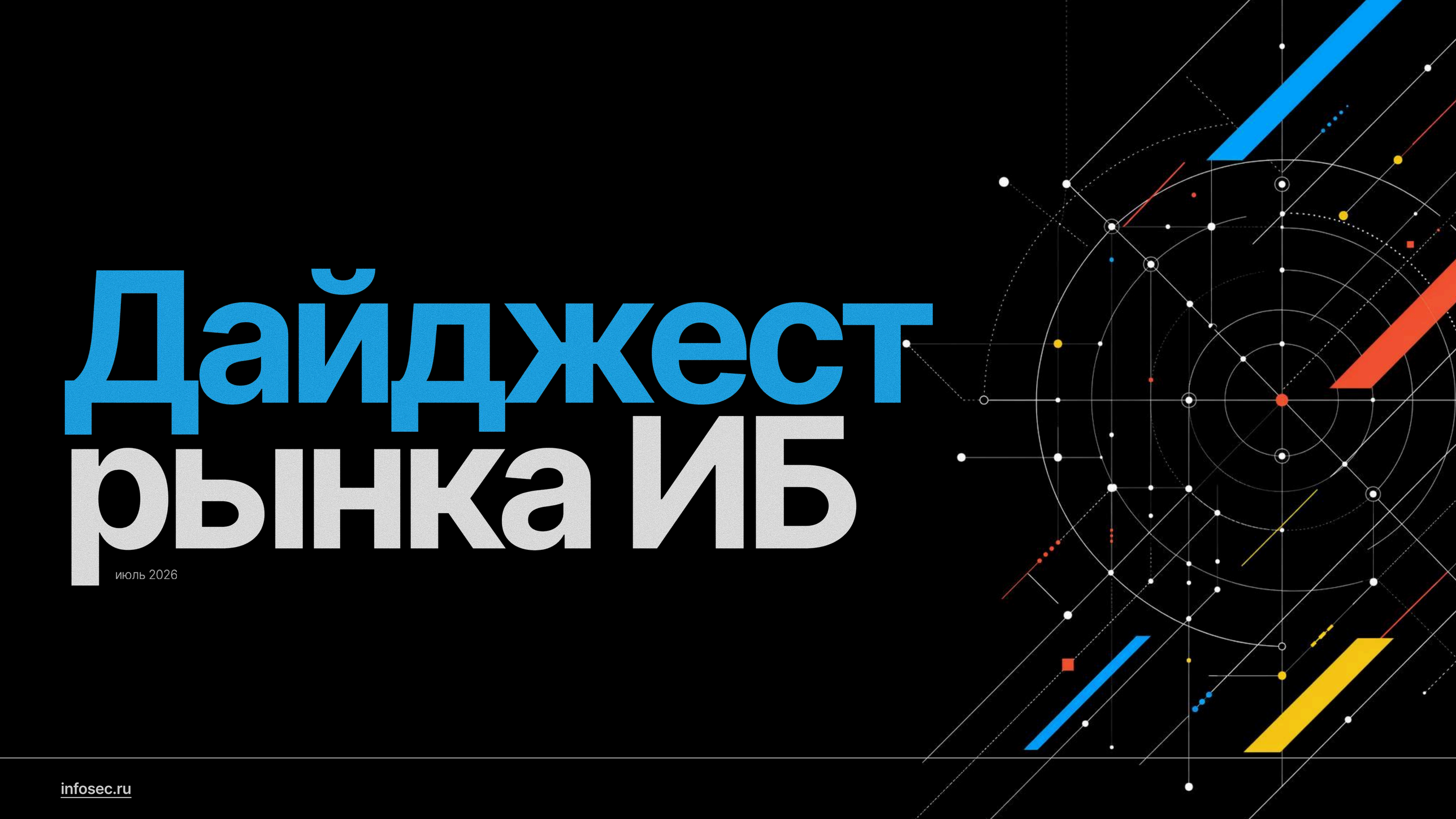
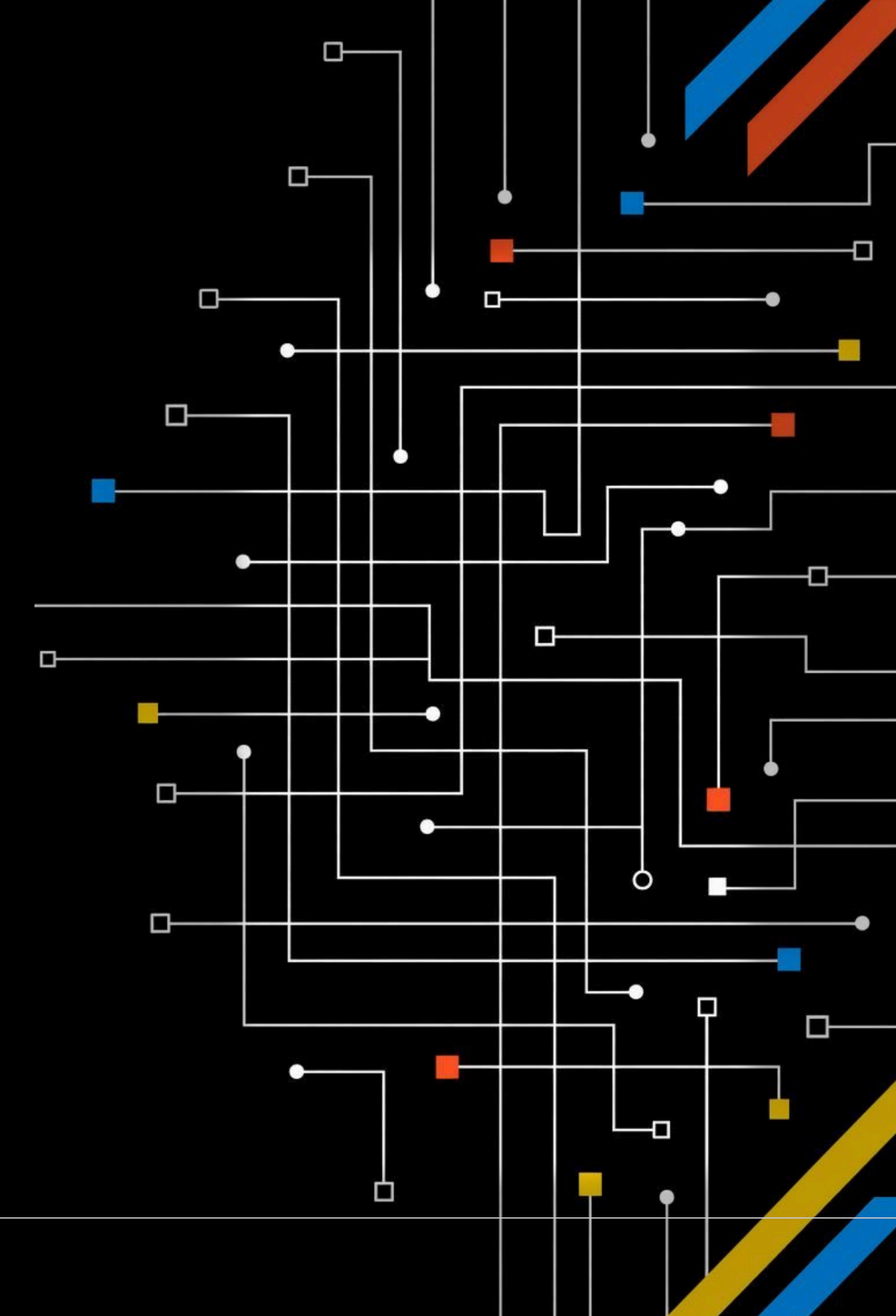
Дайджест рынка ИБ

