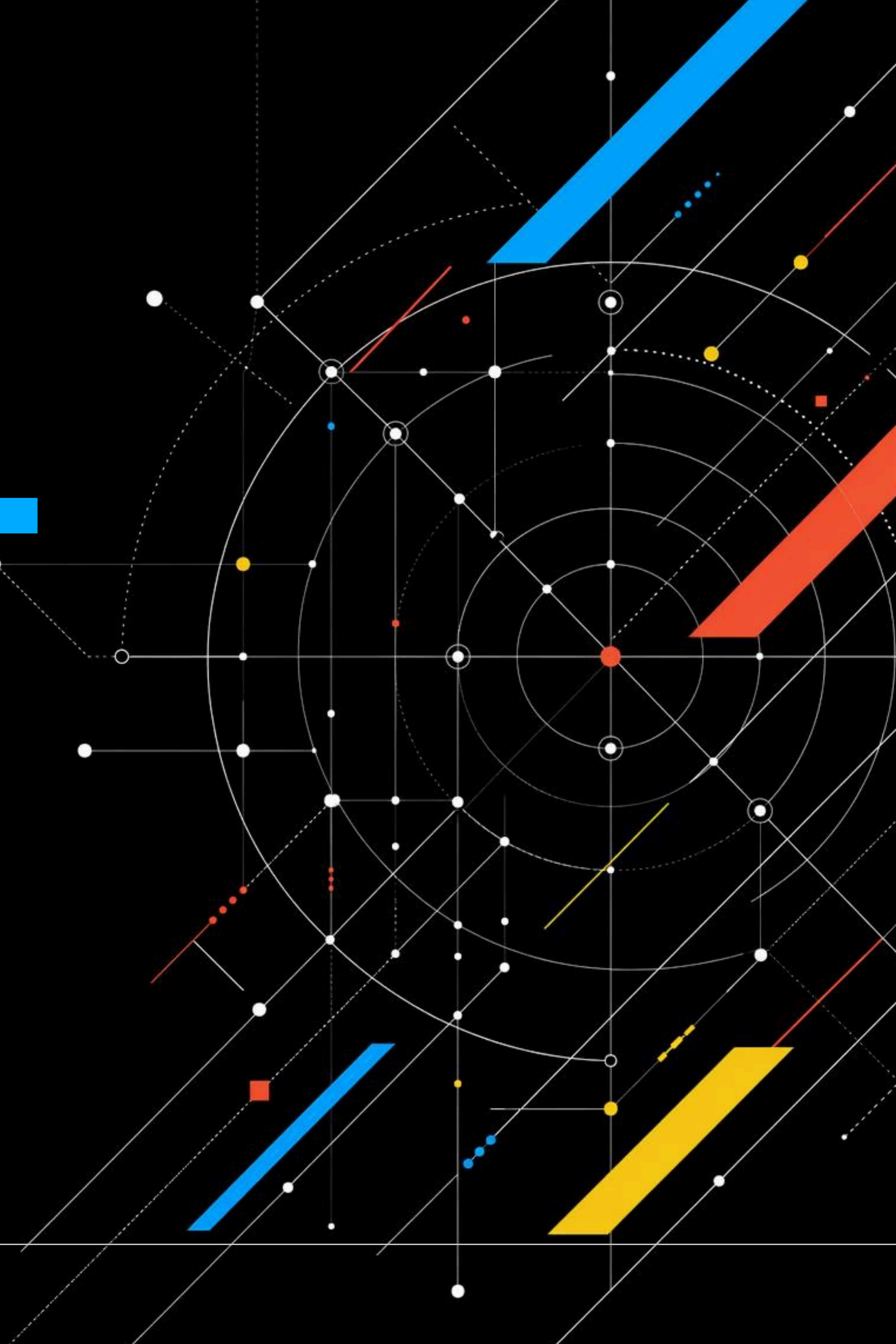


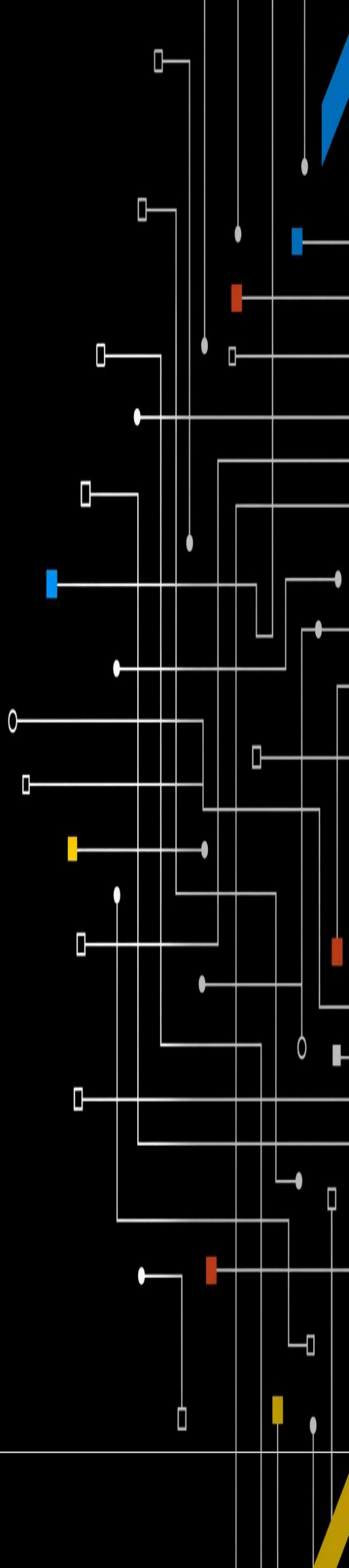
Дайджест рынка ИБ

Август 2026



02 Оглавление

03–04	Резюме
05	Рекомендации
06–11	Регулирование
12–15	Новости компаний
16–18	Тенденции
19–20	Сотрудничество
21	Реестры Минцифры
22	Реестр ФСТЭК



03 Резюме

Госсистемы: оценка подрядчика и условия работы внешнего сервиса

С 1 марта 2027 года приказ ФСТЭК №137 требует оценивать зрелость защиты подрядчика до предоставления ему доступа к госсистеме.

