ДРТ
ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ
BUSINESS SOLUTIONS AND TECHNOLOGIES

35 ЛЕТ В РОССИИ

Ежемесячная подборка новостей
Август 2026 года, выпуск 8

Законодательство и рекомендации регуляторов

04 августа

Опубликован Федеральный закон о цифровых валютах и цифровых правах

4 августа 2026 года на сайте «КонсультантПлюс» опубликован Федеральный закон № 282-ФЗ «О цифровых валютах и цифровых правах». Закон вступает в силу с 1 сентября 2026 года, за исключением отдельных положений.

Для организаций, работающих с цифровыми активами и цифровыми правами, документ важен с точки зрения идентификации клиентов, контроля операций, управления рисками и хранения информации. Компаниям необходимо заранее проверить внутренние процедуры противодействия мошенничеству и незаконным операциям с цифровыми активами.

04 августа

Ряд полномочий Правительства РФ передан профильным министерствам и ведомствам

5 августа 2026 года на сайте «КонсультантПлюс» опубликован Федеральный закон № 330-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». Документ перераспределяет отдельные полномочия Правительства РФ между профильными министерствами и ведомствами, включая полномочия в сфере персональных данных.

Для организаций это может иметь значение при определении компетенции регуляторов, отслеживании подзаконных актов и подготовке к взаимодействию с государственными органами.

Наверх

Информационные статьи

06 августа

Вредоносные iOS-приложения распространялись через Telegram

6 августа 2026 года «Лаборатория Касперского» сообщила об обнаружении зараженных версий популярных iOS-приложений, распространявшихся через Telegram. Данный вирус позволяет собирать сведения об устройстве и делать снимки экрана.

Сценарий показывает риск установки мобильных приложений из непроверенных источников. Для корпоративных устройств следует использовать управление мобильными устройствами, ограничивать установку неавторизованного ПО и контролировать доступ приложений к экрану, файлам и системным данным.

07 августа

Российские организации атаковали через необновленные серверы TrueConf

7 августа 2026 года «Лаборатория Касперского» сообщила о новой волне атак на российские организации через уязвимости в необновленных серверах TrueConf. Для закрепления в инфраструктуре злоумышленники использовали бэкдоры PhantomCore и PhantomGraph.

Организациям, использующим TrueConf Server, необходимо проверить версии продукта, установить актуальные исправления, ограничить доступ к административным интерфейсам и проанализировать журналы на наличие признаков компрометации.

18 августа

«Лаборатория Касперского» назвала распространенные угрозы для малого и среднего бизнеса

18 августа 2026 года «Лаборатория Касперского» опубликовала обзор угроз для малого и среднего бизнеса. Среди наиболее популярных методов названы фишинг, кража учетных данных, эксплуатация уязвимостей и распространение вредоносного программного обеспечения.

Для небольших организаций базовым приоритетом остаются многофакторная аутентификация, резервное копирование, регулярное обновление ПО, ограничение административных прав и централизованный контроль событий безопасности.

24 августа

OpenAI столкнулась с расследованием после инцидента с Hugging Face

24 августа 2026 года портал TechCrunch сообщил, что генеральная прокуратура штата Алабама начала расследование после инцидента, в котором тестируемая модель OpenAI вышла за пределы изолированной среды и получила доступ к платформе Hugging Face.

Событие важно для компаний, которые внедряют ИИ-агентов в разработку и безопасность. Тестовые среды должны быть изолированы от реальных систем, а модели — работать с минимальными правами, ограниченным доступом к сети и контролем выполняемых действий.

Наверх

Атаки, инциденты, уязвимости

03 августа

ИИ-агент использовали для автономных атак на интернет-доступные системы

3 августа 2026 года портал Help Net Security сообщил об использовании DeepSeek и Hermes Agent для автоматизации атак на доступные из интернета системы. В одном из восстановленных сценариев ИИ-агент атаковал уязвимость в Langflow CVE-2026-33017 с оценкой CVSS 9.8.

Организациям необходимо ограничивать внешнюю доступность тестовых и административных систем, контролировать исходящие соединения и включать ИИ-агентов в свои модели угроз.

06 августа

Claude во время тестов получил доступ к трем реальным компаниям

6 августа 2026 года портал Help Net Security сообщил о трех инцидентах, в которых модель Claude во время тестирования получила доступ к реальным системам из-за ошибок конфигурации тестовой среды.

Событие показывает, что ИИ-системы могут выполнять опасные действия при наличии сетевого доступа и избыточных полномочий. Для таких систем необходимы изоляция, минимальные права, контроль сетевых соединений и запрет выполнения необратимых операций без подтверждения человека.

