ДРТ
ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ
BUSINESS SOLUTIONS AND TECHNOLOGIES

35 ЛЕТ В РОССИИ

Ежемесячная подборка новостей

Июнь 2026 года, выпуск 6

Законодательство и рекомендации регуляторов

05 июня

ФСТЭК обновила методику поиска уязвимостей и недекларированных возможностей в ПО

Федеральная служба по техническому и экспортному контролю (ФСТЭК) утвердила новую методику выявления уязвимостей и недекларированных возможностей в программном

обеспечении. Для сферы управления киберрисками это важное изменение: акцент смещается в сторону более системного анализа защищенности ПО на протяжении жизненного цикла, а не только финальной сертификационной проверке. Методика выявления уязвимостей и недекларированных возможностей от 25 декабря 2020 года больше не применяется.

16 июня

Банк России выпустил рекомендации по ИБ при разработке и применении ИИ на финансовом рынке

Банк России утвердил методические рекомендации № 3-МР по обеспечению информационной безопасности (ИБ) при разработке и применении искусственного интеллекта (ИИ) в финансовом секторе. Документ описывает риски ИИ, связанные с ИБ и операционной надежностью, а также рекомендует подходы к модели угроз, мерам защиты, политике ИБ и использованию сторонних ИИ-сервисов или open-source-компонентов. Для банков и финтеха это фактически руководство по встраиванию управления рисками ИИ в действующую систему киберрисков.

26 июня

Приняты законодательные изменения для противодействия преступлениям с использованием ИКТ

В конце июня опубликован Федеральный закон № 210-ФЗ, направленный на совершенствование мер противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий. Изменения затрагивают закон «О связи» и другие акты, а следовательно, имеют важное значение для операторов связи, цифровых сервисов и компаний, выстраивающих процессы по противодействию мошенничеству (антифрод-процессы).

30 июня

Обсуждается единая база IMEI

В конце июня профильные СМИ сообщили о планах передавать данные о смартфонах в единую базу IMEI (International Mobile Equipment Identity), чтобы иметь возможность блокировать украденные и потерянные устройства, а также снизить риски использования незарегистрированных устройств. Инициатива напрямую связана с защитой от мошенничества, мобильной идентификацией и управлением рисками в телеком-инфраструктуре.

Наверх

Информационные статьи

03 июня

ИИ в 2026 году: угроза снаружи и внутри

Компания Positive Technologies выпустила исследование, посвященное развитию угроз, связанных с использованием искусственного интеллекта при кибератаках. Материал важен для управления рисками, поскольку рассматривает ИИ не только как инструмент защиты, но и как фактор усиления атакующих: автоматизация разведки, генерация фишинга, ускорение эксплуатации и новые риски для внутренних процессов.

24 июня

Как выбрать решение для защиты конечных точек

«Лаборатория Касперского» опубликовала чек-лист для выбора современного EPP-решения. В материале выделены базовые технологии защиты конечных точек: файловый, веб- и почтовый антивирус, IDS, поведенческий анализ, защита от эксплойтов и шифровальщиков, HIPS, машинное обучение и песочница (sandbox).

Наверх

Атаки, инциденты, уязвимости

15 июня

«Астрал» подтвердил целевую кибератаку после недельного сбоя сервисов

ГК «Астрал», российский ИТ-разработчик сервисов для бизнеса, сообщила, что 9 июня подверглась серии целенаправленных хакерских атак, что послужило причиной остановки ряда сервисов. Компания заявила о круглосуточном восстановлении инфраструктуры и планах завершить все работы 16 июня. В результате проверки признаков утечки или компрометации данных не обнаружено. После инцидента защитные механизмы компании были дополнительно усилены.

26 июня

Обнаружено более 250 тысяч потенциальных проблем безопасности в рабочих процессах GitHub Actions

«Лаборатория Касперского» проанализировала рабочие процессы GitHub Actions в популярных репозиториях и обнаружила более 250 тыс. потенциальных проблем безопасности в процессах CI/CD. В восьми репозиториях присутствовали критические ошибки конфигурации, способные привести к компрометации цепочки поставок. Этот анализ демонстрирует необходимость соблюдения рекомендаций по безопасной настройке CI/CD и проверки конфигураций на ИБ-риски.