Постановление №1024 с 1 сентября 2026 года обязывает закреплять в договоре восстановление, резервное копирование и возврат данных.

Приказ ФСБ №321 распространяет требования к криптозащите на внешние сервисы госсистем.

Для цифровых депозитариев готовят требования к защите ключей

Закон №282-ФЗ вводит цифровые депозитории: они учитывают цифровые валюты и обеспечивают доступ к активам. Для допуска Банк России проверяет защиту информации и операционную надежность.

Положение №890-П предусматривает внешнюю оценку ИБ и аппаратные модули для ключей к адресам, которыми управляет депозитарий. На 9 сентября документ еще проходил регистрацию в Минюсте.

ФСТЭК уточнила содержание оценки зрелости и аттестации

Методика от 7 августа проверяет 21 направление защиты по восьми критериям, включая результаты работ и независимость контроля.

С 1 сентября приказ №60 включает анализ уязвимостей в аттестацию. Пентест требуется для госсистем и других ИС госорганов, ГУПов и госучреждений классов 1–2 при подключении к интернету или взаимодействию с другими системами; для второго случая предусмотрено исключение при сертифицированной криптозащите.

Обновления SOC: блокировка атак и контроль поступления событий

В MaxPatrol 360 и PT NAD аналитик может изолировать узел через EDR или инициировать блокировку сетевого трафика. Kaspersky MDR сообщает, когда от актива перестают поступать данные.

Для охваченных приказом ФСБ №297 государственных систем с 1 сентября действует срок уведомления Национального координационного центра по компьютерным инцидентам (НКЦКИ): 24 часа с обнаружения инцидента. Это нужно учитывать в договоре с внешним SOC.

04 Резюме

WMX и BI.ZONE описывают многоэтапные атаки и повторное использование доступов

В I полугодии 2026 года 44% веб-атак в наблюдениях WMX и ServicePipe были многоэтапными: DDoS мог отвлекать защиту от атаки на приложение.

BI.ZONE отмечает повторное использование фишинговых доменов, продажу сессий и токенов. Поэтому при утечке пароля важно отозвать уже выданные сессии и токены: смена пароля не всегда прекращает доступ.

Солар, Yandex Cloud и Ideco: результаты I полугодия

В I полугодии 2026 года к I полугодю 2025-го выручка Солара от сервисов и комплексных проектов выросла на 21%, общая выручка — на 13,2%.

За те же периоды доля крупных клиентов Yandex Cloud с ИБ-сервисами выросла с 44% до 53%. Рентабельность Ideco по EBITDA повысилась с 28% до 33%, но первое полугодие 2026 года компания закончила с чистым убытком.

Проверены хранение событий KUMA и передача файлов из PAM

KUMA и VK Object Storage испытали на архиве 3 ПБ при нагрузке более 6 тыс. запросов в секунду. Интеграция Innostage PAM с PT Sandbox позволяет проверить файл до его передачи на сервер.

Также подтверждена совместимость продуктов BI.ZONE с Postgres Pro, InfoWatch с Deckhouse и R-Vision VM со «Штурвалом».

Локальные языковые модели ищут пароли и разбирают инциденты

PT Dephaze использует локальную языковую модель для поиска учетных данных в файлах. Innostage TDIR помогает разобрать сведения из SIEM и подготовить рекомендации по инциденту.

Проект ФСТЭК от 24 августа предлагает выделять модели ИИ в отдельный сегмент госсистемы, ограничивать права агентов и регистрировать их действия. Эти меры пока обсуждаются.

05 Рекомендации

Для заказчиков	Для интеграторов и MSSP	Для вендоров
Запросите у подрядчика результаты оценки зрелости его защиты до открытия доступа к госсистеме. С 1 марта 2027 года приказ №137 связывает доступ с оценкой зрелости; получение результатов стоит заранее включить в договор сопровождения.	Разделите оценку зрелости и аттестацию в программе работ. У первой новая методика ФСТЭК с 21 направлением; у второй с 1 сентября действуют изменения приказа №60, включая пентест госсистем и других ИС госорганов, ГУПов и госучреждений классов 1–2 при указанных в нем условиях.	Для LLM-функций покажите, какие данные остаются внутри заказчика. В PT Dephaze модель анализирует конфигурации с возможными паролями. В демонстрации продукта стоит раскрыть хранение этих данных и доступ к ним.
Пересмотрите сроки уведомления от внешнего SOC. Приказ ФСБ №297 дает охваченным им системам 24 часа с обнаружения инцидента. Согласование с подрядчиком должно уложиться в эти 24 часа.	В договоре внешнего сервиса госсистемы задайте сроки восстановления и возврата данных. Постановление №1024 требует такого регламента; о мерах при сбое поставщик сообщает в течение трех часов после обнаружения сбоя защиты, если регламент не установил иной срок.	Добавьте контроль потери телеметрии в сценарии SOC. Такой контроль появился в Kaspersky MDR: прекращение поступления данных от узла должно быть заметно аналитику, даже когда событий атаки нет.
После утечки учетных данных отзывайте сессии и токены скомпрометированной учетной записи вместе со сменой пароля. BI.ZONE описывает их продажу на теневых ресурсах: действующая сессия может сохранить доступ к сервису после смены пароля.	В архиве SIEM разделите требования к поиску по свежим событиям и емкости холодного архива. В испытаниях KUMA с VK Object Storage использовали архив 3 ПБ с приростом 10 ТБ в сутки; оперативные события оставались на быстром хранении.	Сопровождайте заявленную совместимость результатами испытаний. Пример KUMA и VK Object Storage содержит объем архива и нагрузку; пример Innostage PAM и PT Sandbox — проверенные способы передачи файлов.
В пилоте системы управления уязвимостями (VM) проверьте устранение одной реальной уязвимости. Включите в пилот передачу задачи ИТ, исправление и повторное сканирование. В опросе R-Vision партнеры выделили именно сложности работы после обнаружения.	При проектировании цифрового депозитария определите, какие адреса хранения он будет администрировать. №890-П предусматривает аппаратные модули для управляемых им адресов и внешнюю оценку ИБ. На 9 сентября документ находился на регистрации.	Сверьте инструменты испытаний с августовскими перечнями ФСТЭК. Для разработки программных средств защиты названы статический анализ, фаззинг и динамический анализ. Укажите в плане оснащения инструменты для своих лицензируемых работ.

