ДРТ
ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ
BUSINESS SOLUTIONS AND TECHNOLOGIES

35 ЛЕТ В РОССИИ

Ежемесячная подборка новостей

Май 2026 года, выпуск 5

Законодательство и рекомендации регуляторов

18 мая

Минцифры России утвердило требования к информационной безопасности для государственной единой облачной платформы

Приказ Минцифры России закрепляет требования к обеспечению информационной безопасности при предоставлении облачных услуг через государственную единую облачную

платформу. Это имеет большое значение для государственных органов и организаций, которые используют или планируют использовать государственную облачную инфраструктуру. Документ усиливает акцент на защите облачных сервисов, управлении доступом и надежности инфраструктуры. Для заказчиков облачных услуг это повод уточнить, как требования будут отражаться в договорах, SLA и внутренних регламентах по информационной безопасности.

21 мая

ФСБ России утвердила порядок аккредитации центров ГосСОПКА

Документ устанавливает процедуру аккредитации центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак. Это важно для организаций, которые взаимодействуют с государственным контуром реагирования на компьютерные инциденты. На практике документ влияет на требования к центрам, их функциям, процедурам и подтверждению соответствия. Для ИБ-служб это повод проверить, как выстроены каналы взаимодействия с НКЦКИ/ГосСОПКА и какие обязанности могут возникать у подрядчиков.

22 мая

ФСТЭК разработала проект методики оценки зрелости защиты информации в ИС и на значимых объектах КИИ

ФСТЭК сообщила о разработке методического документа «Методика оценки уровня зрелости деятельности в области технической защиты информации в информационных системах и обеспечения безопасности значимых объектов КИИ РФ». Регулятор предложил профильным специалистам принять участие в рассмотрении проекта; замечания и предложения принимаются до 8 июня 2026 года. Документ важен тем, что смещает акцент от формального наличия мер защиты к оценке зрелости процессов ТЗИ и безопасности КИИ.

Наверх

Информационные статьи

7 мая

Минута — и почти каждый второй пароль взломан

«Лаборатория Касперского» повторно провела исследование стойкости реальных паролей, собранных из утечек в даркнете. Компания изучила 231 млн уникальных паролей из утечек 2023–2026 годов и пришла к выводу, что 48% паролей взламываются менее чем за минуту, а

60% — менее чем за час. В статье отдельно отмечается, что взлом можно осуществить теперь быстрее из-за роста производительности GPU: RTX 5090 перебирает MD5-хеши быстрее, чем RTX 4090.

8 мая

LLMjacking: атаки на локальные ИИ-серверы

«Лаборатория Касперского» разобрала атаки на ИИ-инфраструктуру, включая попытки кражи вычислительных ресурсов и несанкционированного доступа к LLM-серверам. Тема важна для компаний, которые разворачивают локальные модели или используют GPU-инфраструктуру для внутренних задач. В отличие от классических атак на данные, здесь целью может быть дорогостоящий вычислительный ресурс, модель или API-доступ. Для защиты необходимы инвентаризация ИИ-сервисов, контроль доступа, лимиты, мониторинг аномального потребления и изоляция окружений.

27 мая

ИИ ловит ИИ: как российские компании следят за попаданием данных в нейросети

Российские компании активнее применяют ИИ для выявления внутренних угроз и расследования инцидентов. Одновременно растет риск неконтролируемого использования сотрудниками внешних ИИ-сервисов, куда могут попадать фрагменты кода, документы и коммерческая информация. Как говорят эксперты, организациям необходимо не только запрещать, но и управлять использованием ИИ: через политики, разрешенные сервисы, журналирование и обучение сотрудников.

Наверх

Атаки, инциденты, уязвимости

7–12 мая

Взлом Canvas и переговоры Instructure с ShinyHunters

KrebsOnSecurity сообщил о вымогательской атаке на образовательную платформу Canvas, которая нарушила работу школ и университетов в США. Группа ShinyHunters заявляла об угрозе публикации данных миллионов пользователей, а Instructure временно отключала платформу. Позже Reuters сообщил, что Instructure достигла соглашения с группой, включая возврат и уничтожение украденных данных.

