ДРТ
ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ
BUSINESS SOLUTIONS AND TECHNOLOGIES

35 ЛЕТ В РОССИИ

Ежемесячная подборка новостей

Июль 2026 года, выпуск 7

Законодательство и рекомендации регуляторов

1 июля

С 1 июля банки получили новые возможности для противодействия мошенничеству при выдаче займов

С 1 июля банки и микрофинансовые организации могут оперативно получать сведения из всех квалифицированных бюро кредитных историй для выявления попыток оформления займов без добровольного согласия клиента. Механизм направлен на противодействие операциям с использованием украденных персональных данных, поддельных документов и социальной инженерии.

Для финансовых организаций это означает необходимость актуализации антифрод-моделей, процедур проверки согласия клиента и взаимодействия с бюро кредитных историй. Новые возможности также повышают требования к контролю доступа к финансовой и персональной информации.

7 июля

Владельцев сайтов начали штрафовать за использование иностранных сервисов при авторизации пользователей

С 7 июля за отсутствие на сайте российских способов идентификации либо за предоставление пользователям возможности входа через отдельные иностранные сервисы предусмотрена административная ответственность. В качестве допустимых вариантов рассматриваются российский номер телефона, «Госуслуги», Единая система идентификации и аутентификации и Единая биометрическая система.

Изменения важны для владельцев интернет-сервисов, операторов информационных систем и компаний, предоставляющих цифровые платформы. Организациям потребуется проверить сценарии регистрации и входа, тексты пользовательских уведомлений, интеграции с внешними поставщиками идентификации и настройки журналирования событий.

24 июля

Размещен проект нового приказа ФСТЭК России о мерах защиты персональных данных

24 июля 2026 года ФСТЭК России разместила на федеральном портале проектов нормативных правовых актов проект приказа, который должен заменить Приказ ФСТЭК России от 18 февраля 2013 года № 21. Проект приказа ID 01/02/07-26/00169583 предусматривает новый состав организационных и технических мер защиты персональных данных, а также оценку уровня зрелости реализованных мер.

Согласно проекту оценку предполагается проводить до начала обработки персональных данных, далее не реже одного раза в три года и после каждого компьютерного инцидента. Документ является проектом и не устанавливает действующие обязательные требования. Организациям, обрабатывающим персональные данные, рекомендуется отслеживать прохождение проекта и заранее оценить возможное влияние изменений.

26 июля

Подписан закон о поддержке развития технологий искусственного интеллекта

26 июля 2026 года подписан Федеральный закон № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации». Документ закрепляет

правовые основы развития искусственного интеллекта, включая понятия национальных и суверенных больших фундаментальных моделей искусственного интеллекта.

Основные положения закона вступают в силу 1 сентября 2026 года. Для организаций, использующих генеративный искусственный интеллект и ИИ-агентов, это означает необходимость заранее оценить применяемые модели, порядок работы с данными, риски передачи информации во внешние сервисы и процедуры контроля результатов, созданных искусственным интеллектом.

Наверх

Информационные статьи

3 июля

Приложение-приманку под видом психологического теста использовали для совершения атак на государственный сектор и энергетику

3 июля 2026 года «Лаборатория Касперского» сообщила о вредоносной кампании, в которой приложение-приманка распространялось под видом психологического теста. Атаки были выявлены в том числе в России и затрагивали государственный сектор и энергетические организации.

Сценарий показывает, что злоумышленники используют популярные и внешне безобидные форматы для доставки вредоносного программного обеспечения. Для снижения риска необходимо контролировать установку приложений, ограничивать использование непроверенных источников и анализировать аномальную активность браузеров и учетных записей.

13 июля

Июльский дайджест трендовых уязвимостей

13 июля 2026 года Positive Technologies опубликовала июльский дайджест трендовых уязвимостей. В выпуске выделена уязвимость PT-2026-40978, также обозначенная как CVE-2026-42897, в Outlook Web Access.

Для компаний, использующих Microsoft Exchange и веб-доступ к корпоративной почте, необходимо проверить наличие обновлений, ограничить внешнюю доступность административных интерфейсов и проанализировать журналы аутентификации и почтового доступа.

15 июля

Microsoft выпустила обновления для более 570 уязвимостей в июльском выпуске

15 июля 2026 года Microsoft выпустила масштабный пакет обновлений, включивший исправления более чем для 570 уязвимостей. В числе исправленных проблем были две уязвимости, которые уже эксплуатировались злоумышленниками: CVE-2026-56155 и CVE-2026-56164.

Организациям рекомендуется в приоритетном порядке проверить обновление серверов Microsoft, SharePoint, систем удаленного доступа и рабочих станций пользователей с повышенными правами.