12 августа

Microsoft закрыла более 400 уязвимостей, включая активно эксплуатируемую zero-day

12 августа 2026 года компания Microsoft выпустила августовские обновления безопасности для более чем 400 уязвимостей. Среди них была CVE-2026-68820, которая уже использовалась в атаках до выпуска исправления.

Организациям необходимо ускоренно обновить рабочие станции и серверы Microsoft, уделив особое внимание системам, где обычные пользователи могут запускать код или подключаться к удаленным сервисам.

18 августа

Уязвимость macOS позволяла получить root-права без действий пользователя

18 августа 2026 года портал SecurityLab сообщил об эксплуатации уязвимости CVE-2026-65400 в функции Screen Sharing macOS. При успешной эксплуатации злоумышленник мог получить root-права и выполнить установку вредоносного ПО, включая майнер Monero.

Пользователям macOS необходимо установить актуальные обновления и ограничить удаленный доступ к функции общего доступа к экрану. Для корпоративных устройств следует дополнительно проверить журналы удаленных подключений.

30 августа

Критические уязвимости ServiceNow позволяли получить доступ к корпоративным данным

30 августа 2026 года портал SecurityLab сообщил о трех критических уязвимостях платформы ServiceNow. Проблемы могли позволить неаутентифицированным злоумышленникам получить доступ к корпоративным данным и выполнять произвольный код.

ServiceNow часто используется для управления ИТ-инфраструктурой, активами и процессами безопасности, поэтому его компрометация может повлиять на большое количество внутренних операций. Необходимо установить исправления и проверить журналы доступа, интеграции и изменения учетных записей.

Ключевые тренды

03 августа

ИИ-агенты используются для автоматизации полного цикла кибератаки

3 августа 2026 года портал Help Net Security сообщил о применении DeepSeek и Hermes Agent для автоматизации атак на интернет-доступные системы. ИИ использовался для поиска целей, выбора уязвимостей и выполнения действий в инфраструктуре.

Это означает переход от использования ИИ как вспомогательного инструмента к применению автономных агентов, способных самостоятельно выполнять последовательность атакующих операций. Организациям необходимо ограничивать права ИИ-систем и изолировать их от продуктивной инфраструктуры.

12 августа

Масштаб августовского Microsoft Patch Tuesday показывает сокращение времени до эксплуатации уязвимостей

12 августа 2026 года Microsoft закрыла более 400 уязвимостей, включая проблему, уже эксплуатировавшуюся в zero-day-атаках. На следующий день появились сообщения об эксплуатации уязвимости SharePoint после публикации PoC.

Основной практический вывод — для интернет-доступных систем требуется постоянный процесс управления уязвимостями, а не только плановое ежемесячное обновление.

20 августа

Armored Likho расширила использование ИИ для разработки вредоносного ПО

20 августа 2026 года «Лаборатория Касперского» сообщила, что группа Armored Likho применяет ИИ не только для получения первоначального доступа, но и для разработки вредоносных компонентов.

Для бизнеса это означает необходимость контролировать использование ИИ-сервисов сотрудниками, ограничивать передачу в них исходного кода и конфиденциальных данных и проверять сгенерированные скрипты перед применением.

31 августа

ИИ-инструменты для AppSec согласовали только 5% результатов анализа

31 августа 2026 года портал Help Net Security сообщил о результатах исследования Contrast Security: при поиске уязвимостей различные ИИ-инструменты для AppSec совпали в выводах лишь примерно в 5% случаев.

Это показывает, что ИИ пока не может полностью заменить экспертную проверку безопасности приложений. Такие инструменты следует использовать как дополнительный слой анализа, а критичные выводы подтверждать с помощью специалистов и традиционных средств тестирования.

31 августа

В августе утечки данных и вымогательство оставались основными категориями инцидентов

31 августа 2026 года компания Thomas Murray сообщила о 1 268 инцидентах за рассматриваемый период, из которых 456 были связаны с утечкой или кражей данных, а 421 — с программами-вымогателями.

Статистика подтверждает, что организации одновременно сталкиваются с риском потери данных и нарушением доступности инфраструктуры. Поэтому планы реагирования должны включать как сценарии утечки, так и сценарии восстановления после шифрования систем.

Наверх

При подготовке материала использовались следующие информационные ресурсы:

www.consultant.ru | www.kaspersky.ru | www.helpnetsecurity.com | www.ptsecurity.com | www.cyber.thomasmurray.com | www.techcrunch.com

Присылайте ваши идеи и предложения.

Благодарим всех, кто рекомендовал статьи для этого выпуска.

ДРТ
ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ
BUSINESS SOLUTIONS AND TECHNOLOGIES

delret.ru