ДРТ
ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ
BUSINESS SOLUTIONS AND TECHNOLOGIES

35 ЛЕТ В РОССИИ

# Ежемесячная подборка новостей

Март 2026 года, выпуск 4



## Законодательство и рекомендации регуляторов

1 марта

Приказ ФСТЭК № 117 вступил в силу: новая эра регулирования ИБ для государственных систем

С 1 марта 2026 года вступил в силу приказ ФСТЭК России № 117, который заменил действовавший более 10 лет приказ № 17. Новый документ меняет саму модель регулирования: вместо разового проекта защиты вводится режим постоянного мониторинга, управления рисками и регулярной отчетности. Требования распространяются на государственные информационные системы, а через механизмы контрактования — на всех подрядчиков и интеграторов.

10 марта

### В России вынесены первые судебные решения о штрафах за крупные утечки персональных данных

Арбитражные суды Москвы и Санкт-Петербурга рассмотрели первые административные дела в отношении компаний, допустивших утечки персональных данных после вступления в силу новых частей статьи 13.11 КоАП РФ (с 30 мая 2025 года). Вынесенные решения оказались относительно мягкими: суды назначили сравнительно небольшие штрафы или ограничились предупреждениями. Эксперты полагают, что в дальнейшем практика будет ужесточаться — механизм оборотных штрафов за масштабные утечки в законодательстве уже закреплен.

Наверх

## Информационные статьи

23 марта

### Реестр российского ПО: как зарегистрировать продукт и не получить отказ

В условиях цифрового суверенитета наличие корректных документов на программное обеспечение становится едва ли не важнее самого кода. Для ИТ-компании попадание в заветный список Минцифры России — это пропуск в мир крупных государственных контрактов и налоговых льгот. Однако процедура включения в него обросла мифами о бюрократии и сложности.

24 марта

### FIRST: в 2026 году число публично раскрытых уязвимостей может превысить 50 тыс. и приблизиться к 59 тыс.

По прогнозу международной организации Forum of Incident Response and Security Teams (FIRST), в 2026 году число публично раскрытых уязвимостей может превысить 50 тыс. и в медианном сценарии приблизиться к 59 тыс. В более жестких, но реалистичных вариантах оценка поднимается почти до 118 тыс., тогда как за 2025 год было зарегистрировано около

48 тыс. уязвимостей. Эксперты предупреждают: ни одна организация не способна самостоятельно справиться с таким объемом уязвимостей. Именно поэтому в первую очередь важно сосредоточиться на тех, которые реально могут быть использованы злоумышленниками.

30 марта

### Как новые требования мотивируют бизнес повышать защиту от киберугроз

Меняется характер и количество кибератак, новые требования законодательства призваны минимизировать утечку данных в России. Бизнес адаптируется к оборотным штрафам и вкладывается в киберустойчивость, отмечают эксперты.

19 марта

### Отчет об утечках информации в мире за три года

Экспертно-аналитический центр InfoWatch выпустил отчет об утечках информации ограниченного доступа. В его основу легло исследование об утечках информации в мире за три года. Отчет содержит ряд характеристик мировых утечек данных, а также сравнение отдельных показателей в России с общемировыми.

25 марта

### Flashpoint Global Threat Intelligence Report 2026: деньги — главный мотив, вымогательство лидирует с долей 43%

Компания Flashpoint опубликовала ежегодный отчет Global Threat Intelligence Report 2026, адресованный командам киберразведки, управления уязвимостями и руководству служб информационной безопасности. По данным отчета, деньги остаются главным мотивом атак: в 71% случаев злоумышленники были нацелены на финансовую выгоду. Вымогательство с шифрованием данных лидирует с долей 43% инцидентов, следом идет BEC-мошенничество (29%). Авторы выделяют три системные причины, снова и снова открывающих дорогу атакам: слабая аутентификация, несвоевременное исправление уязвимостей и избыточные привилегии учетных записей.

27 марта

### NIST впервые с 2013 года обновил руководство по защите DNS

Национальный институт стандартов и технологий США (NIST) выпустил обновленное руководство по защите DNS — первое за 13 лет. Новый документ учитывает современный ландшафт угроз и предлагает рассматривать DNS не только как инфраструктурный сервис, но и как полноценный инструмент безопасности. Обновленные рекомендации актуальны для любых организаций, эксплуатирующих публичную или внутреннюю DNS-инфраструктуру.

Наверх

## Атаки, инциденты, уязвимости

### 3 марта

#### APT-группировка Mythic Likho возобновила целевые атаки на объекты КИИ России

Специалисты PT ESC TI опубликовали комплексное исследование активности APT-группировки Mythic Likho, целенаправленно атакующей субъекты критической информационной инфраструктуры (КИИ) России. Прежде всего это предприятия машиностроения, добывающей и обрабатывающей промышленности. Злоумышленники разрабатывают уникальный фишинговый сценарий для каждой жертвы на основе детального изучения ее деятельности, контрагентов и сотрудников. Эксперты прогнозируют сохранение угрозы со стороны Mythic Likho в 2026 году.

