ДРТ
ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ
BUSINESS SOLUTIONS AND TECHNOLOGIES

35 ЛЕТ В РОССИИ

Ежемесячная подборка новостей

Февраль 2026 года, выпуск #

Законодательство и рекомендации регуляторов

6 февраля

Правительство РФ утвердило отраслевые особенности категорирования КИИ в банковской сфере

Правительство РФ приняло Постановление № 92, закрепляющее отраслевые особенности категорирования объектов критической информационной инфраструктуры в банковской и иных сферах финансового рынка. Документ вступает в силу 15 февраля 2026 года. Поправки к Федеральному закону № 187-ФЗ усиливают технологическую независимость и безопасность КИИ.

28 февраля

Уже 1 марта 2026 года начинает действовать новый приказ ФСТЭК

Нормативный акт устанавливает обновленные требования к защите информации, содержащейся в ГИС. В связи с утверждением нового приказа утратят силу прежние требования, которые регламентировал Приказ ФСТЭК от 11 февраля 2013 года № 17.

Наверх

Информационные статьи

1 февраля

Аналитики сообщили о росте объема утечек данных из российских сервисов

Forbes пересказывает выводы исследователей: несмотря на снижение числа зафиксированных утечек, общий объем похищенных данных российских пользователей вырос примерно в 1,5 раза, а крупнейшие инциденты приходятся на государственные и окологосударственные сервисы, что усиливает регуляторное давление и подталкивает компании к пересмотру моделей угроз и подходов к защите персональной информации.

2 февраля

Главные киберугрозы 2026 года и динамика утечек данных

Отчет F6 «Киберугрозы в России и Беларуси. Аналитика и прогнозы 2025/26» фиксирует рост числа действующих APT-групп с 24 до 27 и 250 публичных утечек баз данных компаний СНГ (230 — российские), причем суммарный объем похищенных данных увеличился с 457 до 767 млн строк, а фокус атак смещается от массовых кампаний к разрушительным инцидентам с остановкой бизнеса, крупными выкупами и информационным давлением на жертв.

11 февраля

Утечки данных через публичные ИИ-сервисы выросли в 30 раз

Аналитики, исследовавшие трафик около 150 российских компаний, зафиксировали 30-кратный рост объема конфиденциальных данных, передаваемых через публичные ИИ-сервисы, при этом примерно 60% организаций не имеют формализованных правил

использования ИИ, что превращает такие сервисы в новый канал утечек; в качестве противодействия предлагается ограничивать доступ к внешним моделям, разворачивать корпоративные изолированные решения и вводить регламент по работе с конфиденциальной информацией при использовании ИИ.

11 февраля

Ответственность за кибербезопасность в 2026 году: что грозит представителям бизнеса и руководителям

Помимо обзора правовых рисков, авторы дают конкретные рекомендации: формализовать процессы управления ИБ-рисками, закрепить зоны ответственности между ИТ, ИБ и бизнес-подразделениями, пересмотреть договоры с подрядчиками с учетом требований по защите данных и порядку реагирования на инциденты, а также регулярно проводить учения и фиксировать все мероприятия по безопасности для снижения рисков возникновения претензий со стороны регуляторов.

12 февраля

Киберугрозы представителей малого и среднего бизнеса в 2026 году: как выстроить защиту

Материал оценивает ущерб представителей МСБ от кибератак примерно в 1,5 трлн руб. и фиксирует рост числа атак на 35%, при этом злоумышленники все чаще используют фишинг, стилеры, атаки на цепочки поставок и эксплуатацию удаленных сервисов, а компании страдают от нехватки ИБ-специалистов; в качестве минимального набора мер предлагаются инвентаризация активов, базовая сегментация сети, многофакторная аутентификация, резервное копирование и подключение к аутсорсинговым службам мониторинга и реагирования.

