

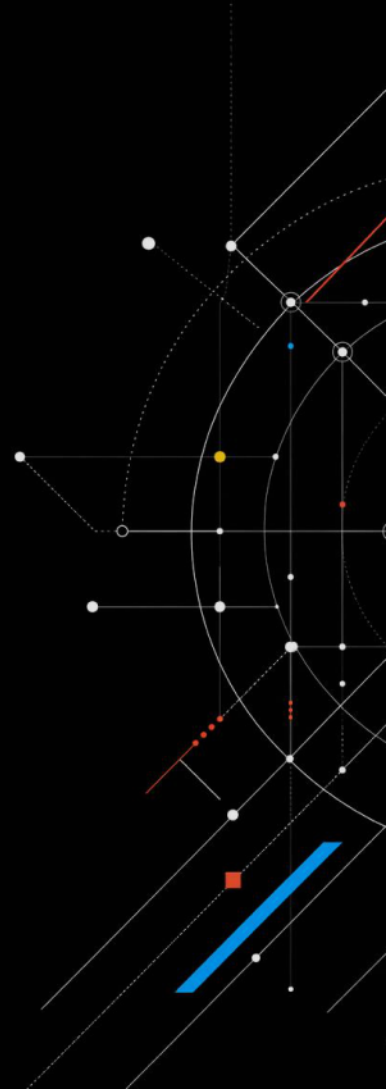
АНАЛИТИЧЕСКИЙ ДАЙДЖЕСТ

Дайджест рынка ИБ

Август 2026

Рынок информационной безопасности России

Регулирование · компании · исследования
Сотрудничество · реестры и сертификация



Как читать этот выпуск

Начните с выводов. Затем выберите акценты для своей роли или перейдите к конкретному разделу с новостями и источниками.

Выводы августа	3
Акценты для заказчиков	7
Акценты для интеграторов и MSSP	8
Акценты для вендоров	9
Регулирование	10
Новости компаний	22
Тенденции и исследования	28
Сотрудничество и интеграции	34
Реестры и сертификация	40

01 Выводы августа

Требования к подрядчикам и внешним сервисам госсистем

Внешний сервис: что согласовать до подключения

Доступ подрядчика	С 01.03.2027: оценка зрелости до допуска
Работа сервиса	Согласовать восстановление, ключи и журналы
Инцидент и выход	Определить уведомление и возврат данных

Августовские изменения уточняют требования к подрядчикам и внешней инфраструктуре госсистем. Приказ [ФСТЭК №137](#) меняет приказ №117: с 1 марта 2027 года подрядчик оценивает зрелость своей защиты до предоставления доступа. [Постановление №1024](#) требует заранее фиксировать в договоре ответственность, восстановление, возврат данных и работу соисполнителей; [приказ ФСБ №321](#) распространяет требования к криптозащите на используемые внешние сервисы. [Приказ Минцифры №702](#) описывает инфраструктуру хостинг-провайдеров и начнет действовать 1 марта 2027 года. [Приказ ФСБ №297](#) устанавливает срок передачи сведений об инциденте для указанных в нем государственных организаций.

Для регулируемых систем граница ИБ проходит через архитектуру соединения с провайдером, доступ подрядчика, ключевую информацию, журналы, резервирование, сроки уведомления и возможность вернуть данные при завершении договора. Ответственность за эти элементы нужно проектировать до подключения сервиса, а не распределять уже после инцидента.

Оценка зрелости и аттестация: разные процедуры проверки

[Методика ФСТЭК](#) вводит 21 направление оценки и восемь критериев. [Приказ №137](#) изменяет пункт 32 приказа №117: с 1 марта 2027 года подрядчик оценивает зрелость своей защиты до получения доступа и затем не реже одного раза в два года. [Приказ №60](#) включает анализ уязвимостей и, в применимых случаях, пентест в аттестационные испытания, а после аттестации сохраняет периодический контроль. [Проект новых требований к защите ПДн](#) также предусматривает регулярную оценку зрелости для оператора и обработчика по поручению. Поэтому доказательная база защиты должна включать подтвержденные проверки, устранение недостатков, разделение исполнения и контроля и историю изменений — наряду с регламентами и установленными средствами.

ИБ встроена в условия допуска и эксплуатации цифровых активов

[Закон №282-ФЗ](#) вводит регулируемые роли организации обмена цифровых валют и цифрового депозитария. Цифровой депозитарий учитывает цифровые валюты и цифровые права и обеспечивает доступ к активам. Для допуска цифрового депозитария [Банк России](#) проверяет соответствие требованиям по защите информации и операционной надежности. В [положении №890-П](#) появляются внешний аудит, требования ГОСТ Р 57580, анализ уязвимостей, пентест и аппаратная защита ключей при определенной схеме хранения. Параллельно началась первая обязательная волна операций с [цифровым рублем](#), а для [универсального платежного кода](#) действует переходный режим.

В этой части ИБ встроена в саму возможность работать в новой финансовой инфраструктуре. Архитектура хранения ключей, процессы допуска, внешняя оценка, антифрод и операционная надежность должны быть определены раньше запуска продукта. При этом [№890-П](#) и [№7429-У](#) на 9 сентября еще находились на государственной регистрации в Минюсте.

Полнота телеметрии и заранее определенные действия — основа управляемого реагирования

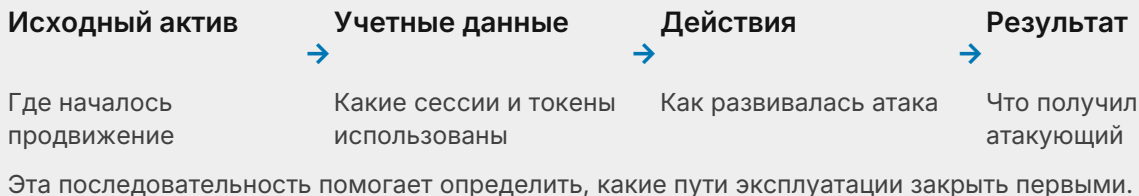


В августе Positive Technologies представила [MaxPatrol 360 2026.2](#) и описала сценарии [PT NAD 13.0](#), представленной в июне. Из этих продуктов можно перейти к изоляции узла или блокировке. [Kaspersky MDR](#) отдельно контролирует отсутствие телеметрии от активов, [Security Vision](#) развивает коннекторы и управление правилами. Для охваченных им государственных организаций [приказ ФСБ №297](#) задает 24 часа с обнаружения инцидента на передачу сведений в Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

Полнота контекста определяет, может ли эта связка работать. Если актив не инвентаризирован, телеметрия пропала или сведения о владельце и категории системы находятся в другом справочнике, действие может быть быстрым, но плохо обоснованным. Для SOC критичны качество CMDB и реестров активов, контроль поступления данных, заранее определенные полномочия на блокировку и проверенные сценарии восстановления.

Контекст атаки складывается из цепочки событий, учетных данных и сессий

Что восстановить при расследовании



[WMX](#) и [ServicePipe](#) относят 44% веб-атак, наблюдавшихся в I полугодии 2026 года, к многоэтапным. [BI.ZONE](#) показывает повторное использование одного фишингового домена через поддомены и персонализированные страницы; [Threat Zone](#) — ценность активных сессий и токенов; в проектах [наступательной безопасности BI.ZONE](#) с июля 2025 по июль 2026 года доступ во внутренний периметр был получен в 93% работ. Общая практическая мысль этих разных источников — расследованию нужен маршрут атаки: исходный актив, использованные учетные данные и сессии, последовательность действий и достигнутый результат. Такая связка помогает приоритезировать исправления по реальному пути эксплуатации, месту уязвимости в цепочке и достигнутому результату.

Испытаны архив KUMA и передача файлов из PAM

В августе опубликованы проверенные связки [KUMA с VK Object Storage](#), решений [BI.ZONE с Postgres Pro](#), продуктов [InfoWatch с Deckhouse](#), [R-Vision VM со «Штурвалом»](#), [Innostage PAM с PT Sandbox](#), [SafeMobile с устройствами MIG](#) и [DS Proxima с MITIGATOR](#). Для KUMA указаны массив 3 ПБ, нагрузка более 6 тыс. запросов в секунду и прирост 10 ТБ в сутки. Innostage PAM передает файл в песочницу до загрузки на сервер; испытаны встроенная работа с файлами, RDP Web, SFTP Web и SFTP Client.