29 июня

76% кибератак направлены на шифрование или разрушение инфраструктуры

По данным, опубликованным информационно-аналитическим центром по информационной безопасности Anti-Malware со ссылкой на компанию «Инфосистемы Джет», 44% атак приходятся на шифрование инфраструктуры, а 32% — на ее разрушение. Исследование показывает, что злоумышленники все чаще используют штатные инструменты администрирования, такие как PowerShell, CMD и средства удаленного управления, что позволяет маскировать вредоносную активность под обычную работу системных администраторов.

30 июня

Активная эксплуатация CVE-2026-46817 в Oracle E-Business Suite Payments

Компания Help Net Security сообщила об активной эксплуатации критической уязвимости CVE-2026-46817 в Oracle Payments, компоненте Oracle E-Business Suite. Уязвимость связана с передачей файлов и проблемами управления привилегиями/аутентификацией. Национальная база данных уязвимостей США NVD указывает CVSS 9.8 и возможность удаленной компрометации Oracle Payments через HTTP без аутентификации. Для компаний, использующих Oracle EBS, это критичный риск финансовых процессов — требуется срочная проверка экспозиции, установка обновлений и контроль признаков компрометации.

Наверх

Ключевые тренды

17 июня

Киберугрозы для веб-приложений и инфраструктуры разработки: тренды и прогнозы на 2026–2027 годы

Компания Positive Technologies выпустила отчет о киберугрозах для веб-приложений и инфраструктуры разработки с прогнозами на 2026–2027 годы. Особое внимание в исследовании уделяется программным интерфейсам взаимодействия (API), средам контейнеризации (Docker, Kubernetes), корпоративной инфраструктуре разработки и развертыванию программных продуктов (Development, CI/CD), открытому программному обеспечению, а также приложениям с большими языковыми моделями (LLM) и ИИ-агентами. В контексте управления киберрисками это означает, что периметр безопасности окончательно сместился в сторону разработки, DevSecOps, контроля зависимостей и защиты пайплайна.

26 июня

Каждая третья кибератака в мире — на Россию: «Лаборатория Касперского» назвала страну главной мишенью хакеров

Информационный портал SecurityLab со ссылкой на данные «Лаборатории Касперского» сообщил, что на Россию с начала 2026 года пришлось около 28% обнаруженных сетевых кибератак, совершенных на организации по всему миру. Отмечается, что рост рисков связан с усложнением атак и развитием искусственного интеллекта. Промежуток между раскрытием уязвимости и первыми попытками ее эксплуатации сокращается с нескольких дней до нескольких часов, что существенно повышает необходимость быстрой реакции на атаки.

30 июня

57% компаний не знают свою инфраструктуру, поэтому дольше расследуют атаки

Информационно-аналитический центр Anti-Malware опубликовал данные ГК «Гарда»: 57% компаний недостаточно хорошо знают свою инфраструктуру, в результате чего дольше расследуют атаки. Это один из ключевых управленческих рисков: без инвентаризации активов, связей, владельцев систем и критичности сервисов сложно оценивать ущерб и быстро локализовать инцидент. Практический вывод: база данных управления конфигурацией (CMDB), управление активами и регулярная проверка фактической инфраструктуры становятся базой для центров мониторинга информационной безопасности (SOC), реагирования и обеспечения соответствия требованиям регуляторов.

Наверх

При подготовке материала использовались следующие информационные ресурсы:

www.consultant.ru | www.securitylab.ru | www.kaspersky.ru | www.helpnetsecurity.com | ptsecurity.com | www.anti-malware.ru

Присылайте ваши мысли и предложения.

Благодарим всех, кто рекомендовал статьи для этого выпуска.

ДРТ
ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ
BUSINESS SOLUTIONS AND TECHNOLOGIES

delret.ru