06 Регулирование

Проверки систем и подрядчиков

Доступ подрядчиков к госсистемам: приказ ФСТЭК №137

Приказ ФСТЭК №137 опубликован 11 августа. Основные изменения действуют с 1 сентября 2026 года, новая редакция пункта 32 приказа №117 — с 1 марта 2027 года.

С марта подрядчик оценивает зрелость своей защиты до получения доступа и затем не реже раза в два года. Показатель защищенности Кзи уже оценивают раз в полгода по приказу №117; результаты этой оценки направляют во ФСТЭК в течение пяти рабочих дней после оценки.

Оператору нужно получать результаты оценки до открытия доступа и закрепить подтверждение зрелости в договоре сопровождения.

ФСТЭК: новая методика оценки зрелости

Методика ФСТЭК от 7 августа охватывает защиту информации в ИС и безопасность значимых объектов КИИ. В ней 21 направление и восемь критериев для каждого. Неприменимые направления исключают из расчета.

Проверяют документы и выполнение процесса, инструменты, квалификацию сотрудников, контроль, обучение, внешний аудит и актуализацию. Одного регламента недостаточно: нужны подтвержденные результаты работ.

Самооценку организуют так, чтобы сотрудники не проверяли функции, которые выполняют сами. Оператору потребуется разделить исполнение и контроль либо привлечь внешнего исполнителя.

Аттестация систем: анализ уязвимостей и пентест

Приказ ФСТЭК №60 опубликован 25 июня и действует с 1 сентября. Анализ уязвимостей включен в аттестационные испытания.

Пентест обязателен для госсистем и иных систем госорганов, ГУПов и госучреждений классов 1–2 при подключении к интернету либо взаимодействию с другими системами. Исключение для сертифицированной криптозащиты относится только к межсистемному взаимодействию.

После аттестации контроль проводят не реже раза в три года; результаты направляют во ФСТЭК в течение пяти рабочих дней после контроля.

07 Регулирование

Внешние сервисы и уведомления об инцидентах

ФСБ: 24 часа на сообщение об инциденте

Приказ ФСБ №297 опубликован 21 августа и действует с 1 сентября. Он регулирует взаимодействие с ГосСОПКА систем госорганов, ГУПов и госучреждений.

Сведения об обнаруженном инциденте передают в НКЦКИ в течение 24 часов. Основной канал — личный кабинет; на случай технического сбоя предусмотрены резервные способы обмена.

Срок отсчитывается от обнаружения. Заказчику внешнего SOC нужно сопоставить сроки уведомления и согласования с этими 24 часами, определить отправителя первичного сообщения и сведения, доступные дежурной смене.

Криптозащита внешних сервисов: приказ ФСБ №321

Приказ ФСБ №321 опубликован 31 августа и действует с 11 сентября. Он заменяет приказ №117 от 18 марта 2025 года.

Требования охватывают криптозащиту госсистем и используемых ими внешних ресурсов, программ и баз данных. Для гостайны и специально перечисленных систем действует другой порядок. Класс СКЗИ внешнего сервиса должен соответствовать требованиям системы или ее сегмента.

Оператору нужно проверить схему соединения, управление ключами, доступы и журналы у провайдера. Внутренний контроль соблюдения требований проводят не реже раза в три года.

Внешние сервисы госсистем: обязанности сторон

Постановление №1024 действует с 1 сентября. Регламент работы госсистем с внешним сервисом включают в закупку и договор: ответственность, восстановление, резервные копии и возврат данных.

О сбое защиты стороны уведомляют друг друга незамедлительно. Поставщик сообщает о мерах не позднее трех часов после обнаружения сбоя, если регламент не установил иной срок. О соисполнителях уведомляют не позднее чем за три рабочих дня до начала их работы; передача им ограниченной информации требует письменного согласия заказчика.

Отдельный приказ Минцифры №702 устанавливает требования к хостинг-инфраструктуре с 1 марта 2027 года.

08 Регулирование

Ведомственные системы, ИИ и персональные данные

Правительство определило правила для ведомственных систем вне режима ГИС

Постановление №1007 действует с 1 сентября. Оно касается внутренних организационных, документационных и финансовых систем госорганов, которые не относятся к ГИС.

Для создания систем используют ПО и ПАК из национального фонда либо российских и евразийских реестров с отметкой «соответствует стандартам». Если подходящего решения или стандарта нет, собственная разработка требует обоснования и положительного заключения Минцифры; срок согласования — 20 рабочих дней.

Одной записи в реестре недостаточно. ТЗ должно учитывать угрозы и защиту ПДн. Для систем госорганов Москвы обязательны только отдельные пункты требований.

Проект ФСТЭК: защита моделей ИИ и права агентов

Проект ФСТЭК от 24 августа предлагает отдельный сегмент для моделей ИИ в госсистемах, усиленную многофакторную аутентификацию привилегированного доступа, минимальные права и регистрацию действий.

