SAST, SCA, поиска секретов, анализа конфигураций и линтеров в едином контуре. Помогает убирать дубли, передавать задачи в трекеры и встраивать проверки в CI/CD

Clearway: МиУ, ЕСАУС, ЛКПС

Группа продуктов на базе платформы ЦУГИ: мониторинг и управление АРМ и серверами, автоматическое управление сертификатами, личный кабинет для сертификатов и секретов

BitScore

Оценивает операции и действия пользователя в каналах онлайн-платежей и ДБО на признаки мошенничества. Работает как прикладной слой контроля риска в финансовом сервисе.

Мобильное приложение «Квантум»

Связано с облачным сервисом комплексной защиты корпоративных сетей: VPN, SOC, анализ SSL / SSH и защита от сетевых угроз.

Программный комплекс «Сервер Бэкапирования»

Комплекс включает управление резервным копированием и компоненты передачи резервных данных между источником и получателем.

Программный модуль «Сирена»

Модуль для выявления противоправных действий в видеодорожке при видеопереговорах или видеосообщениях через специализированную закрытую телефонную сеть.

FingerPOS

Плагин для iiko / Syrve, который авторизует сотрудников по отпечатку пальца, фиксирует смены и подтверждает отдельные операции в кассовом или ресторанном контуре.

16 Реестр Минцифры: ПАК

JaCarta-2 ГОСТ и JaCarta PKI

USB-токены для строгой аутентификации, хранения ключевой информации и работы с электронной подписью. ГОСТ-исполнение закрывает сценарии с отечественными криптоалгоритмами.

Aladdin CryptoFlash

Флеш-накопитель со встроенным шифрованием для хранения и переноса информации ограниченного доступа. Доступ к данным получают только авторизованные пользователи.

Рутокен ЭЦП 3.0 3120

USB-токен и смарт-карта для двухфакторной аутентификации и квалифицированной электронной подписи в государственных и корпоративных системах.

ФПСУ-Q версии 4, несколько исполнений

ПАК для защищенной передачи данных, организации VPN и защиты обмена между площадками.



17 Реестр ФСТЭК

UserGate SIEM

Собирает журналы и события из инфраструктуры, анализирует их, помогает выявлять подозрительные действия и признаки атак.

Нужен для построения мониторинга ИБ, расследования инцидентов, выполнения требований к журналированию и работе SOC в регулируемом контуре.

CoreBit.NGFW

Программно-аппаратный межсетевой экран нового поколения для корпоративных и критических сетей. Закрывает функции контроля сетевого трафика и защиты периметра.

Подходит для замены или расширения сетевых СЗИ, сегментации периметра, контроля доступа между зонами и проектов защиты КИИ

FTData Enterprise Certified

Объектно-реляционная СУБД на базе PostgreSQL. Сертифицированная версия нужна там, где база данных сама входит в защищаемый контур.

Закрывает задачу импортозамещения СУБД для систем с требованиями ФСТЭК: прикладная совместимость, хранение данных и формальное соответствие защиты

Яндекс Браузер для организаций, расширенная версия

Браузер для управляемого доступа к веб-сервисам. Поддерживает централизованное развертывание, настройку политик и интеграцию с ИБ-инструментами.

Закрывает задачи контроля браузерного контура: политики доступа, управление расширениями, работа с веб-сервисами и снижение слепых зон на рабочих местах.

Программный комплекс «Стахановец»

Контролирует действия сотрудников, помогает выявлять утечки, проводить расследования и оценивать рискованное поведение пользователей.

Закрывает задачи внутренней безопасности: контроль инсайдерских сценариев, расследование инцидентов, фиксация действий пользователей и работа с рисками утечки данных.

MS_KEY

Программно-аппаратный комплекс для работы с ключевой информацией на базе интеллектуальных карт и носителей. Используется для защищенного хранения ключей и криптографических операций

Закрывает задачи доверенного доступа, электронной подписи, двухфакторной аутентификации и работы с ключами в регулируемых системах

Инвесткарта РФ

Платформа для поиска, сравнения и подбора инвестиционных площадок на территории России. В реестре ФСТЭК отражена сертификация конкретной прикладной системы

«Учет изменений в файловой системе» версия 1.0

ПО для фиксации изменений в файловой системе в конкретном государственном контуре. Открытой продуктовой страницы с описанием функций нет

Спасибо
за внимание!