июль 2026



Оглавление



03 Резюме

НКЦКИ и ФСТЭК детализируют требования к инцидентам, ИСПДн и сертификации

НКЦКИ установил форматы передачи данных об атаках и инцидентах в ГосСОПКА. ФСТЭК меняет порядок сертификационных испытаний и подготовила новые требования к защите персональных данных взамен приказа № 21. Для организаций это означает больше требований к качеству данных, процессам реагирования, управлению уязвимостями и доказательной базе защиты

Новые требования затрагивают размещение и устойчивость государственной ИТ-инфраструктуры

В июле вышли или обсуждались требования к хостингу внутренних систем госорганов, размещению баз данных и технических средств, ЦОД государственной облачной платформы и категорированию КИИ в ОПК. Заказчикам и провайдерам придется учитывать, где физически находятся компоненты системы, как резервируются связь и электропитание, кто предоставляет инфраструктуру и какие объекты входят в регулируемый контур.

ИИ: принят закон о фундаментальных моделях и подготовлен проект ГОСТ по безопасной разработке

Закон № 243-ФЗ вводит правовую рамку для больших фундаментальных моделей. Проект ГОСТ описывает безопасную разработку ПО с ИИ, включая работу с данными, моделями, зависимостями и тестированием. Единого обязательного режима AI Security пока нет, но круг вопросов, которые разработчикам и крупным заказчикам придется учитывать при создании и эксплуатации ИИ-систем, становится конкретнее.

Антифрод-проекты расширяют обмен данными между банками, операторами связи и государственными системами

Июльские проекты связывают данные банков, операторов связи, ЕСИА, телефонные номера и идентификаторы устройств. Они предусматривают проверку абонентов, выявление мошеннических номеров, обмен сведениями при возврате похищенных денег и привязку номера к конкретному устройству.

Для участников основная техническая задача — быстро сопоставлять данные из разных систем и сохранять историю решений так, чтобы можно было восстановить, на основании каких признаков операция или номер были признаны подозрительными.

Реестры Минцифры и ФСТЭК

Защита корпоративных ИИ-сервисов получила в июле сразу две позиции в реестре Минцифры. Innostage AIDR и AppSec.AIGate работают с запросами и ответами LLM и закрывают близкие задачи вокруг атак на модели и утечек данных.

Самый широкий набор ПО связан с доступом, учетными данными и ключевой инфраструктурой. Jim закрывает жизненный цикл пользовательских прав, dPAM - привилегированный доступ, T-Connect и Амиконнект - удаленные подключения. SomersLKM и продукты Clearway работают с ключами, сертификатами, СКЗИ и секретами.

В реестре ПАК восемь записей соответствуют четырем продуктовым группам. Три исполнения ФПСУ-Q и три варианта центров выработки ключей формируют основную часть обновления. ViPNet Coordinator IG 5 добавляет промышленную сетевую защиту, ВМШ-MUX-1U - шифрование высокоскоростных оптических каналов.

ФСТЭК расширила выбор базовых компонентов для защищенной инфраструктуры. Cloud X OS добавляет сертифицированную серверную платформу, сервисный маршрутизатор Истока - сетевой компонент в шести исполнениях. Print-X, комплекс Инфогорода и РАСЧЕТ ВЧО закрывают более прикладные и специализированные сценарии.

04 Резюме

PT NGFW становится одним из драйверов отгрузок, «Лаборатория Касперского» расширяет корпоративный стек

За I полугодие 2026 г. PT продала PT NGFW больше, чем за весь 2025 г. Компания относит продукт к основным драйверам отгрузок вместе с MaxPatrol SIEM и MaxPatrol VM.

«Лаборатория Касперского» вывела отдельный Kaspersky Vulnerability Management и существенно обновила Kaspersky NGFW для крупных распределенных инфраструктур.

Solar, ShiftLeft и CICADA8 переносят экспертизу в продукт и сервис

«Солар» встроил в Solar SIEM контент Solar JSOC, накопленный на проектах примерно 300 заказчиков. ShiftLeft предлагает SAST через MSSP с ручной проверкой и приоритизацией срабатываний. CICADA8 вывела автоматизированный пентест как продукт и услугу.