Для моделей с ограниченной информацией или значимыми функциями предусмотрены фильтрация запросов и ответов, ограничение запросов и контроль функциональности. Для ИИ-агентов отдельно регулируются права на ресурсы системы.

Набор мер зависит от назначения сервиса. Обязанности подрядчика предлагается закреплять в стандартах и регламентах. Предлагаемая дата применения — 1 марта 2027 года; документ пока имеет статус проекта.

Проект замены №21: оценка защиты персональных данных

В августе обсуждался проект ФСТЭК от 24 июля взамен приказа №21. Он предусматривает оценку зрелости до начала обработки ПДн, затем не реже раза в три года и после инцидента.

Проект предлагает оператору установить требуемую зрелость и для обработчика по поручению; периодичность оценки для него та же.

В проекте отдельно названы контейнеры, облака, API и интернет вещей. Выбор мер связан с архитектурой и угрозами системы; необходимость отдельной модели угроз определяет оператор. Требования пока обсуждаются.

09 Регулирование

Сертификаты НУЦ и лицензирование

Проект Минцифры: виды сертификатов НУЦ

Проект Минцифры от 28 августа описывает одиннадцать видов сертификатов Национального удостоверяющего центра (НУЦ): корневые, промежуточные, доменные, подписи кода и корпоративный.

Для корневых, промежуточных, DV, OV и подписи кода предусмотрены RSA и ГОСТ. Корпоративный сертификат использует российские алгоритмы. DV и OV различаются способом подтверждения прав на домен.

Предлагаемый срок начала действия — 1 марта 2027 года.

Проект Минцифры: когда сертификат НУЦ прекращает действие

Проект Минцифры от 10 августа 2026 года предусматривает четыре дополнительных основания прекращения действия сертификата НУЦ. Недостоверные сведения должны быть установлены вступившим в силу решением суда. Другие основания — прекращение работы НУЦ без передачи функций преемнику, отсутствие у владельца соответствующего ключа идентификации и использование ключа аутентификации, уже содержащегося в ранее созданном сертификате НУЦ.

Потеря ключа или повторное использование ключа аутентификации могут потребовать замены сертификата до окончания его срока. Проектом предложено начало действия с 1 марта 2027 года.

ФСТЭК: новые перечни оснащения лицензиатов

ФСТЭК утвердила перечни оснащения от 10 августа для технической защиты конфиденциальной информации (ТЗКИ) и от 11 августа для разработки и производства средств защиты. Наборы привязаны к видам лицензируемых работ.

Для ТЗКИ названы комплексы пентеста и сканеры с поддержкой Windows, Unix/Linux и БДУ ФСТЭК. Для мониторинга — песочницы, средства работы с угрозами, событиями и инцидентами, защищенные каналы.

Для разработчиков программных средств защиты предусмотрены статический анализ, фаззинг и динамический анализ. Лицензиату нужно сверить свои инструменты с соответствующими строками перечня.

10 Регулирование

Цифровые валюты и цифровой рубль

Цифровые валюты: правила работы депозитариев

Закон №282-ФЗ опубликован 4 августа; основные положения действуют с 1 сентября. Он вводит регулируемые роли организации обмена цифровых валют и цифрового депозитария.

Депозитарий учитывает цифровые валюты и права, обеспечивает их переход и доступ к адресам-идентификаторам. Работать можно после включения в реестр Банка России. При допуске проверяют защиту информации и операционную надежность.

Защита ключей, полномочия сотрудников и контроль операций входят в подготовку к работе с активами: компрометация ключа может привести к потере имущества клиента. Детальные требования к соискателю раскрыты в №890-П.

Цифровой депозитарий: оценка ИБ и защита ключей

Положение Банка России №890-П предусматривает стандартный уровень защиты по ГОСТ Р 57580.1 и внешнюю оценку по ГОСТ Р 57580.2 не ниже четвертого уровня соответствия. Оценщик должен иметь лицензию на ТЗКИ.

Предусмотрены анализ уязвимостей, пентест и устранение недостатков. Для активов на адресах, администрируемых депозитарием, ключи создают и используют в аппаратных модулях безопасности.

Безопасность собственного ПО можно подтвердить через сертифицированный процесс разработки; исключение не касается компонентов, взаимодействующих с СКЗИ. На 9 сентября №890-П и реестровое указание №7429-У находились на регистрации в Минюсте.

Цифровой рубль: первый этап обязательного подключения

С 1 сентября крупнейшие банки обязаны предоставлять операции с цифровым рублем. Принимать оплату должны обслуживаемые ими торговые организации с выручкой за предыдущий год более 120 млн рублей; для точек с годовой выручкой менее 5 млн рублей есть исключение. Для граждан использование добровольно.

Банкам нужно включить кошельки и платежные сообщения в антифрод и расследование операций. Следующие этапы подключения — 2027 и 2028 годы.

По письму ЦБ №ИН-03-45/30 до 1 марта 2027 года Банк России будет воздерживаться от мер к операторам переводов за несоблюдение требований к универсальному платежному коду, если реквизиты или ссылка на них представлены кодом по ГОСТ Р 56042-2014.

11 Регулирование

Инфраструктура и антифрод

Указ №604 вводит временное управление при нарушениях безопасности критической инфраструктуры

Указ Президента РФ от 24 августа 2026 года №604 опубликован и вступил в силу 24 августа. Он касается безопасности объектов критической инфраструктуры, включая противодействие беспилотным аппаратам и восстановление поврежденных объектов.