25 февраля

Исследование: утекшие пароли используют для взлома уже через неделю

Российский сервис разведки утечек данных и мониторинга даркнета DLBI провел исследование скорости распространения утечек данных, содержащих логины и пароли пользователей.

25 февраля

Claude Code вызвал панику у специалистов по безопасности: ИИ-ассистент получил слишком много прав

В сообществе специалистов по безопасности разгорелась дискуссия вокруг инструмента Claude Code после того, как эксперты указали на риски, связанные с его доступом к локальной среде разработки.

Наверх

Атаки и инциденты

6 февраля

Хакеры похитили у Substack данные почти 700 тыс. пользователей

Платформа рассылок Substack сообщила о компрометации, в результате которой злоумышленники получили дамп с 697 313 записями, включающими адреса электронной почты, телефоны и часть служебных данных пользователей; по заявлениям компании, пароли и платежные данные не затронуты, однако инцидент повышает риск таргетированного фишинга и злоупотребления контактной информацией подписчиков и авторов рассылок.

10 февраля

30-летняя уязвимость в libpng поставила под удар миллионы приложений

Анонсирован выпуск libpng 1.6.55 с патчем для опасной уязвимости, присутствовавшей в коде более 28 лет. Уязвимость классифицируется как переполнение буфера в куче, зарегистрирована под идентификатором CVE-2026-25646 и получила 8,3 балла по шкале CVSS. Уязвимости подвержены все версии libpng с 0.90 beta до 1.6.54. Ввиду широкого использования библиотеки пользователям настоятельно рекомендуется перейти на сборку 1.6.55 от 10 февраля 2026 года.

11 февраля

Japan Airlines пострадала от кибератаки, скомпрометированы данные клиентов

9 февраля 2026 года Japan Airlines обнаружила несанкционированный доступ к своим системам. Кибератака скомпрометировала данные клиентов, использовавших сервис с июля 2024 года, включая имена, номера телефонов, адреса электронной почты и информацию о поездках, такую как аэропорты вылета и прибытия, названия отелей и номера рейсов. Это один из крупнейших инцидентов в авиационной отрасли Японии.

11 февраля

Февральские патчи Microsoft устранили шесть активно эксплуатируемых уязвимостей

Microsoft выпустила февральский пакет патчей, закрыв 58 уязвимостей, включая шесть активно эксплуатируемых уязвимостей нулевого дня (0-day) и три публично раскрытых дыры. Пять уязвимостей получили статус критически важных. Помимо устранения уязвимостей, Microsoft начала развертывание новых сертификатов Secure Boot взамен сертификатов 2011 года, срок действия которых истекает летом 2026 года. Февральский пакет стал одним из наиболее заметных в этом году.

16 февраля

Google закрыла первую эксплуатируемую дыру в Chrome в 2026 году

Google выпустила экстренное обновление Chrome, закрывающее опасную уязвимость CVE-2026-2441, которая уже используется в реальных атаках. Это первая уязвимость нулевого дня, пропатченная разработчиками с начала 2026 года. В официальном сообщении Google подтвердила активную эксплуатацию уязвимости злоумышленниками. Пользователям рекомендуется немедленно обновить браузер до последней версии.

20 февраля

Odido: утечка данных затронула более 6 млн клиентов в Нидерландах

Нидерландская телекоммуникационная компания Odido подтвердила кибератаку, затронувшую личную информацию более 6 млн аккаунтов. Украденная информация включает имена клиентов, номера телефонов, адреса электронной почты, номера банковских счетов и паспортные данные. Компания сообщила, что атака была впервые обнаружена 7 февраля, несанкционированный доступ к системе был прекращен. Это один из крупнейших инцидентов в телекоммуникационном секторе Европы.