Заказчик получает готовые правила, проверку результатов или регулярное выполнение части ИБ-функции. Это снижает нагрузку на внутреннюю команду.

В июле появились готовые интеграционные связки для доступа, Kubernetes и АСУ ТП

«Актив», SafeTech Lab и Indeed объединили аутентификацию, сертификаты и управление доступом. Deckhouse и «Киберпротект» подготовили единый сценарий резервного копирования Kubernetes и виртуальной инфраструктуры. UDV Group и ДАТАРК встроили защиту АСУ ТП в готовый модульный ЦОД.

Во всех трех случаях часть интеграционной работы поставщики проводят заранее. Заказчику остается меньше отдельных стыковок между продуктами, а ответственность за работоспособность связки меньше распределяется между несколькими подрядчиками.

Число DDoS-атак выросло на 45%, их суммарная длительность — на 129%

Selectel за I полугодие 2026 г. зафиксировал рост числа DDoS-атак на 45% год к году. Их суммарная длительность увеличилась на 129%.

Длительность растет заметно быстрее количества атак. Для критичных цифровых сервисов поэтому важна не только максимальная мощность атаки, но и то, сколько времени защита и инфраструктура способны работать под постоянной нагрузкой.

ИИ становится одновременно новым активом для защиты и инструментом атакующего

В Solar 4RAYS число уязвимостей ИИ-сервисов выросло с 16 до 33 за квартал — более чем вдвое. Категория пока небольшая, но уже входит в обычный веб-стек и требует тех же процессов инвентаризации, VM и AppSec, что и другие корпоративные системы.

С другой стороны, BI.ZONE показывает, что ИИ уже используется для разведки, подготовки кода и автоматизации отдельных этапов атак. Полностью автономный взлом пока остается скорее исключением: основной эффект — повышение производительности квалифицированного атакующего.

Целевые атаки становятся сложнее для обнаружения по отдельным событиям

По данным PT за II квартал, APT-группировки используют многоступенчатые цепочки, в которых отдельные действия могут выглядеть как обычная активность. Среди техник — легитимные веб-сервисы и API, PowerShell, DLL Side-Loading и другие способы скрыть промежуточные этапы атаки.

Для заказчиков это повышает значение поведенческого анализа и корреляции событий между разными узлами инфраструктуры. Проверять нужно не только отдельные срабатывания средств защиты, но и последовательность действий пользователя, процесса или устройства.

05 Рекомендации

Для заказчиков	Для интеграторов и MSSP	Для вендоров
Подготовить SOC к новым форматам НКЦКИ. Проверить, откуда будут автоматически подтягиваться данные об объектах КИИ, владельцах, категориях и отрасли; связать уведомления с CMDB и внутренними реестрами.	**Подготовить типовой проект адаптации к требованиям НКЦКИ и новой модели ИСПДн**. В него могут входить обследование, нормализация справочников, интеграция SOC с CMDB, автоматизация уведомлений и оценка зрелости процессов.	**Проверить готовность разработки к новым испытаниям ФСТЭК**. Заранее собрать исходный код, зависимости, сведения о сборочной среде, документацию и результаты тестирования, которые потребуются лабораториям.
Пересмотреть приоритизацию уязвимостей. Добавить к CVSS эксплуатируемость, доступность актива извне, наличие рабочего эксплойта и критичность системы для бизнеса.	**Продавать интеграцию готовыми архитектурными сценариями.** В июле такие связки появились вокруг доступа, Kubernetes и АСУ ТП. Ценность интегратора — обследовать среду заказчика и довести совместимость продуктов до рабочей эксплуатации.	**Проверять совместимость до выхода в проект.** Совместные стенды, документированные конфигурации и готовые схемы интеграции снижают риск, что проблемы обнаружатся уже у заказчика.
Включить AI- и LLM-сервисы в AppSec и управление доступом. Инвентаризировать используемые модели, определить владельцев, проверить передачу чувствительных данных, журналирование и тестирование приложений.	**Расширять MSSP за пределы мониторинга SOC там, где есть собственная экспертиза.** Июльские кейсы показывают рабочие модели для SAST, автоматизированного пентеста и других задач, где заказчику нужен разбор результата, а не только инструмент.	**Для AI-продуктов заранее учитывать безопасную разработку и эксплуатацию модели.** Контролировать обучающие данные, зависимости, API, доступ к модели и тестирование на специфические атаки
Проверить устойчивость сервисов к длительным DDoS-атакам. Зафиксировать допустимый простой, проверить постоянную фильтрацию и провести сценарий восстановления вместе с ИБ, ИТ и владельцами сервиса.	**В инфраструктурных проектах связывать ИБ с восстановлением и отказоустойчивостью.** Kubernetes, ЦОД и промышленные объекты требуют одновременно прорабатывать резервное копирование, сетевую защиту, инженерную инфраструктуру и сценарии восстановления.	**Упаковывать накопленную экспертизу в продукт**. Готовые правила детектирования, контент, приоритизация и проверенные сценарии уменьшают объем ручной настройки и делают продукт проще в эксплуатации.

06 Регулирование

НКЦКИ установил форматы передачи сведений об атаках и инцидентах в ГосСОПКА

Приказ НКЦКИ от 14 июля 2026 г. № 2 определяет, какие сведения и технические параметры организации должны передавать в ГосСОПКА. Вместе с приказом опубликованы исходные данные для определения типа компьютерной атаки и правила автоматизированного взаимодействия с инфраструктурой НКЦКИ

Организациям нужно сопоставить внутреннюю классификацию инцидентов со справочниками НКЦКИ. В карточках SOC должны быть доступны сведения об объекте КИИ, его владельце, категории, местонахождении и отрасли. Часть этих данных хранится вне SIEM, поэтому автоматизация уведомлений потребует связи с CMDB, реестром объектов КИИ и организационными справочниками.