Правительство по поручению Президента может вводить временное управление имуществом, долями и имущественными правами хозяйствующего субъекта при непринятии мер безопасности, нарушении требований или несвоевременном восстановлении объекта. Управляющим по умолчанию становится Росимущество. Оно получает полномочия собственника, кроме распоряжения имуществом. Перечень объектов охватывает ТЭК, промышленность, связь, транспорт и системы жизнеобеспечения; он не ограничен критической информационной инфраструктурой по закону №187-ФЗ.

Проект для ЦОД: ответственность за данные клиентов

В августе обсуждалось предложение освободить коммерческие ЦОД от ответственности за утечки данных клиентов, если площадка обеспечивает только размещение оборудования, электропитание, охлаждение и физическую защиту. Условие — отсутствие доступа к данным и участия в определении целей и способов их обработки. Предложение связано с проектом дорожной карты развития рынка ЦОД.

Площадка, которая обслуживает инженерную инфраструктуру, и подрядчик, который администрирует клиентские серверы, выполняют разные функции. Их обязанности по защите данных и расследованию инцидентов должны отражать это различие.

28 августа «Коммерсантъ» сообщил о направлении дорожной карты на межведомственное согласование. Ее нормативная часть включает 22 предложения, в том числе изменение условий строительства и эксплуатации ЦОД.

«Антифрод 3.0»: часть требований к иностранным сайтам исключена

По сообщению «Ведомостей» от 24 августа, из новой редакции третьего антифрод-пакета убрали положения об обязательной регистрации на иностранных сайтах по номеру телефона и связанном трехлетнем хранении данных. Другие предложения о хранении отдельных категорий технической информации сохранились.

Изменение касается обсуждаемой редакции пакета. Для владельцев сайтов это сокращает состав предлагаемых обязанностей по идентификации пользователей и хранению данных, но окончательный набор мер еще зависит от согласования.

12 Новости компаний

Информзащита

34%

систем управления ЦОД
работают на устаревших
прошивках

×2

число атак через уязвимости
нулевого дня
I полугодие 2026 к I полугодю
2025

+58%

значимых облачных
киберинцидентов
I полугодие 2026 к II полугодю
2025

Солар: выручка от сервисов выросла на 21%

Выручка, млн рублей

8 490



I пол. 2025

9 608



I пол. 2026

+13,2%

I полугодие 2026
к I полугодю 2025

OIBDA, млн рублей

974



I пол. 2025

1 093



I пол. 2026

+12,2%

I полугодие 2026
к I полугодю 2025

Маржа OIBDA: 11,5% в I полугодии 2025 → 11,4% в I полугодии 2026

12 августа Солар представил результаты I полугодия 2026 года по управленческим данным, составленным по принципам МСФО. Все изменения ниже рассчитаны к тем же периодам 2025 года.

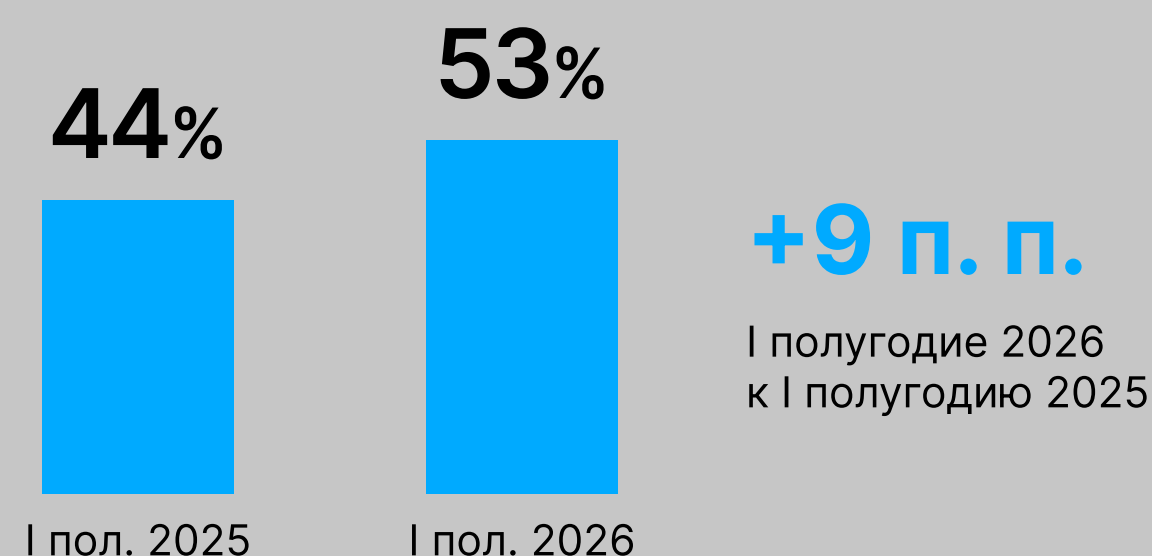
Полугодовая выручка от сервисов и комплексных проектов выросла на 21%. Компания связывает рост с мониторингом и реагированием, защитой веб-приложений и противодействием DDoS.

Во II квартале 2026 года к II кварталу 2025-го выручка выросла на 24,1%, OIBDA — на 39,8%. За полугодие маржа OIBDA почти не изменилась: 11,5% в 2025 году и 11,4% в 2026-м.