Финансовые результаты: сервисы, доля клиентов и рентабельность

У [Солара](#) в I полугодии 2026 года по сравнению с I полугодием 2025 года общая выручка выросла на 13,2%, а выручка от сервисов и комплексных проектов на 21%. Рентабельность по OIBDA почти не изменилась: 11,5% в I полугодии 2025 года и 11,4% в I полугодии 2026 года. У [Yandex Cloud](#) за те же периоды выручка от ИБ-сервисов выросла в 2,7 раза, а доля крупных клиентов с ними с 44% до 53%. [Ideco](#) увеличила выручку на 32% и рентабельность по EBITDA с 28% до 33%, но закончила I полугодие 2026 года с чистым убытком. Улучшение операционного результата еще не обеспечило прибыль за полугодие.

ИИ как объект защиты и компонент ИБ-продуктов

Два применения ИИ требуют разных проверок

Защита ИИ-системы

Сегмент, данные, запросы и ответы, права агента. Меры ФСТЭК пока предложены в проекте.

ИИ в средстве защиты

PT Dephaze ищет учетные данные локально; Innostage TDIR помогает разбирать инциденты.

[Проект ФСТЭК](#) для госсистем предлагает отдельный сегмент для моделей ИИ, усиленный контроль привилегированного доступа, фильтрацию запросов и ответов и управление правами ИИ-агентов. Одновременно [PT Dephaze](#) использует локальную LLM для поиска учетных данных, а [Innostage TDIR](#) — языковую модель для разбора инцидентов и команд.

В первом случае защищают модель, данные, запросы, ответы и действия агента. Во втором модель применяют как компонент средства ИБ; здесь критичны локальность обработки, качество результата, журналирование и границы автоматизации. Для заказчика и разработчика ключевые вопросы — какие данные получает модель, какие решения ей разрешено принимать и как проверяется ее работа.

02 Акценты для заказчиков

1. Включите получение оценки зрелости подрядчика в порядок допуска к госсистеме. С 1 марта 2027 года пункт 32 приказа №117 действует в редакции приказа №137: подрядчик оценивает свою защиту до доступа и затем не реже одного раза в два года. Определите в договоре, кто принимает результаты оценки и получает сведения об устранении недостатков.

2. Проверьте, изменился ли состав предстоящей аттестации вашей системы. С 1 сентября приказ №60 включает в испытания анализ уязвимостей. Для госсистем и других ИС госорганов, ГУПов и госучреждений классов 1–2 пентест требуется при подключении к интернету или взаимодействии с другими системами. Исключение с сертифицированной криптозащитой относится ко второму случаю. Эти условия нужно учесть при расчете объема и стоимости испытаний.

3. Проверить полноту данных SOC и готовность к действию. Инвентаризация активов, владельцы, критичность, поступление телеметрии, связь с CMDB и полномочия на изоляцию должны быть проверены до инцидента. Если система подпадает под приказ ФСБ №297, согласуйте с внешним SOC уведомление, которое позволит оператору передать сведения в НКЦКИ в пределах 24 часов с обнаружения инцидента.

4. При подготовке цифрового депозитария определите, какие адреса хранения он будет администрировать. В №890-П для этой схемы предусмотрены аппаратные модули защиты ключей. Отдельно выделите ПО, взаимодействующее с СКЗИ: исключение о подтверждении безопасности собственной разработки через сертифицированный процесс на него не распространяется. На 9 сентября документ находился на регистрации в Минюсте.

5. Совместимость проверять на уровне конкретных версий и эксплуатационного сценария. Для проектного решения нужны поддерживаемая конфигурация, правила обновления, резервирование и распределение ответственности при сбое.

03 Акценты для интеграторов и MSSP

- 01** Для внешнего сервиса госсистемы подготовьте регламент взаимодействия как часть договора. По постановлению №1024 в нем нужны допустимое время восстановления, резервное копирование и возврат данных. Сообщение о принятых мерах после сбоя защиты поставщик передает в течение трех часов с обнаружения, если регламентом не установлен иной срок. При привлечении соисполнителей отдельно предусмотрите уведомление и согласие на передачу информации ограниченного доступа.
- 02** В SOC/MDR ценность создается связкой обнаружения и управляемого действия. Интегратору важно связать SIEM/NDR/EDR/NGFW технически и процессно: кто имеет право изолировать узел, какие события требуют подтверждения, как контролируется полнота телеметрии и как сохраняется контекст расследования.
- 03** В проекте управления уязвимостями включите в пилот передачу найденной проблемы на исправление и повторное сканирование. В опросе R-Vision партнеры выделили трудности встраивания VM в процессы заказчика и нехватку специалистов. Проверьте на одном реальном случае, кто получает задачу, кто исправляет проблему и каким результатом подтверждается ее устранение.
- 04** Для архива SIEM отдельно рассчитайте требования к поиску по свежим событиям и емкости длительного хранения. В испытаниях KUMA с VK Object Storage недавние события оставались на быстром хранении, а холодный архив на HDD. Массив 3 ПБ, прирост 10 ТБ в сутки и более 6 тыс. запросов в секунду описывают этот стенд; для проекта нужны собственные объемы и нагрузка.
- 05** В госсистеме с ИИ разделите доступ справочной модели и агента, который обращается к ведомственным данным или выполняет действия. Проект ФСТЭК от 24 августа отдельно описывает сегментацию моделей, привилегированный доступ и права агентов. При обсуждении архитектуры с заказчиком отметьте, какие предложенные меры затрагивают его сценарий. Дата 1 марта 2027 года пока предложена в проекте.

04 Акценты для вендоров

- 01** Для выбора продукта важны доказательства эксплуатационной готовности: поддерживаемые версии, типовые схемы интеграции, API, телеметрия, журналирование, отказоустойчивость и понятные ограничения. Проверенная совместимость должна описывать конфигурацию и сценарий, а не ограничиваться фактом совместного теста.
- 02** Продукты для SOC и реагирования должны передавать контекст дальше по цепочке. Ценность дают качество данных об активе, объяснимое основание срабатывания, интеграция с EDR/NGFW/SOAR, контроль потери телеметрии и возможность восстановить историю решения — вместе с самим обнаружением.
- 03** Сопоставьте оснащение испытаний с перечнем ФСТЭК для вашего вида лицензируемых работ. Августовский перечень для разработки программных средств защиты предусматривает статический анализ, фаззинг и динамический анализ. Не подменяйте его перечнем для услуг мониторинга: в нем названы другие инструменты, включая песочницы и средства работы с событиями и инцидентами.
- 04** Если в продукте используется ИИ, нужно отдельно объяснять, где работает модель, какие данные получает, что передается наружу, какие действия автоматизированы и как пользователь может проверить результат. Если продукт защищает ИИ-систему — столь же конкретно описывать защиту запросов, ответов, моделей, агентов и привилегированного доступа.
- 05** Покажите в продуктах управления доступом, как прекращается доступ скомпрометированной учетной записи. BI.ZONE описывает продажу действующих сессий и токенов: смена пароля не всегда завершает уже выданную сессию. В демонстрации сценария проверьте отзыв сессий и токенов и фиксацию результата в журнале.

05 Регулирование

Государственные информационные системы

ФСТЭК уточнила требования к защите госсистем и оценке подрядчиков

Приказ №137: две даты и разные проверки

01.09.2026

Основные поправки

Изменения к требованиям защиты госсистем

01.03.2027

Новая редакция п. 32

Зрелость подрядчика: до допуска, затем не реже раза в два года

Кзи: отдельная полугодовая оценка по действующему приказу №117; результаты направляют за пять рабочих дней.

Приказ ФСТЭК России от 8 мая 2026 года №137 опубликован 11 августа. Основные изменения действуют с 1 сентября 2026 года; новая редакция пункта 32 приказа №117 вступит в силу 1 марта 2027 года.