Стоит проверить шаблоны сообщений, правила назначения TLP-маркеров, порядок запроса помощи ФСБ и резервный ручной процесс на случай сбоя автоматического обмена. Для интеграторов это работа по настройке SOC, нормализации справочников и автоматизации отчетности.

ФСТЭК подготовила новые требования к защите персональных данных взамен приказа № 21

ФСТЭК вынесла на обсуждение проект приказа, который должен заменить действующий приказ № 21. Защита ИСПДн описывается через постоянные процессы: управление уязвимостями, конфигурациями и обновлениями, мониторинг ИБ, защиту удаленного доступа, безопасную разработку и непрерывность.

Проект вводит оценку достаточности и эффективности мер через показатель зрелости. Ее предлагается проводить перед началом обработки ПДн, не реже одного раза в три года и после инцидентов. Требования к зрелости распространяются и на организации, которым оператор поручает обработку данных.

Для заказчиков это означает более тесную связь ПДн-комплаенса с реальной эксплуатацией ИТ и ИБ, а не только с комплектом документов и СЗИ.

ФСТЭК меняет порядок сертификационных испытаний средств защиты с 1 августа

С 1 августа 2026 г. сертификация СЗИ по новым решениям ФСТЭК и испытания при внесении изменений должны проводиться по методике выявления уязвимостей и недекларированных возможностей, утвержденной 12 мая. Работы, начатые до этой даты, в отдельных случаях можно завершить по прежней методике.

Для разработчиков и лабораторий становится важнее доказательная часть сертификации: исходный код, зависимости, сборочная среда, документация и результаты тестирования.

Вендорам стоит заранее проверить готовность процессов разработки и материалов, передаваемых на испытания.

07 Регулирование

Федеральный закон № 243-ФЗ закрепил требования к большим фундаментальным моделям ИИ

26 июля подписан Федеральный закон № 243-ФЗ о поддержке развития технологий искусственного интеллекта. Он вводит понятия больших фундаментальных моделей, включая суверенные и национальные модели, определяет меры государственной поддержки и отдельные требования к разработчикам. Основные положения начнут действовать с 1 сентября 2026 года, часть требований вводится позже

Это не специализированный закон об ИБ искусственного интеллекта, но он впервые формирует отдельный регулируемый контур вокруг крупных моделей. Для разработчиков и заказчиков возрастает значение происхождения модели, инфраструктуры ее эксплуатации, работы с данными и последующих подзаконных требований.

Для рынка ИБ важнее всего дальнейшее развитие требований к защите самих моделей, данным, доступу, журналированию и безопасной эксплуатации.

Подготовлен стандарт безопасной разработки программного обеспечения с ИИ

Завершена первая редакция проекта ГОСТ Р по безопасной разработке ПО, реализующего технологии искусственного интеллекта. Он развивает требования ГОСТ Р 56939-2024 и переносит Secure SDLC на системы, где частью продукта становятся модели, обучающие данные и специализированная ИИ-инфраструктура.

В контур безопасности попадают не только исходный код приложения, но и наборы данных, модели и их параметры, библиотеки и фреймворки, API, среды обучения и тестирования. Предусматриваются моделирование угроз, контроль цепочки поставок, тестирование и безопасное сопровождение.

Для разработчиков это означает необходимость строить отдельный процесс управления рисками ИИ на всем жизненном цикле продукта. Пока речь идет о проекте стандарта, его требования еще не являются обязательными.

Уточнены правила трансграничной передачи ПДн и отдельные нормы по КИИ

Федеральный закон № 265-ФЗ меняет правила признания иностранных государств обеспечивающими адекватную защиту прав субъектов персональных данных. Для компаний это повод пересмотреть трансграничные потоки, включая зарубежные SaaS, облачные платформы, централизованные HR- и CRM-системы и другие сервисы, через которые данные российских граждан уходят за пределы страны.

Закон также позволяет Правительству до 2030 г. устанавливать на определенных Президентом территориях особенности применения отдельных положений 187-ФЗ. Речь идет о требованиях к использованию российского ПО и программно-аппаратных средств на значимых объектах КИИ

Конкретные территории, сроки и исключения пока не определены. Субъекты КИИ продолжают работать по действующим требованиям, пока Правительство не установит для них специальный режим.

08 Регулирование

С 1 сентября усилят контроль иностранных баз данных и технических средств

Постановление Правительства № 845 устанавливает порядок контроля за соблюдением запрета на использование размещенных за пределами России баз данных и технических средств в государственных, муниципальных и ряде корпоративных информационных систем. Новые правила начинают действовать с 1 сентября 2026 года.

Организациям нужно определить, какие системы и внешние инфраструктурные зависимости попадают в регулируемый контур. Речь идет не только о прямом использовании зарубежного облака: проверять придется архитектуру размещения данных и технических компонентов, используемых при эксплуатации системы.

Миграция затронет и ИБ-архитектуру: после замены СУБД или инфраструктуры придется перепроверять управление доступом, журналирование, резервирование, интеграции с СЗИ и мониторингом.

Внутренние системы госорганов включили в регулируемый контур хостинга

С 1 сентября требования к провайдерам хостинга распространятся не только на ГИС, но и на информационные системы, созданные госорганами для организационного, документационного, финансового и технического обеспечения собственной деятельности

Изменение закрывает заметный пробел: внутренняя система могла работать с чувствительной информацией, но формально не иметь статуса ГИС. Теперь при выборе инфраструктуры размещения такой формальный статус будет иметь меньшее значение.

Госорганам стоит инвентаризировать внутренние системы и используемых провайдеров. Для облачных и хостинг-компаний расширяется потенциальный государственный сегмент, но одновременно растет значение соответствия требованиям по защите, взаимодействию с ФСТЭК и ФСБ и работе с регулируемыми заказчиками.