13 Новости компаний

Yandex Cloud: ИБ-сервисы у 53% крупных клиентов

Крупные клиенты с ИБ-сервисами, %

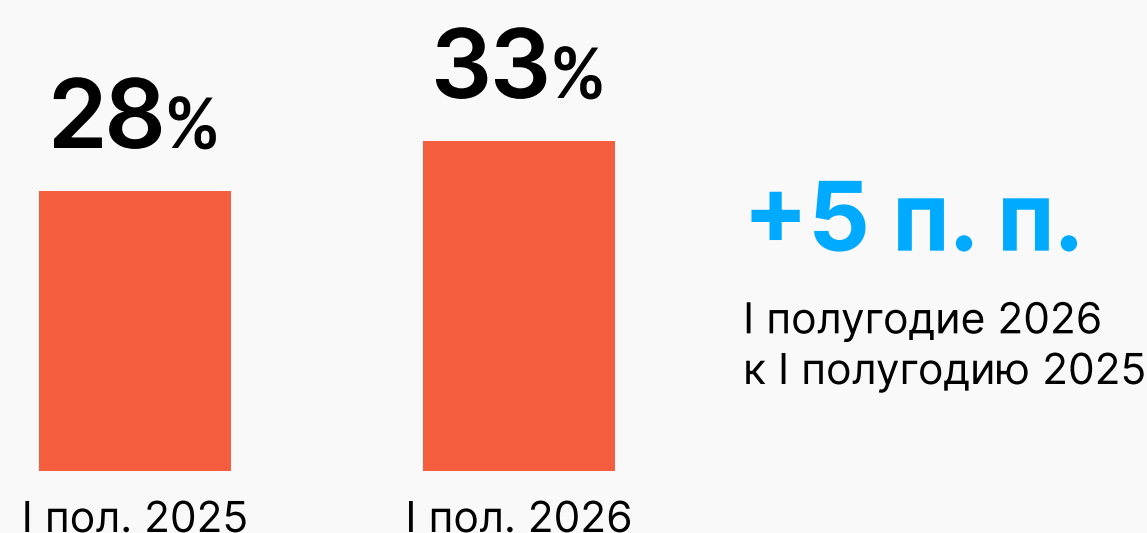


За I полугодие 2026 года к I полугодию 2025-го выручка ИБ-сервисов выросла в 2,7 раза. По итогам полугодия число клиентов Smart Web Security за год выросло в 2,5 раза. На этот сервис защиты веб-приложений приходится 22% выручки ИБ-направления.

Доля крупных клиентов с ИБ-сервисами выросла с 44% до 53% за те же периоды. Выручка 16,7 млрд рублей относится ко всей платформе; абсолютная выручка ИБ отдельно не раскрыта.

Ideco: рентабельность по EBITDA выросла до 33%

Рентабельность по EBITDA, %



По отчетности РСБУ за I полугодие 2026 года выручка Ideco выросла на 32% к I полугодию 2025-го. Рентабельность по EBITDA за те же периоды повысилась с 28% до 33%.

Чистая прибыль II квартала 2026 года не покрыла убыток I квартала. Первое полугодие компания закончила с чистым убытком.

Smart Fraud Detection получила модуль защиты цифровых кошельков

26 августа Fuzzy Logic Labs обновила Smart Fraud Detection для операций с цифровым рублем. Модуль проверяет цифровые кошельки и новые платежные идентификаторы вместе с традиционными банковскими реквизитами.

Для банков это позволяет включить операции с цифровым рублем в действующие антифрод-процессы. Проверка учитывает платежные и сессионные события, профиль клиента и параметры устройства.

Dr.Web сообщила о сертификации Mobile Security Suite для Авроры 3.3

24 августа «Доктор Веб» сообщила о сертификации Dr.Web Mobile Security Suite для ОС Аврора версии 3.3. В официальном перечне производителя сертификат ФСБ №СФ/СЗИ-0894 датирован 1 июля 2026 года и действует до 1 мая 2031 года. В августовском сообщении указано соответствие требованиям ФСБ к программным антивирусным средствам класса Д и возможность защиты информации, включая сведения, составляющие государственную тайну.

14 Новости компаний

PT Dephaze ищет учетные данные с помощью локальной LLM

25 августа [Positive Technologies](#) представила обновление PT Dephaze — системы автопентеста внутренней инфраструктуры. Встроенная LLM анализирует конфигурационные и текстовые файлы в сетевых папках, извлекает возможные логины и пароли и проверяет их применимость в тестируемой среде. Модель поставляется с продуктом и не передает эти данные во внешние сервисы.

Расширены проверки Unix- и Linux-инфраструктуры, добавлена поддержка служб каталогов на базе FreeIPA. Это позволяет проверять маршруты атак в средах, где Windows-компоненты заменены другими ОС и каталогами.

Innostage TDIR автоматизирует первичный разбор инцидентов

5 августа [Innostage](#) представила версию TDIR 1.0.0. Решение работает внутри инфраструктуры заказчика и помогает анализировать и расследовать инциденты, используя данные действующих SIEM и SOAR.

В этой версии доработаны запросы к SIEM и фильтрация ложных срабатываний, улучшена интерпретация индикаторов компрометации и PowerShell-команд. Используемая языковая модель обновлена с Qwen 2.5 до Qwen 3.x. Для аналитика SOC это прежде всего помощь в первичном разборе: получить сведения из SIEM, разобрать команду и подготовить рекомендации по инциденту.

K2 объединяет физическую, пожарную и кибербезопасность промышленного предприятия

1 августа K2Tech и K2 Кибербезопасность представили комплексную услугу для промышленных предприятий. Она охватывает контроль физического доступа и видеонаблюдение, пожарную защиту, сетевой доступ, мониторинг ИБ и восстановление после инцидентов.

Для промышленного заказчика такой проект связывает защиту производственной площадки с защитой ее цифровых систем. Например, управление доступом к оборудованию должно учитывать и физическое проникновение, и подключение устройства к сети.

15 Новости компаний

MaxPatrol, PT NAD, Kaspersky MDR и Security Vision обновили сценарии SOC

В MaxPatrol 360 2026.2, представленном 3 августа, появилась подсистема интеграций с внешними системами. Через MaxPatrol EDR можно включать в сценарий реагирования изоляцию узла или завершение вредоносного процесса. Доступны уведомления через мессенджеры и корпоративную почту. Интеграции позволяют использовать уже установленные средства защиты в общих сценариях расследования.