24 февраля

Злоумышленник взломал более 600 брандмауэров Fortinet через подбор паролей

Неизвестный атакующий просканировал интернет на наличие административных интерфейсов Fortinet по стандартным портам и получил доступ более чем к 600 устройствам, используя перебор типовых и слабых паролей, после чего мог изменять конфигурацию, перехватывать трафик и использовать скомпрометированные брандмауэры как плацдарм для дальнейших атак на внутренние сети компаний, что еще раз подчеркивает необходимость отказа от дефолтных учетных записей и ограничения доступа к административным панелям из интернета.

25 февраля

Вероятно, крупнейшая утечка в истории

Одна из крупнейших компаний, обслуживающих американские страховые программы, оказалась в центре масштабной утечки данных, которая продолжает увеличиваться. Речь идет о Conduent — подрядчике, обрабатывающем платежи, печать и документы для крупных медицинских страховщиков.

Наверх

Ключевые тренды

3 февраля

Анализ активности хакерских группировок, IV квартал 2025 года

В IV квартале 2025 года департамент Threat Intelligence PT ESC продолжил мониторинг активности хакерских группировок, нацеленных на российские организации. Внимание было сосредоточено на выявлении и сопоставлении повторяющихся паттернов атак, техник и семейств вредоносного ПО с ретроспективой предыдущих кварталов и лет. Такой подход позволяет не только описывать отдельные инциденты, но и подтверждать устойчивые паттерны группировок на примере сопоставимых цепочек.

10 февраля

Positive Technologies представила февральский дайджест трендовых уязвимостей

Эксперты Positive Technologies представили февральский дайджест трендовых уязвимостей, включающий критические проблемы в популярных приложениях и сервисах. Дайджест содержит анализ наиболее опасных уязвимостей, выявленных в феврале 2026 года, с рекомендациями по их устранению. Документ помогает компаниям оперативно реагировать на новые угрозы и своевременно обновлять используемое ПО.

11 февраля

Краткий дайджест отчета «Лаборатории Касперского» по спаму и фишингу за 2025 год

За 2025 год система антифишинга «Лаборатории Касперского» предотвратила более 554 млн попыток перехода по фишинговым ссылкам, а почтовый антивирус заблокировал почти 145 млн вредоносных вложений. При этом почти 45% всех электронных писем в мире оказались спамом. В отчете разобраны самые яркие примеры фишинговых и спамерских схем прошлого года. Мошенники изобретают новые способы обмана, используя темы криптовалют, искусственного интеллекта и актуальных событий.

19 февраля

Количество кибератак на финансовые учреждения в России выросло на 43%

Согласно бюллетеню «Лаборатории Касперского» «Киберпульс.Финансы», представленному на Уральском форуме «Кибербезопасность в финансах», финансовая отрасль остается одной из самых атакуемых в России: в 2025 году по сравнению с 2024 годом количество кибератак выросло на 43%. В четыре раза увеличилось число атак с применением банкеров, на 42% — число атак со шпионским ПО, на 32% — с программами-вымогателями.

24 февраля

Законодательные тренды: антифрод-меры и регулирование цифровых платформ

Обзор описывает развитие общих режимов регулирования ИИ, данных, ЦОД и цифровых платформ и расширение полномочий Роскомнадзора по контролю телеком-инфраструктуры и интернет-трафика. Для операторов КИИ и крупных ИТ-компаний это означает необходимость адаптации архитектуры и процессов к ужесточающимся требованиям по

мониторингу трафика, обмену информацией об угрозах и противодействию кибермошенничеству.

Наверх

При подготовке материала использовались следующие информационные ресурсы:

digital.gov.ru | www.garant.ru | www.rbc.ru | www.securitylab.ru | www.anti-malware.ru | www.rb.ru | www.gazeta.ru | www.itsec.ru | www.vedomosti.ru | www.comnews.ru | www.xakep.ru | www.forbes.ru | www.ria.ru

Присылайте ваши мысли и предложения.

Благодарим всех тех, кто рекомендовал статьи для этого выпуска.

ДРТ
ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ
BUSINESS SOLUTIONS AND TECHNOLOGIES

delret.ru