Для оборонной промышленности уточнили категорирование объектов КИИ

С июля действуют отраслевые особенности категорирования объектов КИИ организаций оборонно-промышленного комплекса. **Постановление № 796** конкретизирует порядок определения значимости с учетом специфики отрасли и вводит дополнительные отраслевые признаки.

Среди них — использование объекта КИИ при выполнении государственного оборонного заказа, работе по договорам с военной приемкой и обеспечении функционирования опасных производственных объектов. Для предприятий это повод сопоставить новые критерии с действующими перечнями объектов и ранее проведенным категорированием.

Если исходные показатели или состав объектов изменятся, потребуется актуализировать решения комиссии и связанные документы. Для интеграторов основной объем работ будет связан с обследованием и последующим уточнением требований к защите.

09 Регулирование

Минцифры предложило требования к ЦОД государственной облачной платформы

Проект Минцифры определяет требования к центрам обработки данных, на которых размещается инфраструктура государственной единой облачной платформы. В проекте учитываются локализация ЦОД в России, резервирование каналов связи и электроснабжения, использование нескольких операторов, климатические системы и мониторинг инженерной инфраструктуры.

Для таких проектов ИБ фактически начинается ниже уровня программных средств защиты. Отказ канала, электропитания или системы охлаждения напрямую влияет на доступность государственных сервисов и поэтому становится частью общего контура устойчивости.

Операторам ЦОД и интеграторам нужно учитывать требования уже при проектировании площадки: отдельно проверять связность, резервирование инженерных систем, мониторинг, физическую защиту и сценарии восстановления.

Банк России дополнил модель угроз при работе банков с биометрическими данными

С 25 июля действует Указание Банка России № 7362-У. В перечень актуальных угроз добавлены риски при сборе биометрии сотрудниками банков с использованием портативных устройств и ее передаче во внутреннюю инфраструктуру. Регулятор отдельно учитывает подмену и удаление данных, компрометацию и внесение фиктивной биометрической информации.

Практически это расширяет защищаемый контур до мобильного рабочего места и канала, по которому данные попадают в банковскую систему. Банкам стоит проверить доверенность устройств, контроль целостности, шифрование каналов, аутентификацию сотрудников и журналирование операций.

Для микрофинансовых организаций уточнены угрозы при работе со сведениями о степени соответствия биометрических образцов.

Минцифры предложило единую систему противодействия ИКТ-преступлениям до 2035 года

Проект Доктрины Минцифры задает долгосрочную модель противодействия преступлениям с использованием ИКТ. В нее должны быть глубже включены государственные органы, банки, операторы связи, цифровые платформы и другие организации. Реализация рассчитана на три этапа до 2035 года.

Для рынка важен сам переход от набора отдельных антифрод-мер к межотраслевой системе. В документе рассматриваются оперативный обмен данными, отраслевые стандарты антифрода, аудит, оценка фрод-потенциала информационных систем и развитие цифровых доказательств.

Доктрина пока не создает прямых обязанностей. Это рамка, из которой в последующие годы должны появляться отдельные законы, подзаконные акты и технологические механизмы.

10 Регулирование

Минцифры определяет признаки мошеннических номеров и порядок возврата денег

Два июльских проекта развивают механизм взаимодействия банков и операторов связи. Первый устанавливает критерии, по которым номер может быть отнесен к используемым для противоправных действий или, наоборот, к номерам потенциальных жертв. Второй определяет порядок обмена сведениями между банком и оператором при рассмотрении вопроса о возмещении похищенных средств.

Антифрод все меньше ограничивается анализом банковской транзакции. Для принятия решения приходится сопоставлять перевод, телефонный номер, историю звонков и сообщений и данные разных участников.

Банкам и операторам понадобятся надежные интеграционные каналы, синхронизация временных меток, единые идентификаторы и прозрачное журналирование решений. Для ИБ-интеграторов это прежде всего проекты обмена данными и оркестрации процессов.

Идентификацию абонента хотят связать с ЕСИА и конкретным устройством

Еще два проекта дополняют антифрод-контур идентификационными данными. Предлагается повторно проверять сведения об абоненте после изменения его данных в ЕСИА, а также развивать базу идентификаторов пользовательского оборудования и порядок взаимодействия операторов с этой базой.

Это делает идентификацию не разовой процедурой при заключении договора, а поддерживаемым состоянием. Антифрод получает возможность связывать человека, номер телефона и используемое устройство и отслеживать изменения этой связки.

Для операторов ключевыми станут качество идентификационных данных, обработка расхождений и автоматизация повторной проверки. Для ИБ-систем устройство становится дополнительным устойчивым признаком, который можно использовать при корреляции телеком- и финансовых событий.

ФАС меняет подход к контролю иностранных инвестиций в ИТ- и ИБ-компаниях

ФАС продолжает корректировать проект поправок к законодательству о стратегических инвестициях. В актуальной версии к стратегическим направлениям предлагается относить, в частности, деятельность по технической защите конфиденциальной информации, при этом ряд ранее обсуждавшихся ИТ-направлений - ЦОД, цифровые платформы, разработка ИИ и доверенного российского ПО - не включен в жесткий перечень.

Речь идет о порядке корпоративных сделок с иностранным участием. Для компаний из попадающих в перечень сфер приобретение иностранным инвестором контроля может требовать дополнительного согласования.

11 Новости компаний

Информзащита

+46% рост числа атак с использованием ботов за 1 пг 2026г к 1 пг 2025г

58% организаций не могут уверенно установить, какие уязвимости с наибольшей вероятностью будут использованы в реальных атаках. На практике это означает, что список из тысяч CVE не превращается в список из 5-10 реально опасных точек входа.

77% закладывают на восстановление всей ИТ-инфраструктуры из резервных копий более четырех часов.