Поправки уточняют оценку зрелости защиты, допуск подрядчиков и способы аутентификации. В отдельных положениях об удаленном доступе и мобильных устройствах наряду со строгой аутентификацией разрешена усиленная многофакторная аутентификация. Из части требований исключены уточнения о постоянном или непосредственном подключении к интернету: применимость этих мер зависит от новой формулировки соответствующего пункта, а не только от наличия постоянного интернет-соединения.

С 1 марта 2027 года новая редакция пункта 32 закрепляет оценку уровня зрелости самим подрядчиком: до получения доступа к системе или информации, затем не реже одного раза в два года. Полугодовая оценка показателя защищенности Кзи уже предусмотрена действующим приказом №117. Срок направления результатов Кзи во ФСТЭК составляет пять рабочих дней после оценки.

Оператору госсистемы потребуется получать результаты оценки от исполнителя до открытия доступа. В договоре сопровождения нужно определить, как подрядчик подтверждает свою зрелость и сообщает об устранении недостатков. Интегратору оценку собственной защиты придется включать в подготовку к проекту, а не откладывать до начала работ у заказчика.

[Приказ ФСТЭК №137](#) · [КонсультантПлюс: текст и сроки применения](#) · [Кредос: разбор изменений](#)

ФСТЭК выпустила методику оценки зрелости защиты информации

Как устроена оценка зрелости

21

направление оценки

8

критериев для каждого направления

Неприменимые направления исключают. Исполнение и самооценку функций разделяют.

Методика ФСТЭК от 7 августа 2026 года охватывает техническую защиту информации в информационных системах и безопасность значимых объектов КИИ. В ней выделено 21 направление оценки, включая управление уязвимостями и обновлениями, привилегированный доступ, мониторинг и работу с подрядчиками. Направления, не применимые к используемым технологиям, исключаются из расчета.

Для каждого направления установлены восемь критериев. Проверяется, как процесс документирован и выполняется, обеспечен ли он инструментами и квалифицированными сотрудниками. Отдельно оцениваются контроль, обучение, внешний аудит и актуализация процесса. Например, при оценке управления обновлениями одного регламента недостаточно: результаты должны подтверждать, что предусмотренные им работы действительно проводятся.

Самооценку нужно организовать так, чтобы сотрудники не оценивали функции, которые выполняют сами. Для оператора это требует разделить исполнение и проверку внутри команды либо привлечь внешнего исполнителя. Подрядчикам госсистем методика нужна и для подготовки оценки собственной защиты перед получением доступа к системам заказчика.

[Методика ФСТЭК от 7 августа](#) · [Гарант: полный текст](#) · [Кредос: применение методики](#)

При аттестации части госсистем стали обязательными анализ уязвимостей и пентест

Приказ ФСТЭК России от 27 февраля 2026 года №60 зарегистрирован 24 июня, опубликован 25 июня и вступил в силу 1 сентября.

Документ изменил порядок аттестации объектов информатизации. Анализ уязвимостей включен в состав аттестационных испытаний. Обязательный пентест выделен в пункте 16.1: он касается госсистем и иных систем госорганов, ГУПов и госучреждений первого и второго классов защищенности при подключении к интернету либо взаимодействию с другими системами, в том числе системами подрядчиков. Исключение для сетей с сертифицированной криптографической защитой относится к межсистемному взаимодействию; оно не отменяет самостоятельное условие о подключении к интернету.

При аттестации части госсистем стали обязательными анализ уязвимостей и пентест · продолжение

После аттестации оператор должен представлять отчет о периодическом контроле защиты не реже одного раза в три года. Результаты направляются во ФСТЭК в течение пяти рабочих дней после контроля. При изменении состава системы или условий эксплуатации могут потребоваться дополнительные испытания, а при повышении класса защищенности — повторная аттестация.

Заказчикам предстоит включать проверку уязвимостей и возможных путей проникновения в программу аттестационных работ. Для испытательных лабораторий и интеграторов это расширяет состав проверки: одного сопоставления внедренных мер с документацией недостаточно, когда порядок прямо требует испытаний на проникновение.

[Приказ ФСТЭК №60](#) · [Полный текст изменений](#) · [КонсультантПлюс: обязательный пентест](#)

ФСБ установила суточный срок передачи сведений об инцидентах в ГосСОПКА

24 часа от обнаружения инцидента

0 ч

24 ч

Обнаружили инцидент

Передали сведения в НКЦКИ

Внешний SOC должен уведомить заказчика так, чтобы оператор успел передать сведения в НКЦКИ. Порядок действует для перечисленных в приказе №297 государственных организаций.

Приказ ФСБ России от 6 августа 2026 года №297 зарегистрирован 20 августа, опубликован 21 августа и действует с 1 сентября.

Порядок распространяется на взаимодействие с ГосСОПКА информационных систем государственных органов, государственных унитарных предприятий и государственных учреждений. Сведения о выявленном компьютерном инциденте необходимо передать в НКЦКИ в течение 24 часов. Основной канал — личный кабинет; для технических сбоев предусмотрены резервные способы обмена. Взаимодействие оформляется регламентом.

Срок отсчитывается от обнаружения инцидента. Организации, которые пользуются внешним SOC, должны сопоставить его срок уведомления заказчика с этими 24 часами. Если подрядчик передает сообщение только после длительного согласования, у оператора остается меньше времени на обязательное уведомление НКЦКИ. В регламенте потребуются определить, кто отправляет первичное сообщение и какие сведения должны быть доступны дежурной смене.

[Приказ ФСБ №297](#) · [Полный текст порядка](#) · [КонсультантПлюс: правовой статус](#)

Новые требования ФСБ к криптозащите охватывают внешние сервисы госсистем

Приказ ФСБ России от 22 августа 2026 года №321 опубликован 31 августа и вступает в силу 11 сентября. Он заменяет приказ ФСБ от 18 марта 2025 года №117.

Требования охватывают криптографическую защиту информации в госсистемах и используемых ими электронных сервисах — внешних вычислительных ресурсах, программах и базах данных. Для информации, составляющей государственную тайну, и ряда специально перечисленных в приказе систем действует другой порядок. При использовании внешнего сервиса класс СКЗИ должен соответствовать требованиям к той системе или ее сегменту, где этот сервис применяется. Выбор криптосредств связан с моделью угроз и техническим заданием.

Документ устанавливает требования к размещению криптосредств, контролю доступа, регистрации действий и обращению с ключевой информацией. Внутренний контроль соблюдения требований проводится не реже одного раза в три года.

При подключении внешнего сервиса оператору нужно проверить, как провайдер обеспечивает требуемый класс криптозащиты. Это влияет на выбор площадки и схему соединения с госсистемой. Распределение обязанностей по управлению ключами, доступом и журналами следует согласовать до размещения информации.

[Приказ ФСБ №321](#) · [Полный текст требований](#) · [Ведомости: защита подключаемых сервисов](#) · [CNews: изменения требований](#)

Ведомственные системы и внешняя инфраструктура

Правительство определило правила для ведомственных систем вне режима ГИС

Постановление Правительства РФ от 13 августа 2026 года №1007 опубликовано 14 августа и действует с 1 сентября. Оно касается информационных систем государственных органов, которые обеспечивают организационные, документационные, финансовые и другие внутренние функции, но не относятся к ГИС.

При создании таких систем госорганы должны использовать ПО и ПАК из национального фонда алгоритмов и программ либо российских и евразийских реестров с отметкой «соответствует стандартам». Если подходящего решения с этой отметкой или утвержденного стандарта нет, собственная разработка требует технико-экономического обоснования и положительного заключения Минцифры. На согласование отведено 20 рабочих дней.

Одного включения продукта в реестр для выбора по этому порядку недостаточно: заказчику нужна отметка о соответствии стандартам либо согласованное обоснование разработки. Техническое задание должно учитывать модель угроз и уровни защищенности персональных данных. Для систем госорганов Москвы предусмотрено исключение: обязательны только пункты 8, 11, 18, 19 и 21 требований.