В публикации от 31 августа Positive Technologies описала возможности PT NAD 13.0, представленной на запуском вебинаре 4 июня. Аналитик может инициировать сдерживание атаки из консоли: изоляцию узла через MaxPatrol EDR или блокировку через механизм внешних динамических списков NGFW. Решение о блокировке принимает специалист. PT Expert Cloud дополняет локальные обнаружения сведениями об угрозах; архивные метаданные можно хранить в S3-совместимых и сетевых файловых хранилищах.

Обновление Kaspersky MDR от 24 августа связывает сведения об утекших учетных данных с событиями в инфраструктуре клиента. В сервисе появился контроль поступления телеметрии от активов: отсутствие данных становится отдельной проблемой, которую нужно устранить, чтобы узел не выпадал из мониторинга.

Security Vision 5 получила изменения в коннекторах, аналитике и управлении правилами корреляции. В числе обновлений — поддержка аутентификации SASL/SCRAM в Kafka-коннекторе, сжатие при передаче событий и отдельный раздел редактирования правил корреляции.

BI.ZONE PAM, Indeed ITDR и MULTIDIRECTORY обновили работу с доступом

BI.ZONE PAM 2.6 поддерживает беспарольную аутентификацию через подтверждение доступа в браузере, в том числе с использованием токенов и биометрии. Для неинтерактивных SSH-сеансов, например при работе Ansible, предусмотрены текстовые журналы. Они сохраняют содержание автоматизированных действий там, где видеозапись сеанса малоинформативна.

В Indeed ITDR 2.2 от 19 августа добавлены TOTP-сценарии для изолированных сетей, где нельзя использовать push-уведомления. Расширены фильтры журналов доступа, включая пользователя, ресурс, протокол и IP-адрес.

MULTIDIRECTORY 3.2.0 от 20 августа получила поддержку атрибутов мандатного управления доступом Astra Linux, изменения групповых политик и балансировку запросов между контроллерами домена с проверкой их доступности.

16 Тенденции

BI.ZONE

BI.ZONE получила доступ во внутреннюю сеть в 93% заказных проектов

Июль 2025 — июль 2026 · более 100 проектов

Доступ во внутренний периметр



>820 выявленных уязвимостей; 26% высоких или критических

20 августа BI.ZONE опубликовала результаты более 100 проектов пентеста, AppSec и red team с июля 2025 по июль 2026 года.

Доступ во внутренний периметр получен в 93% проектов, в 85% проектов проверяющие выполнили все поставленные задачи. Их определяли для конкретной компании и модели нарушителя. Выявлено более 820 уязвимостей; 26% отнесены к высоким или критическим. На крупный бизнес приходилось 64% проектов.

Инфосистемы Джет

Инфосистемы Джет: низкая киберустойчивость у 64% обследованных компаний

64% из 50 российских компаний получили низкую оценку киберустойчивости

17 августа «Инфосистемы Джет» опубликовали оценку киберустойчивости 50 российских компаний. У 64% участников она оказалась низкой.

Наиболее слабыми оказались предотвращение первого проникновения и подготовка к восстановлению после уничтожения или шифрования данных. Защита внутри сети была развита лучше.

17 Тенденции

WMX · ServicePipe

WMX и ServicePipe: 44% веб-атак были многоэтапными

849,7 млн веб-атак в I полугодии 2026; +27% к I полугодю 2025

Доля многоэтапных веб-атак

I полугодие 2026



×2
автоматизированные сканирования
I полугодие 2026 к I полугодю 2025

×5
DDoS свыше 100 Гбит/с в I полугодии 2026
База сравнения в публикации не указана

WMX и ServicePipe наблюдали инфраструктуру почти 600 крупных организаций в I полугодии 2026 года. Зафиксировано 849,7 млн веб-атак, на 27% больше, чем в I полугодии 2025 года; 44% были многоэтапными.

DDoS может отвлекать защитников, пока параллельная атака направлена на приложение, API или бизнес-логику. События сетевой защиты, WAF и приложения нужно разбирать совместно, с участием специалистов по приложению.

BI.ZONE

BI.ZONE: фишинговых доменов меньше, их используют повторно

-73% заблокированных фишинговых доменов: I полугодие 2026 к I полугодю 2025

>13,5 тыс. доменов заблокировано

За I полугодие 2026 года BI.ZONE DRP заблокировала более 13,5 тыс. фишинговых доменов, на 73% меньше, чем в I полугодии 2025 года. Один домен используют повторно через поддомены и персонализированные страницы. Падение их числа не означает пропорционального сокращения атак.

В Threat Zone 2026 изучены более 35 тыс. объявлений с лета 2025 по лето 2026 года. Среди продаваемых доступов есть активные сессии и токены; старые базы объединяют и продают как новые.

Обнаружив утечку, нужно проверить сессии, токены и связанные доступы. Смена пароля не всегда завершает ранее выданную сессию.

18 Тенденции

Лаборатория Касперского

«Лаборатория Касперского»: критических уязвимостей во II квартале стало на 34% больше

≈2 700 критических уязвимостей во II квартале 2026; +34% ко II кварталу 2025

≈5 200 за I полугодие 2026; +47% к I полугодию 2025

В анализе «Лаборатории Касперского» использованы CVE, GHSA и БДУ ФСТЭК. Во II квартале 2026 года найдено около 2 700 критических уязвимостей, на 34% больше, чем во II квартале 2025-го. За I полугодие 2026 года — около 5 200, на 47% больше, чем за I полугодие 2025-го.

Лаборатория Касперского

«Лаборатория Касперского»: 82% опрошенных представителей МСБ сообщили об инцидентах

Ответы российских участников · публикация 18 августа 2026

Увеличили бюджет по сравнению с прошлым годом



Расширили ИТ/ИБ-команду



Передали функции подрядчикам



0%

100%

В российской части опроса «Лаборатории Касперского» 82% представителей МСБ сообщили об инцидентах за последний год. Весь опрос охватил 1 800 респондентов из 18 стран; российская подвыборка отдельно не раскрыта.