32% уязвимостей, обнаруженных при пентестах AI- и LLM-приложений, относятся к высокорисковым. По всем классам активов тот же показатель составляет около 12%, поэтому риск-профиль AI-приложений в 2,7 раза выше среднего.

Positive Technologies

Финансовые результаты за 1 пг 2026: рост сформировали новые отгрузки, PT NGFW становится отдельной продуктовой опорой

+45% отгрузки PT г/г

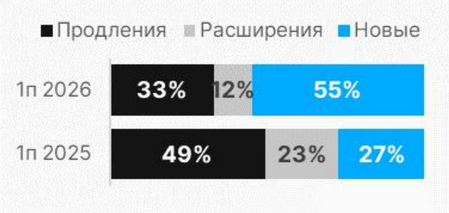
55% новые отгрузки в структуре

12% доля PT NGFW в R&D PT

Среди основных драйверов компания называет MaxPatrol SIEM, MaxPatrol VM и PT NGFW.

Структура отгрузок

Доля новых отгрузок: 27% → 55% (+28 п.п.)



Ключевые факты

Отгрузки: 10,7 млрд руб. (+45% г/г)

Новые отгрузки: 2,02 → 5,86 млрд руб.

Общий прирост: +3,31 млрд руб.

Отгрузки PT NGFW за шесть месяцев уже превысили показатель за весь 2025 г.

«Лаборатория Касперского»

«Лаборатория Касперского» расширяет корпоративный стек: отдельный VM-продукт и усиление NGFW

«Лаборатория Касперского» вывела на российский рынок Kaspersky Vulnerability Management - отдельный продукт для поиска, приоритизации и контроля устранения уязвимостей. Решение рассчитано на инфраструктуры от 10 устройств

Kaspersky NGFW получил крупнейшее обновление с момента запуска. Старшая платформа рассчитана на производительность до 140 Гбит/с в режиме NGFW, появились виртуальные контексты и функции для крупных распределенных инфраструктур

12 Новости компаний

ГК «Солар»

Solar SIEM: сервисная экспертиза SOC становится частью продукта

В Solar SIEM 2026.2 встроен полный набор контента Solar JSOC, сформированный на практике мониторинга и расследований примерно у 300 заказчиков. Добавлены Threat Intelligence, мультитенантность для холдингов и MSSP и расширенный ИИ-агент.

SIEM все больше продается как связка платформы, готового контента и экспертного знания. Вендоры с собственной большой SOC-практикой получают дополнительное преимущество: сервисная статистика и опыт расследований становятся сырьем для продукта.

Для интеграторов меньше ценности остается в простой установке платформы. Больше - в подключении источников, нормализации активов, настройке процессов SOC и интеграции мониторинга с реальным реагированием.

CICADA8

CICADA8: автоматизированный пентест переходит из эксперимента в коммерческий сервис

CICADA8 представила ИИ-пентестер для автоматизированной проверки внешнего периметра, веб-приложений и API. Разработчик заявляет анализ сценариев авторизации и ошибок бизнес-логики. Решение продается как модуль платформы и как услуга, в том числе для регулярной проверки.

Infosecurity

CYBERID: цифровой след руководителя становится отдельным объектом ИБ

Infosecurity запустила CYBERID - сервис для защиты цифрового следа собственников, руководителей и других ключевых сотрудников. Он ищет в открытых источниках сведения, которые могут использоваться для фишинга, социальной инженерии и атак на личные учетные записи.

K2Tex+K2 Кибербезопасность

Физическая, инженерная и кибербезопасность промышленного объекта собираются в один проект

K2Tex и K2 Кибербезопасность запустили единую услугу защиты промышленных объектов. В один проект объединены физическая безопасность, инженерные системы, защита АСУ ТП и КИИ, SOC-мониторинг и дальнейшее сопровождение.

Интеграторы расширяют ИБ-проекты в сторону непрерывности промышленного объекта. Чем больше контуров входит в один контракт, тем выше роль отраслевой экспертизы, проектирования и длительного сервиса.

Для промышленной компании главный эффект такой модели - меньше разрывов ответственности между физической безопасностью, АСУ ТП и ИБ. Для рынка это переход от поставки средств защиты к длинному инфраструктурному контракту.

13 Новости компаний

Актив+SafeTech Lab+ Indeed

Интеграционная работа вокруг доступа переносится в готовую платформу

Актив, SafeTech Lab и Indeed объединили аппаратную аутентификацию, корпоративный удостоверяющий центр, управление ключевыми носителями и политики доступа в единой Платформе управления доступом

После основной волны импортозамещения ценность смещается от наличия российских компонентов к готовым совместным архитектурам. Вендоры, которые заранее собирают и поддерживают связки, уменьшают стоимость внедрения и получают преимущество в проектах с ограниченными ресурсами заказчика.

Для крупной компании готовая связка доступа снижает риск, что ответственность за сертификаты, носители и аутентификацию окажется разнесена между несколькими поставщиками.

UDV Group+ДАТАРК

Киберзащита встроена в готовый модульный ЦОД (МЦОД)

UDV Group и ДАТАРК представили модульный ЦОД, где заранее объединены мониторинг ИТ-инфраструктуры, инженерных систем и защита АСУ ТП. За инженерный контур отвечает DATCHECK, за ИТ-мониторинг — UDV ITM, за кибербезопасность технологического сегмента — UDV DATAPK Industrial Kit.

ShiftLeft Security+УЦСБ

ShiftLeft Security начала предоставлять SASTAV через MSSP, включая УЦСБ

Провайдер берет на себя запуск анализа, ручную проверку срабатываний, приоритизацию проблем и повторное тестирование после исправлений.