[Постановление №1007](#) · [Полный текст](#) · [Техэксперт: требования к ведомственным системам](#)

Размещение госсистем у внешних поставщиков потребует подробного разделения ответственности

В договоре закрепляют работу сервиса и выход из него	
Во время работы	Хранение, резервное копирование, доступ к данным
При сбое	Восстановление и незамедлительное взаимное уведомление
При завершении	Передача данных заказчику при окончании или расторжении договора

Постановление Правительства РФ от 18 августа 2026 года №1024 опубликовано 20 августа и действует с 1 сентября. Оно определяет использование внешних электронных сервисов при создании и эксплуатации госсистем и иных информационных систем государственных органов, указанных в части 1.1 статьи 13 закона №149-ФЗ. Под сервисами понимаются вычислительные ресурсы, программы и базы данных, доступные по сети.

Регламент взаимодействия включается в закупочную документацию и договор. В нем определяются ответственность сторон и допустимое время восстановления сервиса. Поставщик обеспечивает хранение и резервное копирование данных, доступ заказчика к ним на срок договора и их передачу по завершении работ или при расторжении. О сбое защиты стороны уведомляют друг друга незамедлительно. Сведения о принятых мерах поставщик направляет не позднее трех часов после обнаружения сбоя, если регламентом не установлен иной срок.

Заказчик сможет закрепить сроки восстановления и возврат данных еще в условиях закупки. Отдельно регулируется привлечение соисполнителей: поставщик уведомляет об этом не позднее чем за три рабочих дня до начала их работы, а перед передачей информации ограниченного доступа получает письменное согласие заказчика. Эти условия важны для облачных услуг, где часть обработки или сопровождения выполняет другая компания.

Отдельный приказ Минцифры России от 31 июля 2026 года №702, опубликованный 20 августа, относится к предоставлению вычислительных мощностей в постоянно подключенной к интернету инфраструктуре. Среди обслуживаемых систем названы ГИС, иные системы госорганов, муниципальные системы и системы государственных и муниципальных предприятий и учреждений. Приказ начнет действовать 1 марта 2027 года и заменит приказ №677. Хостинг-провайдерам необходимо сопоставить требования к своей инфраструктуре с составом систем заказчиков; новый документ прямо включает иные информационные системы госорганов.

[Постановление №1024](#) · [Полный текст условий размещения](#) · [Приказ Минцифры №702](#) · [Текст требований к хостинг-провайдерам](#)

Проекты требований к ИИ и персональным данным

ФСТЭК предложила отдельные меры защиты ИИ-компонентов госсистем

Предложения ФСТЭК: статус и область применения	
ИИ в госсистемах	Персональные данные
Проект изменений приказа №117. Отдельные меры для моделей, данных и прав ИИ-агентов.	Проект замены приказа №21. Требования к оператору и обработке по поручению.

ФСТЭК подготовила 24 августа 2026 года проект изменений приказа №117. Модели ИИ предлагается размещать в отдельном сегменте системы или инфраструктуры. Для привилегированного доступа в этот сегмент предусмотрены усиленная многофакторная аутентификация, минимальные необходимые права, регистрация и анализ действий пользователей.

Дополнительные меры относятся к моделям, обрабатывающим информацию ограниченного доступа или выполняющим значимые функции оператора. Для них проект предусматривает фильтрацию запросов и ответов, ограничение числа запросов и контроль функциональности модели. Для ИИ-агентов отдельно предложено управление правами доступа к ресурсам системы.

ФСТЭК предложила отдельные меры защиты ИИ-компонентов госсистем · продолжение

Если проект примут, оператору потребуется учитывать назначение ИИ-сервиса при выборе мер. Модель для общедоступных справок и агент с доступом к ведомственной базе получают разный набор ограничений. В проекте обязанности подрядчика по защите предлагается закрепить во внутренних стандартах и регламентах. Предложенная дата начала действия — 1 марта 2027 года.

[Проект №170500](#) · [Техэксперт: изменения приказа №117](#) · [ComNews: проект защиты ИИ в ГИС](#)

[Гарант: текст проекта по защите ИИ](#)

Проект замены приказа ФСТЭК №21 расширяет требования к защите персональных данных

В августе обсуждался проект новых мер защиты персональных данных, подготовленный ФСТЭК 24 июля 2026 года взамен приказа №21. Проект вводит оценку зрелости защиты до начала обработки ПДн, затем не реже одного раза в три года и после компьютерного инцидента.

Проект предусматривает, что оператор устанавливает требуемое значение зрелости и для организации, которая обрабатывает данные по его поручению. Для такого обработчика предусмотрена та же периодичность оценки. Проект добавляет оценку защиты к условиям работы с таким подрядчиком наряду с условиями передачи персональных данных.

В проекте отдельно названы защита контейнеров и их оркестрации, облачных вычислений, API и устройств интернета вещей. Выбор мер привязан к архитектуре, технологиям и актуальным угрозам конкретной системы. Решение о необходимости отдельной модели угроз проект оставляет оператору. При подготовке к изменениям следует проверить прежде всего эти технические зависимости и состав передаваемых подрядчикам данных.

[Проект №169583](#) · [УЦСБ: ключевые изменения](#) · [Кредос: подготовка оператора ПДн](#)

[Гарант: текст проекта по защите ПДн](#)

Сертификаты и цифровое доверие

Минцифры подготовило правила сертификатов НУЦ для сайтов, подписи кода и корпоративного использования

Проект Минцифры от 28 августа 2026 года описывает создание, выдачу, использование и прекращение действия сертификатов безопасности Национального удостоверяющего центра (НУЦ). В перечне одиннадцать видов: корневые и промежуточные сертификаты, доменные сертификаты с разными способами проверки владельца, сертификаты подписи кода и корпоративный сертификат.

Корневые, промежуточные, доменные DV и OV и сертификаты подписи кода предусмотрены в вариантах RSA и ГОСТ. Корпоративный сертификат использует российские алгоритмы. Разработчикам ПО проект задает требования к подтверждению целостности и происхождения программы. Для владельца сайта выбор DV или OV связан со способом подтверждения прав на домен.

При внедрении подписи кода разработчику потребуется проверить, как целевые операционные системы и средства установки проверяют сертификат НУЦ. Поддержка этой цепочки доверия определяет, сможет ли клиент подтвердить происхождение дистрибутива. Предлагаемый срок начала действия правил — 1 марта 2027 года.

[Проект №170667 · Коммерсантъ: «Ключ к доверию»](#)

[Гарант: текст требований к сертификатам НУЦ](#)

Для сертификатов НУЦ предложены дополнительные основания прекращения действия

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.

Проект связывает действие сертификата с конкретной ключевой парой. Если предложенные основания примут, потеря ключа или повторное использование ключа аутентификации могут потребовать замены сертификата до окончания его срока. Проектом предложено начало действия с 1 марта 2027 года.

[Проект №170134 · ComNews: основания отзыва сертификатов · Телеспутник: последствия для владельцев доменов](#)

[Гарант: текст проекта об отзыве сертификатов](#)

Финансовая инфраструктура

Закон о цифровых валютах вводит регулируемых посредников и требования к хранению активов

Федеральный закон от 4 августа 2026 года №282-ФЗ опубликован в день подписания. Основные положения вступили в силу 1 сентября; для отдельных норм установлены более поздние сроки.

Закон вводит регулируемые роли организации обмена цифровых валют и цифрового депозитария. В статье 17 цифровой депозитарий определен как организация, оказывающая услуги по учету и переходу цифровых валют и цифровых прав, а также по предоставлению доступа к адресам-идентификаторам; работать он вправе после включения в реестр Банка России. Статья 52 закрепляет разрешительный контур: перед включением в реестр Банк России проверяет соответствие соискателя требованиям закона и требованиям к защите информации и операционной надежности цифрового депозитария.

Для ИБ особенно значимо появление регулируемого хранения активов. Компрометация ключей может непосредственно привести к утрате имущества клиента. Поэтому защита ключевой информации, разграничение полномочий сотрудников и контроль операций становятся частью условий работы посредника. Конкретные требования к соискателям статуса цифрового депозитария Банк России раскрывает в положении №890-П.