### 4 марта

#### Европол ликвидировал крупнейшую PhaaS-платформу Tycoon2FA: изъято 330 доменов

Благодаря международной операции, координируемой Европолом, остановлена работа Tycoon2FA — крупнейшей фишинговой платформы, которая функционирует по модели «фишинг как услуга» (PhaaS). В ходе операции изъято 330 доменов, включая панели управления и фишинговые страницы. Платформа работала с 2023 года, генерировала более 30 млн фишинговых писем в месяц и атаковала более 500 тыс. организаций. Tycoon2FA обходила МФА через механизм «противник посередине» (AitM).

### 5 марта

#### Wikipedia атакована самораспространяющимся JavaScript-червем: затронуты почти 4 000 страниц

5 марта 2026 года Wikimedia Foundation зафиксировала ИБ-инцидент: проекты поразил самораспространяющийся JavaScript-червь, который модифицировал пользовательские скрипты и портил страницы Meta-Wiki. Вредоносный код был активен 23 минуты, после чего инженеры временно перевели все проекты в режим «только для чтения». Червь успел затронуть порядка 3 996 страниц и заменить common.js-файлы примерно у 85 пользователей.

### 10 марта

#### Мартовский Patch Tuesday Microsoft: 79 уязвимостей, два нулевых дня и критические баги в Office и Excel

10 марта 2026 года компания Microsoft выпустила плановый пакет обновлений безопасности, закрыв 79 уязвимостей, в том числе три критические. Два публично

раскрытых нулевых дня: CVE-2026-21262 в SQL Server (повышение привилегий до уровня SQLAdmin, CVSS 8,8) и CVE-2026-26127 в .NET (отказ в обслуживании). Особого внимания заслуживают критические уязвимости удаленного выполнения кода в Microsoft Office (CVE-2026-26110, CVE-2026-26113), срабатывающие через панель предварительного просмотра, а также CVE-2026-26144 в Excel, позволяющая Copilot Agent несанкционированно передавать данные вовне.

### 13 марта

#### Google экстренно закрыл два нулевых дня в Chrome, уже используемых в реальных атаках

13 марта 2026 года компания выпустила внеплановое обновление Chrome, закрыв сразу две опасные уязвимости — обе активно эксплуатировались в реальных атаках. CVE-2026-3909 — ошибка записи за пределами границ в графическом движке Skia, CVE-2026-3910 — уязвимость в движке V8, обрабатывающем JavaScript. Обе проблемы выявлены 10 марта 2026 года.

### 18 марта

#### Ботнет Kimwolf атаковал российские компании: волна DDoS-атак с участием более 4 млн IP-адресов

В начале марта 2026 года российские компании подверглись массированной серии DDoS-атак с использованием ботнета Kimwolf. Атаки охватили десятки целей и задействовали более 4 млн уникальных IP-адресов. Пик пришелся на 4 марта: мощность атак достигала 700 тыс. запросов в секунду. По оценке StormWall, речь идет об организованной заказной кампании: на это указывают масштаб ботнета, стоимость его аренды и высокий уровень координации.

### 19 марта

#### InfoWatch: за три года в России утекло 4,5 млрд записей персональных данных

Экспертно-аналитический центр группы компаний InfoWatch опубликовал исследование «Утечки информации ограниченного доступа. Мир, 2023–2025 годы». За три года в России произошла утечка 4,5 млрд записей персональных данных из общемирового объема в 100 млрд записей. Существенно выросла доля утечек коммерческой тайны, составив более трети инцидентов. Средний объем одной утечки в России в 2025 году составил 3,27 млн записей — на 25,8% больше, чем годом ранее.

### 20 марта

#### «Лаборатория Касперского»: мошенники используют сервисы Яндекса для криптовалютных скам-рассылок

«Лаборатория Касперского» зафиксировала всплеск мошеннических рассылок, в которых злоумышленники маскируют ссылки на вредоносные ресурсы с помощью легитимного сервиса «Яндекс Взгляд». Главная хитрость схемы — ссылка на авторитетный сервис — снижает настороженность получателей, а форма опроса используется лишь как промежуточное звено для перенаправления на мошеннические страницы.

30 марта

### Группировка Interlock использовала критическую уязвимость в Cisco Secure Firewall Management Center

Уязвимость CVE-2026-20131 получила максимальную оценку по шкале CVSS — 10,0. Она находится в веб-интерфейсе FMC (Firewall Management Center — центр управления межсетевыми экранами) и связана с небезопасным методом преобразования (десериализации) данных, передаваемых через Java-поток.

Наверх

## Ключевые тренды

3 марта

### Positive Technologies: CODE RED 2026 — актуальные киберугрозы для российских организаций

Компания Positive Technologies представила масштабный аналитический отчет CODE RED 2026. Ключевые выводы: доля атак, завершившихся утечкой данных, выросла с 44% до 56%; доля инцидентов с нарушением деятельности организаций — с 37% до 40%.

12 марта

### Утечки информации в России: новый отчет

За прошедший год возникло нескольких новых тенденций в отношении утечек информации в России. С одной стороны, отмечено падение количества утечек данных как в нашей стране, так и в мире в целом. С другой — доля России в общем количестве утечек в мире увеличилась.

17 марта

### Positive Technologies: тренды кибербезопасности финансовой отрасли России в 2026 году

Аналитики компании Positive Technologies выпустили исследование, посвященное киберустойчивости российского финансового сектора. Ключевой тезис: даже организации с высоким уровнем зрелости ИБ уязвимы перед многошаговыми атаками с применением ИИ и компрометацией цепочек поставок.

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