12 мая

Microsoft May Patch Tuesday: 118 уязвимостей, включая критичные RCE

В майском Patch Tuesday Microsoft закрыла не менее 118 уязвимостей. Среди наиболее заметных — CVE-2026-41089 в Windows Netlogon, которая дает атакующему SYSTEM-привилегии на контроллере домена без участия пользователя. Также отмечены критичные проблемы в Windows DNS Client и Entra ID. Для ИБ-команд это пакет обновлений с высоким приоритетом, особенно для доменных контроллеров и серверной инфраструктуры.

18 мая

Positive Technologies: 83% атак на российскую промышленность совершены с использованием ВПО

Positive Technologies сообщила, что вредоносное ПО остается ключевым инструментом атак на российскую промышленность. Это подчеркивает значимость защиты АСУ ТП, сегментации, мониторинга технологических сетей и контроля съемных носителей. Для промышленных предприятий риск особенно высок из-за длительного жизненного цикла оборудования и ограничений на обновления. Заключение экспертов — необходимо использовать классическую защиту конечных точек с сетевым мониторингом и планами реагирования на инциденты в OT-среде.

21 мая

Microsoft выпустила исправления для двух 0-day в Defender

Microsoft начала распространять обновления для двух уязвимостей Microsoft Defender, которые уже использовались в атаках. Первая, CVE-2026-41091, позволяет повысить привилегии до SYSTEM, а вторая, CVE-2026-45498, может приводить к отказу в обслуживании на незащищенных устройствах. Проблема имеет особое значение, потому что Defender часто является базовым защитным компонентом Windows-инфраструктуры. В приоритете — проверка версии движка и платформы Defender и уверенность в том, что автоматические обновления не отключены.

26 мая

Активно эксплуатируемая уязвимость Trend Micro Apex One попала в поле зрения CISA

Help Net Security сообщил об эксплуатации CVE-2026-34926 в Trend Micro Apex One. Уязвимость связана с path traversal и может позволить внедрить вредоносный код через доверенный канал распространения агентов. Trend Micro призвала обновить on-premise-развертывания Apex One и проверить доступ к административной консоли. Для организаций это особенно критично, потому что компрометация защитной платформы может превратить ее в механизм доставки вредоносного ПО.

Наверх

Ключевые тренды

18 мая

ИИ сокращает окно эксплуатации уязвимостей до часов

Help Net Security со ссылкой на отчет Synack сообщает, что разрыв между обнаружением уязвимости и ее эксплуатацией сокращается до часов. В 2025 году среднее время устранения уязвимостей снизилось с 63 до 38 дней, но атакующие также ускорились. Особенно растет значение непрерывной проверки безопасности (continuous security validation), потому что периодические проверки уже не всегда успевают за темпом атак. Для ИБ-процессов это означает необходимость быстрее приоритизировать CVE по реальной экспозиции и критичности активов.

22 мая

Майский дайджест трендовых уязвимостей

Positive Technologies опубликовала майский обзор уязвимостей, которые эксперты отнесли к трендовым: это недостатки безопасности, которые уже активно эксплуатируются злоумышленниками или могут быть использованы в ближайшее время. В дайджест вошли уязвимости в Microsoft SharePoint Server, Adobe Acrobat Reader и Apache ActiveMQ Classic. Для части уязвимостей указаны признаки эксплуатации в реальных атаках: например, Microsoft предупреждала об эксплуатации CVE-2026-32201 в SharePoint, Adobe подтвердила использование CVE-2026-34621 в реальных атаках, а Fortinet фиксировала эксплуатацию CVE-2026-34197 в Apache ActiveMQ.

29 мая

Паттерны современных вредоносных кампаний

«Лаборатория Касперского» опубликовала обзор изменений в паттернах вредоносной активности, которые помогают атрибутировать ВПО, своевременно обнаруживать атаки и снижать последствия инцидентов. Ландшафт угроз за последнее время заметно изменился: злоумышленники меняют инфраструктуру, инструменты и методы доставки вредоносного ПО.

Наверх

При подготовке материала использовались следующие информационные ресурсы:

www.consultant.ru | www.securitylab.ru | www.kaspersky.ru | www.helpnetsecurity.com | www.bleepingcomputer.com | krebsonsecurity.com | ptsecurity.com | www.reuters.com

Присылайте ваши комментарии и предложения.

Благодарим всех тех, кто рекомендовал статьи для этого выпуска.

ДРТ
ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ
BUSINESS SOLUTIONS AND TECHNOLOGIES

delret.ru