[Закон №282-ФЗ](#) · [Росфинмониторинг: новый режим цифровых валют](#) · [Юридический разбор закона](#)

[Банк России: цифровые депозитарии](#)

Соискателям статуса цифрового депозитария потребуется внешняя оценка ИБ

№890-П и №7429-У: статус на 9 сентября

Оба документа находятся на государственной регистрации в Минюсте.

Положение Банка России от 27 августа 2026 года №890-П определяет квалификационные требования к ключевым сотрудникам участников рынка цифровых валют и условия решений об их допуске. Отдельная глава посвящена защите информации и операционной надежности организации, претендующей на деятельность цифрового депозитария.

Документ предусматривает как минимум стандартный уровень защиты по ГОСТ Р 57580.1-2017 и внешнюю оценку по ГОСТ Р 57580.2-2018 с результатом не ниже четвертого уровня соответствия. Для оценки привлекается организация с лицензией на техническую

защиту конфиденциальной информации. Предусмотрены анализ уязвимостей, пентест и устранение выявленных недостатков.

Для соискателя, который намерен учитывать цифровые активы на администрируемых им адресах, предусмотрено создание и использование ключей в аппаратных модулях безопасности. Требования к прикладному ПО допускают подтверждение безопасности собственной разработки через сертифицированный процесс по ГОСТ Р 56939-2024. Это исключение не распространяется на ПО, которое взаимодействует со средствами криптографической защиты.

Оценка ИБ и проверка ПО входят в подготовку к допуску на рынок. Состав работ зависит от выбранной депозитарием схемы хранения активов и использования ключей.

Организации, планирующей администрировать адреса хранения, нужно заранее заложить аппаратную защиту ключей; разработчику ее платформы — определить, какие программные компоненты взаимодействуют с СКЗИ и требуют отдельного подтверждения безопасности.

Указание Банка России от той же даты №7429-У определяет порядок ведения реестров участников. По состоянию на 9 сентября оба документа находятся на государственной регистрации в Минюсте.

[Положение №890-П](#) · [Указание №7429-У](#) · [Банк России: документы и текущий статус](#)

С 1 сентября крупнейшие банки обязаны предоставлять операции с цифровым рублем

С 1 сентября 2026 года крупнейшие банки должны предоставлять клиентам операции с цифровым рублем. Принимать такую оплату обязаны обслуживаемые ими торговые организации с выручкой за предыдущий год более 120 млн рублей. Для торговых точек с годовой выручкой менее 5 млн рублей предусмотрено исключение. Следующие этапы подключения установлены на 2027 и 2028 годы. Для граждан использование цифрового рубля остается добровольным.

Для банков подключение требует включить новые идентификаторы кошельков и платежные сообщения в антифрод, финансовый мониторинг и расследование спорных операций.

Для торговых организаций основные изменения приходятся на прием платежа, подтверждение его результата и взаимодействие с обслуживающим банком.

Для платежных кодов действует отдельное послабление. Согласно письму Банка России от 21 августа 2026 года №ИН-03-45/30, до 1 марта 2027 года к операторам перевода денежных средств не применяются меры по статье 74 закона о Банке России за указанное в письме несоблюдение требований к универсальному платежному коду. Условие: реквизиты перевода или ссылка на них должны быть закодированы по ГОСТ Р 56042-2014. Банкам, использующим такие коды, предоставлено время на переход; на остальные способы кодирования это послабление не распространено.

[Банк России: этапы внедрения цифрового рубля](#) · [Универсальный платежный код](#) · [Письмо №ИН-03-45/30](#)

[Банк России: текст письма](#)

Ответственность и инфраструктурная безопасность

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.

[Указ №604](#) · [КонсультантПлюс: содержание указа](#)

В проекте развития рынка ЦОД предложено разделить ответственность площадки и владельца данных

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.

Для договора colocation существенны фактические полномочия сторон. 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.

[Юридический разбор предложения об ответственности ЦОД](#) · [Коммерсантъ: дорожная карта развития ЦОД](#) · [Anti-Malware.ru: обсуждение ответственности за утечки](#)

Из межведомственной редакции «Антифрода 3.0» исключили часть требований к иностранным сайтам

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.

[Ведомости: изменения третьего антифрод-пакета](#) · [Юридический разбор требований к хранению данных](#)

ФСТЭК обновила перечни оборудования для лицензиатов

ФСТЭК утвердила два перечня оборудования и программных средств: от 10 августа 2026 года — для работ по технической защите конфиденциальной информации (ТЗКИ), от 11 августа — для разработки и производства средств ее защиты. Состав оснащения в таблицах привязан к виду лицензируемых работ.

В перечне для ТЗКИ названы комплексы пентеста и сканеры с поддержкой Windows, Unix/Linux и взаимодействием с БДУ ФСТЭК. Для услуг мониторинга отдельно указаны песочницы, средства работы с информацией об угрозах, управления событиями и инцидентами, а также защищенные каналы связи. В перечне для разработчиков программных средств защиты предусмотрены статический анализ исходного кода, фаззинг и динамический анализ. Лицензиату нужно сопоставить свою инструментальную базу с соответствующими строками и графами перечня: набор для мониторинга отличается от оснащения для разработки или контроля защищенности.

[Информационное сообщение ФСТЭК №240/13/5521](#) · [Перечень от 10 августа](#) · [Перечень от 11 августа](#)

[Полный перечень для ТЗКИ](#)

[Полный перечень для разработки и производства СЗКИ](#)

06 Новости компаний

Финансовые результаты

Солар: сервисы растут быстрее общей выручки, операционная маржа почти не изменилась

12 августа Солар представил результаты первого полугодия 2026 года по управленческим данным, сформированным в соответствии с принципами МСФО.

Показатель	I полугодие 2025	I полугодие 2026	Изменение
Выручка	8,49 млрд руб. <div><div></div></div>	9,61 млрд руб. <div><div></div></div>	+13,2%
OIBDA	974 млн руб. <div><div></div></div>	1 093 млн руб. <div><div></div></div>	+12,2%
Рентабельность по OIBDA	11,5%	11,4%	−0,1 п. п.

Длина полос: выручка — шкала 0–10 млрд руб.; OIBDA — 0–1,2 млрд руб. У каждой строки своя шкала.

Выручка от сервисов и комплексных проектов увеличилась на 21% в I полугодии 2026 года по сравнению с I полугодием 2025 года. Компания связывает динамику с мониторингом и реагированием, защитой веб-приложений и противодействием DDoS.

Сервисное направление росло быстрее общей выручки, но полугодовая операционная маржа осталась практически на прежнем уровне. Во II квартале 2026 года по сравнению со II кварталом 2025 года выручка выросла на 24,1%, OIBDA на 39,8%.

[Солар: результаты первого полугодия](#) · [Таблицы финансовых результатов](#)

Yandex Cloud: сервисы ИБ используют 53% крупных клиентов

В I полугодии 2026 года по сравнению с I полугодием 2025 года выручка от сервисов ИБ Yandex Cloud увеличилась в 2,7 раза. По итогам полугодия число компаний, использующих Yandex Smart Web Security, выросло в 2,5 раза за год.

Показатель	Результат
Рост выручки от сервисов ИБ: I полугодие 2026 к I полугодию 2025	в 2,7 раза
Рост числа клиентов Smart Web Security за год, по итогам I полугодия 2026	в 2,5 раза
Доля крупных клиентов, использующих сервисы ИБ	I полугодие 2025 и 2026
	2025 <div><div></div></div> 44%
	2026 <div><div></div></div> 53%
Доля Smart Web Security в выручке от сервисов ИБ, I полугодие 2026	22%

Шкала доли: 0–100%.

Рост доли крупных клиентов с подключенными средствами защиты на 9 п. п. показывает расширение использования ИБ-сервисов внутри клиентской базы облака. Smart Web Security формирует более пятой части выручки направления.

Общая выручка Yandex Cloud за I полугодие 2026 года составила 16,7 млрд рублей. Эта сумма относится ко всей облачной платформе; абсолютную выручку ИБ-направления компания в публикации не раскрыла.

