

Октябрь — месяц осведомлённости о кибербезопасности: полный гид по событиям и трендам 2026 года

Весь октябрь по всему миру будет проходить Cybersecurity Awareness Month — глобальная инициатива, которая в 2026 году отмечает 23-й год. Кампания стартовала в 2004 году как совместный проект Министерства внутренней безопасности США и Национального альянса кибербезопасности, а сегодня охватывает десятки стран, включая Канаду, страны Евросоюза и Россию.

Сразу несколько организаций задали свои лозунги — но все сводятся к одному: базовые привычки по-прежнему решают больше, чем сложные технологии.

CISA (США) — «Securing the Next 250», с акцентом на защиту критической инфраструктуры.

National Cybersecurity Alliance — «Don't Make It Easy for Them» — «Не облегчай им задачу». NCA прямо говорит: «Это про выработку привычек и их повторение каждый день в мелочах».

Канада (Get Cyber Safe) — «Your best defence is you» — «Твоя лучшая защита — это ты».

Главная особенность 2026 года — искусственный интеллект радикально изменил ландшафт угроз. Простого «осведомления» больше недостаточно: задачей становится устойчивость (resilience) — способность не только предотвратить атаку, но и быстро восстановиться после неё.

По данным Yandex Cloud, в первом полугодии 2026 года число отражённых кибератак в облачных средах выросло на 60% по сравнению с тем же периодом 2025 года. Количество DDoS-атак на веб-приложения (L7) за неполный 2026 год уже превысило показатели всего 2025 года более чем в два раза: 15 140 против 6 348.

Google Threat Intelligence Group обнаружила: половина уязвимостей, выявленных при помощи ИИ, позволяет добиться удалённого выполнения кода (RCE), тогда как среди остальных раскрытых ошибок доля таких — только 26%. Среднее количество эксплуатируемых уязвимостей выросло с 10,5 до 18 в месяц. ИИ ускоряет не только поиск, но и превращение известных патчей в рабочие эксплойты.

Отчёт Thales (Data Threat Report 2026) называет ИИ новой главной киберугрозой из-за массового внедрения ИИ-агентов. 61% организаций сообщают об атаках на ИИ-приложения. Ключевые риски: изменение экосистемы (70%), доверие (58%), конфиденциальность (46%). Самые уязвимые цели — облачные хранилища (35%), SaaS-приложения (34%), облачная инфраструктура управления (32%).

Positive Technologies прогнозирует: Shadow AI (теневой ИИ — использование сотрудниками несанкционированных ИИ-сервисов) станет одним из ключевых источников корпоративных угроз. Границы между массовыми и целевыми атаками стираются. Развивается модель AIaaS (AI scam as a service).

По данным Anthropic, 832 заблокированных аккаунта злоумышленников использовали Claude, 80% — именно агентный интерфейс Claude Code. Доля злоумышленников среднего и высокого риска выросла с 33,5 до 56,1% — без роста квалификации самих атакующих.

В сентябре Gambit Security связала серию инцидентов с хакером, который с 10 по 15 сентября атаковал до 100 организаций с помощью ИИ-агентов на базе Claude, DeepSeek и Kimi. Операция обошлась примерно в \$8 тыс., атака на отдельную организацию — несколько долларов.

29 сентября, накануне Месяца кибербезопасности, в Москве состоялся BIS Summit 2026 — XIX ежегодная конференция по информационной безопасности, организованная BISA при поддержке ГК InfoWatch. Главная тема — «Искусственный интеллект: где граница между прогрессом и угрозой».

Ключевые заявления с площадки:

Федеральная служба по техническому и экспортному контролю (ФСТЭК) России разрабатывает новые требования к безопасности систем ИИ. Они будут привязаны к рискам и угрозам, а не к конкретным моделям. Главная задача — не допустить утечки данных через ИИ-модели и влияния ИИ-агентов на критическую информационную инфраструктуру (КИИ);

Наталья Касперская, президент ГК InfoWatch: «Риски внедрения ИИ начали осознавать на самом высоком уровне. Поскольку наша страна находится в чрезвычайно уязвимой в плане технологий позиции, нам надо быстрее, чем западному миру, адаптировать систему безопасности к искусственному интеллекту».

Анна Кулашова, вице-президент «Лаборатории Касперского»: «Атаки с ИИ начались с более качественного фишинга, а теперь используются в сложных таргетированных кампаниях. Что касается теневого ИИ, задача — не запретить, а возглавить и сделать процесс прозрачным и предсказуемым».

Yandex B2B Tech инвестировал более 7,5 млрд рублей в запуск нового направления Yandex Security и вывел на рынок решения класса AI-SPM для защиты ИИ-инфраструктур.

Месяц осведомлённости о кибербезопасности в 2026 году проходит на переломе: угрозы ускорились до машинной скорости благодаря ИИ, а защита по-прежнему держится на четырёх базовых привычках — уникальные пароли, MFA, обновления ПО и бдительность к фишингу. Разрыв между сложностью атак и простотой профилактики не сокращается, но именно это делает цифровую гигиену не формальностью, а критическим навыком.

Целуйко А.В.,
кандидат военных наук, доцент,
доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ

Косенок Ю.Н.,
доктор технических наук, профессор,
профессор кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