Сервисная модель AppSec начинает повторять путь SOC и MDR: специализированную ИБ-функцию можно передать внешнему провайдеру

Deckhouse+Киберпротект

Единый сценарий резервного копирования для Kubernetes и виртуальной инфраструктуры

Для Kubernetes резервной копии данных недостаточно: при восстановлении нужны конфигурация кластера, метаданные и инфраструктурный контекст. Партнерство закрывает один из эксплуатационных барьеров при переносе критичных систем в отечественную контейнерную среду.

Positive Technologies+Netwell

Широкому продуктовому портфелю нужен инженерный канал продаж

Netwell стал официальным дистрибьютором всего продуктового портфеля PT и создает отдельную инженерную команду для поддержки партнеров, пилотов и сложных внедрений.

14 Тенденции

«АйТи Бастион» / Piccard

PAM для МСБ требует другой продуктовой и коммерческой модели

540+ млн ₽ — текущий объем сегмента PAM в российском МСБ

1,2 млрд ₽ — потенциальная емкость в год PAM в сегменте МСБ

Где появляется спрос

Спрос возникает в точке, где привилегированный доступ влияет на контракт или сохранность актива

- ✓ **Контроль подрядчиков** — запись действий
- ✓ **Требования заказчиков** — аудит доступа
- ✓ **Защита активов** — код, базы, документы
- ✓ **Учетные записи** — права, роли, MFA

Solar 4RAYS

Обзор сетевых уязвимостей в 2-м квартале 2026 года

+60% — **количество обнаруженных уязвимостей** во 2кв 2026 года по сравнению с 1 кв 2026 года: с 426 до 681.

84% — обнаруженных уязвимостей имели сетевой вектор, как и в 1 кв 2026

7,9 — средний уровень критичности обнаруженных сетевых уязвимостей (CVSS). В первом квартале — 8,1.

90% — всех обнаруженных сетевых уязвимостей эксплуатируются через HTTP

74% — в совокупности занимают сетевые уязвимости уровня Critical и High

ИИ-сервисы: 16 → 33 уязвимости

Категория пока небольшая, но уже становится частью обычного контура управления уязвимостями.

Уязвимостей больше, средняя критичность не выросла

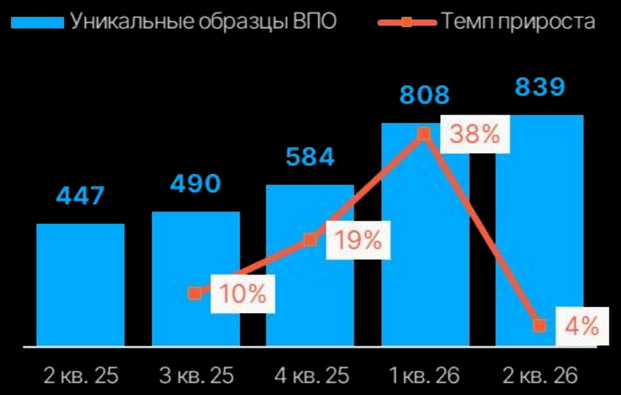
Это повышает роль приоритизации по эксплуатируемости и критичности актива, а не только по CVSS

15 Тенденции

Positive Technologies

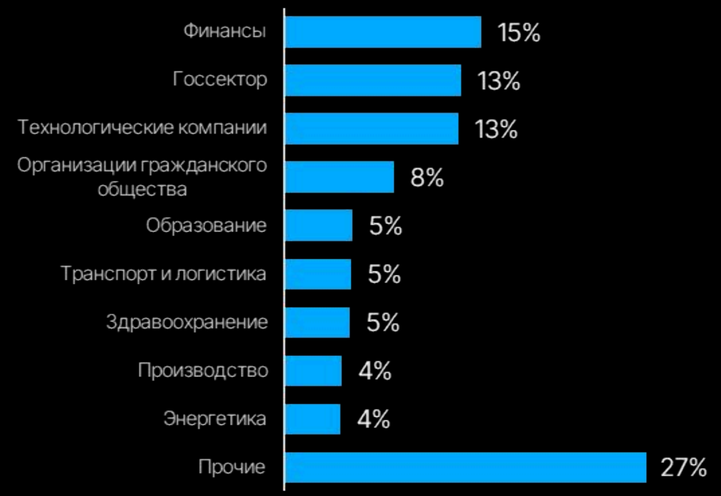
Анализ активности хакерских группировок, 2 кв. 2026 г.

Динамика уникальных образцов APT-группировок по кварталам



60% всех образцов ВПО обеспечили пять наиболее активных группировок

Наиболее атакуемые сектора экономики, Q2 2026



Техническое усложнение атак

Во 2-м квартале 2026 года хакерские группировки перешли от прямого заражения к многоступенчатым цепочкам, где каждый этап маскируется под легитимную активность. Это меняет экономику защиты: сигнатурные и периметровые средства срабатывают хуже, а цена ошибки растет - и по времени обнаружения, и по размеру ущерба

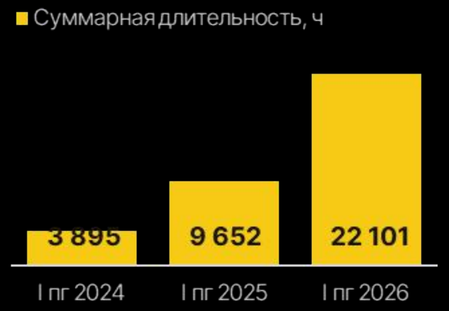
Практические шаги

- **Пересмотреть KPI безопасности.** Сместить акцент с количества заблокированных доменов на время обнаружения аномального поведения и долю endpoint с поведенческим детектированием.
- **Инвестировать в EDR/XDR с поведенческим анализом:** традиционные антивирусы не видят блокчейн-резолверы, oEmbed-цепочки и DLL Side-Loading
- **Внедрить контроль за PowerShell и скриптами:** логирование всех запусков PowerShell, особенно с зашифрованными командами и обращениями к Chrome/DPAPI
- **Усилить сегментацию сети:** ограничить доступ рабочих станций к публичным API (блокчейн-обозреватели, WordPress/oEmbed) только через прокси с глубоким анализом параметров
- **Провести red team с новыми техниками:** проверить, детектируются ли атаки с использованием oEmbed, блокчейн-резолверов и DLL Side-Loading в вашей среде