[Яндекс: результаты Yandex Cloud за первое полугодие](#)

Idesco увеличила выручку на 32% и повысила рентабельность по EBITDA

По РСБУ выручка Idesco в I полугодии 2026 года выросла на 32% по сравнению с I полугодием 2025 года. За те же периоды рентабельность по EBITDA повысилась с 28% до 33%.

Показатель	I полугодие 2026
Рост выручки к I полугодию 2025	+32%
Рентабельность по EBITDA	33%
Изменение рентабельности по EBITDA к I полугодию 2025	+5 п. п.
Чистый результат за полугодие	Убыток

Во втором квартале компания получила чистую прибыль, однако ее оказалось недостаточно для покрытия убытка первого квартала. Рост продаж и улучшение операционной рентабельности пока не обеспечили положительный чистый результат за полугодие.

[Idesco: отчет за первое полугодие](#) · [Отчетность для инвесторов](#)

ИИ и автоматизация проверок

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. Результат такой проверки — конкретные доступы и пути продвижения к критичным системам, которые необходимо закрыть.

[Positive Technologies: обновление PT Dephaze](#)

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.

[Innostage: TDIR 1.0.0](#)

Мониторинг и реагирование

Обновления SOC-продуктов сокращают разрыв между обнаружением и действием

Реагирование требует полного контекста

Актив	→ Телеметрия	→ Решение	→ Действие
Владелец, критичность, CMDB	Проверить поступление данных	Полномочия и основание действия	Изоляция, блокировка, восстановление

Связь рабочих процессов SOC. Конкретные интеграции продуктов раскрыты в новостях.

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

Обновления SOC-продуктов сокращают разрыв между обнаружением и действием · продолжение

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.

[MaxPatrol 360 2026.2](#) · [PT NAD 13.0](#) · [Kaspersky MDR](#) · [Security Vision 5](#)

[PT NAD 13.0: запускной вебинар](#)

Управление доступом

PAM и средства аутентификации дорабатывают работу с администраторами и изолированными сетями

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.

[BI.ZONE PAM 2.6](#) · [Indeed ITDR 2.2](#) · [MULTIDIRECTORY 3.2.0](#)

Новые услуги и сертификация

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. Исполнение требует совместной работы специалистов по инженерной инфраструктуре, физической безопасности и ИБ.

[K2: комплексная защита промышленного предприятия](#)

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.

[Fuzzy Logic Labs: модуль для цифрового рубля](#) · [CNews: комментарий компании и устройство решения](#)

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.

[Доктор Веб: сообщение от 24 августа](#) · [Сертификаты ФСБ на продукты Dr.Web](#) · [Dr.Web для Авроры](#)

Информзащита

34%

систем управления **инфраструктурой ЦОД** работают на устаревших прошивках

×2

выросло число **атак через уязвимости нулевого дня**
I полугодие 2026 к I полугодию 2025

+58%

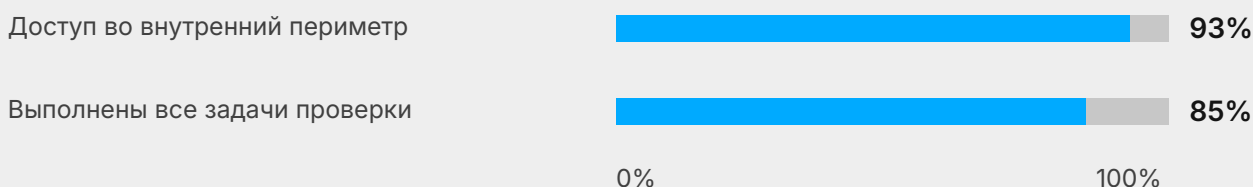
значимых **облачных киберинцидентов**
I полугодие 2026 к II полугодию 2025

07 Тенденции и исследования

Проверка защищенности

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

Два результата одной выборки проектов



Более 100 заказных проектов BI.ZONE, июль 2025 — июль 2026. Задачи определяли для конкретной компании и модели нарушителя.

20 августа BI.ZONE опубликовала результаты более 100 проектов пентеста, AppSec и red team, выполненных с июля 2025 по июль 2026 года. В 93% проектов специалисты получили доступ во внутренний периметр, в 85% выполнили все поставленные задачи проверки. Задачи определяли для конкретной компании и модели нарушителя.

В ходе работ выявлено более 820 уязвимостей, 26% из них отнесены к высокому или критическому уровню опасности. На крупный бизнес приходилось 64% выполненных проектов.

BI.ZONE: результаты проектов наступательной безопасности

В исследовании «Инфосистем Джет» слабее оказались подготовка к атаке и восстановление

Киберустойчивость обследованных компаний

64%

участников получили низкую оценку

50

российских компаний в исследовании

«Инфосистемы Джет»: слабее предотвращение проникновения и подготовка к восстановлению после уничтожения данных.

В опубликованном 17 августа исследовании «Инфосистемы Джет» оценили киберустойчивость 50 российских компаний. Низкую оценку получили 64% участников.

Исследование выделяет слабые участки в начале и конце атаки: предотвращение первоначального проникновения и готовность восстановиться после уничтожения или шифрования данных. Защита внутри инфраструктуры в обследованных организациях развита лучше.

Это различие важно для планирования работ. Установка средств обнаружения внутри сети не закрывает проблемы внешних сервисов и не обеспечивает восстановление бизнеса после инцидента. Проверка резервных копий должна включать восстановление конкретной системы, а план реагирования — распределение решений между ИБ, ИТ и владельцем бизнес-процесса.

[Инфосистемы Джет: исследование киберустойчивости](#)

Веб-атаки и фишинг

WMX и ServicePipe: 44% веб-атак были многоэтапными

3 августа WMX и ServicePipe представили результаты наблюдений за инфраструктурой почти 600 крупных организаций в первом полугодии 2026 года.

WMX и ServicePipe: 44% веб-атак были многоэтапными · продолжение

Показатель	Результат
Зафиксированные веб-атаки, I полугодие 2026	849,7 млн
Изменение их количества к I полугодию 2025	+27%
Доля многоэтапных атак, I полугодие 2026	44%
	<div><div></div></div>
Рост автоматизированной разведки	Вдвое: I полугодие 2026 к I полугодию 2025
Рост числа DDoS-атак мощностью свыше 100 Гбит/с	В пять раз в I полугодии 2026; база сравнения не указана

Шкала доли: 0–100%.

Авторы описывают сочетание разных способов воздействия: DDoS перегружает сервис и отвлекает защитников, а параллельная атака направлена на приложение, API или бизнес-логику.

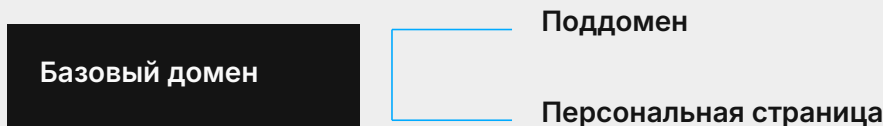
Для владельца интернет-сервиса это требует совместного разбора событий сетевой защиты, WAF и приложения. Проверка доступности сайта не выявит, например, злоупотребление платёжной функцией, если она продолжает отвечать на запросы. В реагировании должны участвовать и специалисты по приложению, которые понимают нормальное поведение пользователей и операций.

Данные описывают инфраструктуру, наблюдаемую WMX и ServicePipe.

[WMX и ServicePipe: отчет за первое полугодие](#)

BI.ZONE: сокращение числа фишинговых доменов сопровождается их повторным использованием

Один домен может обслуживать несколько атак



BI.ZONE DRP связывает снижение числа заблокированных доменов с повторным использованием инфраструктуры. Количество доменов не описывает количество атак.

В I полугодии 2026 года BI.ZONE DRP заблокировала более 13,5 тыс. фишинговых доменов — на 73% меньше, чем в I полугодии 2025 года. Компания связывает снижение с изменением способа работы атакующих: один базовый домен используется многократно, а под отдельных адресатов создаются поддомены и персонализированные страницы.

Поэтому уменьшение числа доменов не означает пропорционального сокращения атак. Для мониторинга бренда и фишинга важны повторное использование инфраструктуры и изменения страниц, уже связанных с известным доменом.