Наверх

Атаки, инциденты, уязвимости

7 июля

Кибератаки на российскую промышленность выросли почти вдвое

7 июля 2026 года Anti-Malware.ru опубликовал данные Kaspersky ICS CERT о росте атак на российские промышленные организации. По сравнению с аналогичным периодом прошлого года доля компьютеров, столкнувшихся с вредоносным программным обеспечением, выросла на 97%.

Для промышленных компаний это повышает значение сегментации ИТ- и ОТ-контуров, контроля удаленного доступа, управления уязвимостями и мониторинга съемных носителей.

15 июля

Доля атак на российские медицинские организации выросла до 15%

15 июля 2026 года Anti-Malware.ru сообщил о росте доли атак на российские медицинские организации с 6% до 15%. В рамках одной из кампаний злоумышленники использовали уязвимости в TrueConf Server для компрометации серверов видео-конференц-связи и установки бэкдоров.

Организациям здравоохранения рекомендуется проверить версии TrueConf Server, закрыть административные интерфейсы от внешнего доступа и проанализировать серверы на наличие признаков компрометации.

24 июля

Группа Laundry Bear эксплуатировала уязвимость в Zimbra Collaboration Suite

24 июля 2026 года Help Net Security сообщил, что группа Laundry Bear использовала уязвимость CVE-2025-66376 в Zimbra Collaboration Suite для совершения атак на государственные и критически значимые организации.

Организациям, использующим Zimbra Collaboration Suite, необходимо установить актуальные обновления, проверить журналы входа в почтовые ящики, проанализировать подозрительные правила пересылки и отозвать несанкционированные пароли приложений.

29 июля

Российские ИТ-компании атакуют с помощью писем с «поврежденными» документами

29 июля 2026 года «Лаборатория Касперского» сообщила о фишинговой кампании группы GOFFEE, направленной преимущественно на российский технологический сектор. В электронных письмах использовались документы, имитирующие поврежденные файлы, чтобы заставить пользователя открыть вложение или выполнить дополнительные действия.

Для защиты необходимо блокировать опасные типы вложений, ограничивать запуск макросов и скриптов и обучать сотрудников распознавать электронные письма, в которых проблема с документом используется как предлог для совершения действия.

30 июля

Злоумышленники эксплуатируют уязвимость Cisco Secure Firewall Management Center

30 июля 2026 года Help Net Security сообщил об эксплуатации уязвимости CVE-2026-20316 в Cisco Secure Firewall Management Center (FMC). Проблема связана со статическими учетными данными.

Поскольку FMC используется для централизованного управления межсетевыми экранами, компрометация системы может повлиять на конфигурацию средств защиты всей сети. Необходимо установить обновления, проверить учетные данные и проанализировать журналы действий администраторов.

Наверх

Ключевые тренды

6 июля

ИИ-агент впервые мог самостоятельно провести атаку с шифровальщиком

6 июля 2026 года в публикациях по безопасности обсуждался сценарий, в котором автономный ИИ-агент выполнял значительную часть цепочки атаки, включая поиск уязвимости, получение доступа и подготовку действий с данными. Отдельно Help Net Security сообщал об эксплуатации уязвимости CVE-2026-55255 в Langflow.helpnetsecurity.

Тренд показывает, что ИИ-агенты становятся самостоятельным элементом модели угроз. Организациям необходимо ограничивать права таких систем, изолировать среды их выполнения и предусматривать обязательное подтверждение человеком для выполнения критически важных действий.

13 июля

Атаки на уязвимые маршрутизаторы используются для проникновения в критически значимую инфраструктуру

13 июля 2026 года BleepingComputer сообщил о предупреждении США и союзников об атаках на уязвимые и неправильно настроенные маршрутизаторы. Такие устройства могут использоваться как первоначальная точка проникновения в сети организаций критически важной инфраструктуры.

Практический вывод для компаний — регулярно проверять интернет-доступные устройства, отключать ненужные сервисы, своевременно устанавливать обновления и защищать административный доступ многофакторной аутентификацией.

15 июля

Автоматизация поиска уязвимостей с помощью искусственного интеллекта влияет на скорость выпуска исправлений

15 июля 2026 года Help Net Security связал масштаб июльского Microsoft Patch Tuesday с ростом возможностей автоматизированного поиска уязвимостей. Чем быстрее выявляются ошибки и создаются инструменты их эксплуатации, тем меньше становится период между публикацией информации об уязвимости и атакой.

Для управления киберрисками это означает необходимость автоматизировать инвентаризацию активов, приоритизацию уязвимостей и контроль установки обновлений.

Наверх

При подготовке материала использовались следующие информационные ресурсы:

www.consultant.ru | www.kaspersky.ru | www.helpnetsecurity.com | ptsecurity.com | www.anti-malware.ru | www.mk.ru | www.buh.ru | www.regulation.gov.ru | www.bleepingcomputer.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