16 Тенденции

Selectel

Аналитика о DDoS-атаках за 1 пг 2026



+45% атак в 1 пг 2026г к 1 пг 2025г

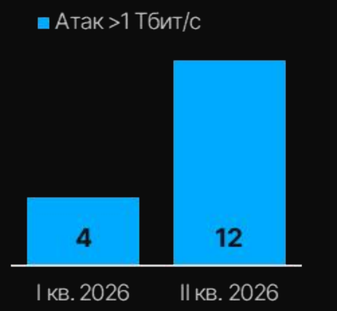
+129% суммарной длительности атак в 1 пг 2026г к 1 пг 2025г

Практические шаги

- Определить допустимый простой критичных цифровых сервисов
- Проверить защиту сети, веб-приложений и API вместе.
- Проверить постоянную фильтрацию и порядок эскалации
- Провести учение по потере доступности с ИБ, ИТ и владельцами процессов.

CURATOR

DDoS, боты и BGP-инциденты во 2 квартале 2026 года



Отраслевой разрез

ОБНОВЛЕНИЕ

17 Реестр Минцифры: ПО

Амиконнект для Windows, macOS и Linux, №34330, 34331, 34549

Организует защищенное подключение пользователей и разграничивает сетевой доступ к корпоративным ресурсам.

Innostage AIDR, №34483

Анализирует запросы и ответы LLM, выявляет атаки на модель и утечки чувствительных данных.

SomersLKM, №34440

Обеспечивает защищенную загрузку криптографических ключей в платежные терминалы.

KarmaGate, №34430

Поддерживает тестирование веб- и мобильных приложений, анализ запросов, API и поиск уязвимостей.

Jim, №34416

IDM-система для централизованного управления доступом и автоматизации жизненного цикла учётных записей.

Мастер ПДн, №34402

Автоматизирует учет процессов обработки персональных данных и подготовку связанной документации.

FixCPT, №34398

Отслеживает внешние ИТ-активы и изменения инфраструктуры, доступной из интернета

NTA eSensor, №34374

Анализирует сетевой трафик, выявляет подозрительную активность и сохраняет данные для расследований.

Метла, №34299

Средство гарантированного уничтожения информации на носителях.

AppSec.AIGate, №34280

Контролирует обращения к LLM, выявляет атаки и утечки и позволяет блокировать или маскировать данные.

Облачная платформа Квантум, №34162

Предоставляет функции защиты сетевого периметра в облачной сервисной модели.

СМИОК, СУУ СКЗИ и Единое хранилище секретов, №34133, 34132, 34131

Три модуля Clearway закрывают управление сертификатами, учет СКЗИ и централизованное хранение секретов.

Diamond NEXT, №34092

Объединяет межсетевое экранирование, предотвращение вторжений, VPN и контроль сетевого трафика.

dPAM, №34089

Управляет привилегированным доступом к информационным ресурсам.

T-Connect, №34080

Организует контролируемое удаленное подключение пользователей к корпоративным ресурсам.

ОБНОВЛЕНИЕ

18 Реестр Минцифры: ПАК

ФПСУ-Q версии 4 - 3 исполнения, №34332, 34333, 34334

В реестр вошли исполнения HSTB-ULT8.1, MAX8.1 и HSTB-MAX8.1. ФПСУ-Q защищает сетевой обмен и поддерживает сценарии с квантовым распределением ключей.

Закрывает задачи защиты соединений между офисами и ЦОД и построения распределенных защищенных сетей

Центры выработки ключей ФПСУ - 3 варианта, исполнение ORD4.2, №34339, 34348, 34349

В реестр вошли центры для ФПСУ версии 3, ФПСУ-INT версии 3 и ФПСУ версии 4.

Формирование ключевой информации для аутентификации и защищенного взаимодействия комплексов ФПСУ

ViPNet Coordinator IG 5, №34335

Индустриальный шлюз объединяет межсетевое экранирование, VPN и контроль сетевого взаимодействия.

Обеспечивает сегментацию технологических сетей и защищенное взаимодействие промышленных и корпоративных сегментов.

ВМШ-MUX-1U, №34336

Аппаратный модуль защищает оптические каналы передачи данных со скоростью до 100 Гбит/с.

Закрывает задачи шифрования магистральных соединений между ЦОД и территориально разнесенными площадками.

ОБНОВЛЕНИЕ

19 Реестр ФСТЭК

Сервисный маршрутизатор НПП Исток - 6 исполнений

Сертификат распространяется на шесть исполнений. Оборудование сочетает маршрутизацию, VPN и функции межсетевого экранирования

Защита сетевого периметра и сегментация систем с требованиями к сертифицированным межсетевым экранам.

Print-X

Контролирует выдачу заданий на печать и позволяет аутентифицировать пользователя перед получением документа.

Обеспечивает снижение риска доступа посторонних к распечатанным документам и централизованный контроль корпоративной печати.

Cloud X OS

Серверная операционная система со встроенными механизмами защиты от несанкционированного доступа.

Базовая серверная платформа для информационных систем с формальными требованиями к защите.

Программный комплекс идентификации и аутентификации пользователей ГКУ Инфогород

Специализированное ПО для идентификации и аутентификации пользователей.

Контроль доступа пользователей в конкретном государственном информационном контуре.

РАСЧЕТ ВЧО

Рассчитывает показатели эффективности защиты речевой информации от утечки за счет высокочастотного облучения.

Оценка защищенности при специальных исследованиях технических каналов утечки речевой информации.

Спасибо
за внимание!