Отчет Threat Zone 2026 дополняет эту картину со стороны продажи доступов. BI.ZONE изучила более 35 тыс. объявлений на теневых площадках за период с лета 2025 по лето 2026 года. Доступы продаются вместе со сведениями об организации и ее инфраструктуре; отдельную ценность имеют сессии и токены. Авторы отмечают и составные утечки, когда старые базы объединяют и предлагают как новый массив.

Для компании обнаружение своих учетных данных на внешней площадке должно вести к проверке активных сессий, токенов и связанных доступов. Простая смена пароля не всегда завершает уже выданную сессию. При оценке утечки нужно установить, какие записи действительно новые, а какие повторно опубликованы.

[BI.ZONE: персонализированный фишинг](#) · [Полный отчет Threat Zone 2026](#) · [Основные результаты Threat Zone](#)

Уязвимости и малый бизнес

«Лаборатория Касперского»: число критических уязвимостей во втором квартале выросло на 34%

26 августа «Лаборатория Касперского» опубликовала анализ критических уязвимостей на основе записей CVE, GHSA и банка данных угроз ФСТЭК.

Период	Критические уязвимости в анализируемой базе	К тому же периоду 2025 года
II квартал 2026 года	Около 2 700	+34%
I полугодие 2026 года	Около 5 200	+47%

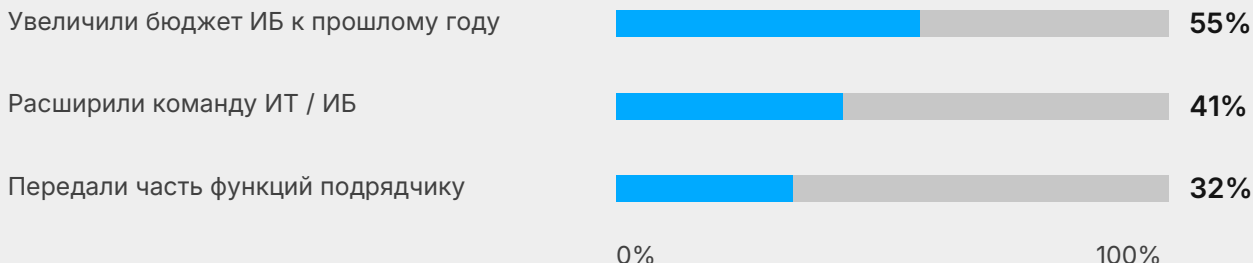
II квартал входит в I полугодие. Показатели за эти периоды не складываются.

Рост увеличивает объем задач для команд управления уязвимостями. Очередность исправлений должна учитывать наличие уязвимого компонента в инфраструктуре, доступность системы извне и возможность эксплуатации. В отчете рассматриваются случаи появления средств эксплуатации до выпуска исправления — для таких ситуаций нужны временные меры защиты до установки патча.

[«Лаборатория Касперского»: критические уязвимости во втором квартале](#) · [Securelist: уязвимости и эксплойты](#)

В российской части опроса «Лаборатории Касперского» 82% представителей МСБ сообщили об инцидентах

Какие меры называли участники опроса



Российская часть опроса «Лаборатории Касперского»: размер подвыборки не раскрыт. Весь опрос: 1 800 респондентов, 18 стран. Ответы могут пересекаться.

18 августа «Лаборатория Касперского» представила результаты международного опроса 1 800 респондентов из 18 стран. В российской части 82% представителей малого и среднего бизнеса сообщили о киберинцидентах за последний год. Размер российской подвыборки отдельно не раскрыт.

Среди названных угроз — вредоносное ПО, эксплуатация уязвимостей и несанкционированный удаленный доступ. Об увеличении бюджета ИБ по сравнению с предыдущим годом сообщили 55% российских респондентов, о расширении команды ИТ или ИБ — 41%, о передаче части функций внешним исполнителям — 32%. Эти ответы показывают, какие способы усиления защиты выбирали участники опроса.

[«Лаборатория Касперского»: киберугрозы для малого и среднего бизнеса](#)

08 Сотрудничество и интеграции

Совместимость с инфраструктурными платформами

KUMA и VK Object Storage проверили на архиве объемом 3 ПБ

KUMA + VK Object Storage: условия испытаний

Оперативные данные

Быстрое хранение

Холодный архив

VK Object Storage / HDD

3 ПБ

массив данных

>6 000

запросов в секунду

10 ТБ

прирост за сутки

Недавние события остаются на быстром хранении; холодный архив размещается в объектном хранилище на HDD. Числа описывают испытание.

«Лаборатория Касперского» и VK Tech подтвердили совместимость KUMA с VK Object Storage. Испытания проводились на массиве 3 ПБ, при нагрузке более 6 тыс. запросов в секунду и ежедневном приросте данных 10 ТБ.

Проверенная схема разделяет оперативные данные SIEM и холодный архив. Недавние события остаются на быстром хранении, архив размещается в объектном хранилище на HDD. Для крупных SOC это позволяет отдельно планировать производительность поиска по текущим событиям и емкость длительного хранения.

«Лаборатория Касперского» и VK Tech: результаты испытаний

Проверенные связки инфраструктурных платформ		
KUMA	↔ VK Object Storage	Разделение оперативных данных и архива
BI.ZONE	↔ Postgres Pro	Редакции и версии зависят от продукта
InfoWatch	↔ Deckhouse + Astra Linux SE	Испытано конкретное сочетание среды
R-Vision VM	↔ «Штурвал»	Проверены функции и масштабирование

BI.ZONE подтвердила совместимость пяти классов решений с Postgres Pro

13 августа BI.ZONE сообщила о совместимости EDR, PAM, Mail Security, WAF и Secure DNS с определенными редакциями и версиями Postgres Pro. Набор поддерживаемых версий различается по продуктам: например, для WAF указаны Standard и Enterprise 16–18, для PAM — Enterprise 18.

При проектировании связки необходимо сверять конкретные версии СУБД и ИБ-продукта.

[BI.ZONE: перечень совместимых решений и версий](#)

InfoWatch и Флант подтвердили совместимость восьми продуктов

17 августа Deckhouse сообщила о завершении совместных испытаний с InfoWatch в среде Astra Linux SE. С Deckhouse Kubernetes Platform проверены Traffic Monitor, Activity Monitor, Device Monitor и Vision, а также Device Control, Data Discovery, Prediction и Data Access Tracker. Это подтверждение конкретного сочетания продуктов, контейнерной платформы и операционной системы.

[InfoWatch: совместимость с Deckhouse](#)

[Флант: результаты совместных испытаний](#)

[Deckhouse: результаты испытаний](#)

R-Vision VM проверили для работы на платформе «Штурвал»

28 августа R-Vision и «Лаборатория Числитель» объявили технологическое партнерство. Испытания подтвердили работу R-Vision VM на контейнерной платформе «Штурвал», включая сохранение функций и масштабирование.

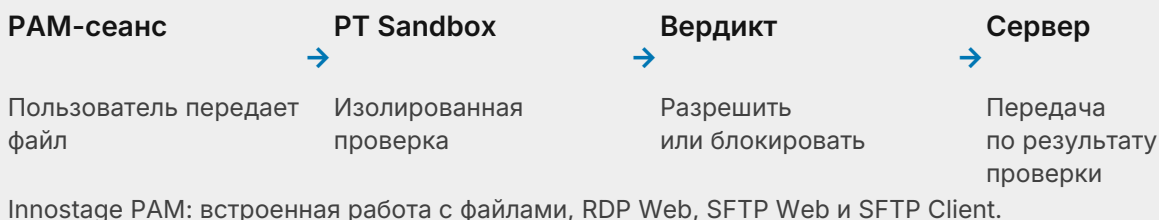
Для заказчиков это вариант размещения системы управления уязвимостями в собственной Kubernetes-инфраструктуре.

[R-Vision и «Лаборатория Числитель»: результат испытаний](#)

Доступ, проверка файлов и мобильные устройства

Innostage PAM передает файлы в PT Sandbox до загрузки на целевой ресурс

Проверка файла до передачи на сервер



Интеграция Innostage PAM и PT Sandbox добавляет проверку файлов в привилегированные сеансы. PAM направляет файл в изолированную среду песочницы и по ее вердикту разрешает или блокирует передачу на сервер.