Участники назвали увеличение бюджета, расширение команды и передачу функций подрядчикам. Можно было выбрать несколько ответов.

19 Сотрудничество

KUMA и VK Object Storage

Испытания проводили на архиве 3 ПБ при нагрузке более 6 тыс. запросов в секунду и приросте данных 10 ТБ в сутки. Оперативные события остаются на быстром хранении, холодный архив — в объектном хранилище.

Innostage PAM и PT Sandbox

Файл из привилегированного сеанса проверяется в песочнице; передача на сервер разрешается или блокируется по вердикту.

Испытания охватили встроенные файловые средства, RDP Web, SFTP Web и SFTP Client.

Проверенная совместимость

BI.ZONE и Postgres Pro

Подтверждена совместимость EDR, PAM, Mail Security, WAF и Secure DNS. Поддержка зависит от редакции и версии: WAF — Standard/Enterprise 16–18, PAM — Enterprise 18.

InfoWatch и Deckhouse

Восемь продуктов InfoWatch проверили с Deckhouse Kubernetes Platform в Astra Linux Special Edition.

R-Vision VM и «Штурвал»

Проверили работу R-Vision VM на платформе «Штурвал», включая сохранение функций и масштабирование.

Двухфакторная аутентификация

SECURITM и САКУРА

Локальная интеграция: подтверждение входа в приложении без одноразового кода. Включение и отключение 2FA фиксируется в журнале.

MULTIFACTOR и Selectel

Облачная двухфакторная аутентификация MULTIFACTOR доступна компаниям, использующим инфраструктуру и сервисы Selectel.

20 Сотрудничество

SafeMobile и MIG

Совместный ПАК предусматривает подключение устройства к управлению через QR-код. Специальная лицензия UEM SafeMobile действует только на устройствах MIG; это ограничение важно для смешанного парка.

SolarShip: результаты партнерского канала

На 5 августа 2026 года в программе 455 партнеров против примерно 300 в I полугодии 2025 года. За два года реализовано более 1 100 проектов.

Солар сообщил о росте выручки партнерского канала на 50% год к году, но не уточнил отчетный период.

DS Proxima и MITIGATOR

Проверена распределенная очистка: для TCP Splicing прямой и обратный трафик проходят через один узел. Отдельно испытана балансировка MITIGATOR Web Challenger.

R-Vision: чего партнеры ждут от проектов VM

В опросе участвовали 43 представителя партнеров, интеграторов и дистрибьюторов.

Участники выделяют сопровождение, пилот, совместимость и работу после сканирования. Среди сложностей — встраивание VM в процессы и нехватка специалистов.

21 Реестры Минцифры

«Грифон» · встроенное ПО

НПП «Цифровые решения»

Запись №34634 от 4 августа 2026 года.

Встроенное ПО криптомаршрутизатора для шифрования и имитозащиты данных в территориально распределенных сетях.

ПК УИБ

«Управление информационной безопасности»

Запись №34703 от 4 августа 2026 года.

Автоматизация документации и мероприятий ИБ, контроль выполнения требований.

«Аргос FW» · управление и ПАК

ТехАргос

ПО централизованного управления: №34658 от 4 августа. ПАК «Аргос FW» Y.V02: №34815 от 18 августа.

Это разные компоненты одной семьи. Межсетевой экран уже был в реестре с ноября 2024 года. В линейке предусмотрены сегментация, NAT, REST API и Active-Standby.

Coshkey 2.0

Фриматик

Запись №34664 от 4 августа 2026 года.

Корпоративное хранилище паролей для коробочного Битрикс24. Разграничивает доступ, группирует учетные данные и сохраняет журнал действий.



22 Реестр ФСТЭК

Комплекс ФПСУ версии 3 · №5093

Амикон

Сертификат №5093 внесен 3 августа 2026 года, действует до 3 августа 2031 года.

В записи указаны четвертый уровень доверия и профили защиты межсетевых экранов типов А и Б четвертого класса: ИТ.МЭ.А4.ПЗ и ИТ.МЭ.Б4.ПЗ.

Сертификат относится к серийному выпуску комплекса.

Портал инфраструктурных подключений · №5098

Внесен 19 августа 2026 года.

Заявитель: ГКУ «Инфогород».

«Расчет АЭП» · №5103

ООО «НОВО»

Сертификат №5103 внесен 24 августа 2026 года, действует до 24 августа 2031 года.

Комплекс рассчитывает эффективность защиты речевой информации от утечки за счет акустоэлектрических преобразований.

В записи указаны технические условия и методика АЭП-2018.

Сервис аутентификации и каталог управления пользователями · №5099

Внесен 20 августа 2026 года.

Заявитель: ГКУ «Инфогород».

РНИП · №5095

«Кабинет администратора начислений» информационной системы РНИП.

Внесен 13 августа 2026 года.
Заявитель: Департамент информационных технологий города Москвы.

Модуль мониторинга транспортных событий · №5100

Внесен 20 августа 2026 года.

Заявитель: ГКУ «Инфогород».

«Миллион призов» · №5097

Внесен 19 августа 2026 года.

Заявитель: ГКУ «Инфогород».

Система мониторинга инцидентов · №5101

Система мониторинга инцидентов в сферах деятельности органов исполнительной власти города Москвы.

Внесен 21 августа 2026 года.
Заявитель: Департамент информационных технологий города Москвы.

Спасибо за внимание!

Рынок ИБ РФ · Август 2026

ИЗ | информзащита

Автор: Елена Рухлова

Ведущий аналитик Департамента маркетинга
ГК «Информзащита»