Испытания охватили встроенные средства работы с файлами, RDP Web, SFTP Web и SFTP Client. Это закрывает отдельный риск административного доступа: легитимный пользователь может передать на критичный ресурс зараженный файл.

[Innostage: проверка файлов через PT Sandbox](#)

SECURITM подключила двухфакторную аутентификацию САКУРА

10 августа SECURITM сообщила об интеграции с САКУРА: после логина и пароля вход подтверждается в мобильном приложении, без одноразового кода. Сценарий работает в локальном контуре организации; включение и отключение двухфакторной аутентификации фиксируется в журнале безопасности.

[SECURITM: интеграция с САКУРА](#)

MULTIFACTOR стал доступен клиентам Selectel

26 августа МУЛЬТИФАКТОР и Selectel представили совместное предложение по подключению облачной двухфакторной аутентификации. Оно адресовано компаниям, использующим инфраструктуру и сервисы Selectel.

[Selectel: подключение MULTIFACTOR](#)

SafeMobile и MIG предложили устройства с готовым централизованным управлением

SafeMobile и MIG выпустили совместный ПАК на базе смартфонов MIG S6, MIG A65 и планшета MIG T8X. При первом запуске устройство подключается к системе управления заказчика через QR-код и получает настройки.

Для предложения предусмотрена специальная лицензия UEM SafeMobile, работающая только на устройствах MIG. Заказчик получает заранее проверенную связку оборудования и управления, но при планировании смешанного парка должен учитывать ограничение лицензии по производителю.

[SafeMobile: состав решения и лицензирование](#) · [CNews: совместное предложение MIG и SafeMobile](#)

DS Proxima и MITIGATOR проверили распределенную очистку DDoS-трафика

25 августа НПП «Цифровые решения» сообщило об испытаниях DS Proxima совместно с MITIGATOR. Балансировщик распределяет трафик между узлами очистки и сохраняет прохождение прямого и обратного трафика соединения через один узел. Это необходимо для работы контрмер на основе TCP Splicing.

Для защиты приложений проверена балансировка запросов между экземплярами MITIGATOR Web Challenger. Связка позволяет наращивать число узлов проверки при росте нагрузки.

[НПП «Цифровые решения»: проверенные сценарии](#)

Партнерства и канал продаж

С-Терра и «Газпром нефть» подписали соглашение о сотрудничестве

14 августа, на закрытии IT Camp 2026, С-Терра и «Газпром нефть» подписали соглашение о стратегическом сотрудничестве в области ИТ. Компания сообщила о соглашении 19 августа.

[С-Терра: соглашение с «Газпром нефтью»](#)

Zecurion расширяет сотрудничество с VertexMon в Монголии

11 августа Zecurion сообщила о развитии партнерства с VertexMon, начавшегося в 2023 году. Сотрудничество охватывает DLP, контроль доступа к данным и защиту веб-доступа. Компании работают с заказчиками финансового, государственного, телекоммуникационного и промышленного секторов Монголии.

[Zecurion: развитие партнерства с VertexMon](#)

В SolarShip стало 455 партнеров

5 августа 2026 года Солар сообщил, что программа SolarShip объединяет 455 партнеров; в I полугодии 2025 года их было около 300. За два года через программу реализовано более 1 100 проектов.

По данным компании, выручка через партнерский канал выросла на 50% год к году; точный отчетный интервал не указан. Среди востребованных направлений названы безопасная разработка, контейнерная безопасность, DLP, защита веб-доступа и управление привилегированным доступом.

[Солар: результаты партнерской программы](#)

Партнеры R-Vision выделили сопровождение и интеграцию в числе условий выбора VM

12 августа R-Vision опубликовала результаты опроса 43 респондентов из числа представителей партнеров, интеграторов и дистрибьюторов. Ответы собирались с 12 февраля по 9 апреля 2026 года.

Участники отмечают спрос на полный процесс управления уязвимостями, включая работу после сканирования. При выборе решения существенны поддержка интегратора, результаты пилота и совместимость с архитектурой заказчика. Среди трудностей внедрения — встраивание продукта в существующие процессы и нехватка специалистов у клиента.

Для проекта VM это означает необходимость заранее определить, кто получает результаты сканирования, кто отвечает за исправления и как повторно проверяется устранение уязвимости. Эти задачи должны входить в состав внедрения вместе с настройкой самого продукта.

[R-Vision: опрос партнеров по VM](#)

09 Реестры и сертификация

Минцифры

Новые записи о программном обеспечении и ПАК

Два вида подтверждения	
Минцифры Запись о ПО или ПАК. Назначение и состав продуктовой семьи раскрыты в таблице.	ФСТЭК Сертификат средства защиты. Даты внесения в реестр отделены от дат выдачи сертификатов.

Продукт	Разработчик	Назначение и изменение
Встроенное ПО криптомаршрутизатора «Грифон»	НПП «Цифровые решения»	Встроенное ПО криптомаршрутизатора для шифрования и имитозащиты данных в территориально распределенных сетях. Запись №34634 от 4 августа 2026 года.
Централизованная система управления и мониторинга «Аргос FW»; ПАК «Аргос FW» Y.V02	TexAproс	ПО централизованного управления: запись №34658 от 4 августа 2026 года. ПАК межсетевого экрана «Аргос FW» Y.V02: №34815 от 18 августа 2026 года. Это разные компоненты одной продуктовой семьи.
ПК УИБ	«Управление информационной безопасности»	Автоматизация работы с документацией и мероприятиями ИБ, контроль выполнения требований. Запись №34703 от 4 августа 2026 года.
Coshkey 2.0	Фриматик	Корпоративное хранилище паролей для коробочного Битрикс24: разграничение доступа, группировка учетных данных и журналирование. Запись №34664 от 4 августа 2026 года.

Для «Аргос FW» августовские записи дополняют ранее зарегистрированный продукт: сам межсетевой экран уже присутствовал в реестре российского ПО с ноября 2024 года. В продуктовой линейке предусмотрены сегментация сети, NAT, управление через REST API и отказоустойчивая конфигурация Active–Standby.

Грифон: [страница продукта](#) · Аргос FW: [описание семейства](#) · ПК УИБ: [сообщение разработчика о включении](#) · Coshkey 2.0: [карточка продукта](#) · Freematiq: [разработчик Coshkey](#)

ФСТЭК

«Комплекс ФПСУ версии 3» получил сертификат

3 августа 2026 года в реестр ФСТЭК внесен сертификат №5093 на комплекс «ФПСУ» версии 3 компании «Амикон». Срок действия — 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.

[Амикон: сертификаты на комплекс ФПСУ](#)

Другие записи, внесенные в реестр в августе:

13 августа — «Кабинет администратора начислений» информационной системы РНИП, сертификат №5095; заявитель — Департамент информационных технологий города Москвы.

14 августа — [Dionis-SMP](#), №5096; заявитель — ООО «Фактор-ТС».

19 августа — «Миллион призов», №5097, и «Портал инфраструктурных подключений», №5098; заявитель — ГКУ «Инфогород».

20 августа — «Сервис аутентификации и каталог управления пользователями», №5099, и «Модуль мониторинга транспортных событий», №5100; заявитель — ГКУ «Инфогород».

21 августа — «Система мониторинга инцидентов в сферах деятельности органов исполнительной власти города Москвы», №5101; заявитель — Департамент информационных технологий города Москвы.

24 августа — «Расчет АЭП», №5103; заявитель — ООО «НОВО». Комплекс рассчитывает показатели эффективности защиты речевой информации от утечки за счет акустоэлектрических преобразований. В записи указаны технические условия и методика АЭП-2018; сертификат действует до 24 августа 2031 года.

[ФПСУ версии 3: сертификаты «Амикон»](#) · [Dionis-SMP: страница продукта](#) · [Расчет АЭП: ООО «НОВО»](#)

Спасибо за внимание!

ИЗ | информзащита
infosec.ru

Автор: Елена Рухлова

Ведущий аналитик Департамента маркетинга
ГК «Информзащита»

